Fiabilité et disponibilité du DNS

Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

16 mars 2010

Nous allons tous mourir !

(Exposé de Rod Beckstrom, ICANN, à la réunion de Nairobi en mars 2010.)

« *The DNS is more fragile than it has ever been and it could stop at any time. . . . As CEO of ICANN I met with heads of security for the 3 largest countries in the world and they are concerned.* »

Nous allons tous mourir !

(Exposé de Rod Beckstrom, ICANN, à la réunion de Nairobi en mars 2010.)

« *The DNS is more fragile than it has ever been and it could stop at any time. . . . As CEO of ICANN I met with heads of security for the 3 largest countries in the world and they are concerned.* »

Info ou intox ? Par delà son désir de « vendre » le projet de DNS-CERT, il faut bien constater que les problèmes existent.

Quelques problèmes de 2009

Quelques problèmes de 2009

1. Le 19 mai, presque tout l'Internet chinois paralysé par une panne du service de résolution de noms (attaque contre Baofeng, mais ayant rebondi sur les opérateurs réseaux).
   `http://www.bortzmeyer.org/panne-dns-chine.html`

Quelques problèmes de 2009

1. Le 19 mai, presque tout l'Internet chinois paralysé par une panne du service de résolution de noms `http://www.bortzmeyer.org/panne-dns-chine.html`
2. Le 12 octobre, tous les noms de domaine suédois disparaissent pendant une heure, suite à une bogue du logiciel de génération de la zone. `http://www.bortzmeyer.org/panne-de-point-se.html`

Quelques problèmes de 2009

1. Le 19 mai, presque tout l'Internet chinois paralysé par une panne du service de résolution de noms `http://www.bortzmeyer.org/panne-dns-chine.html`
2. Le 12 octobre, tous les noms de domaine suédois disparaissent pendant une heure `http://www.bortzmeyer.org/panne-de-point-se.html`
3. Le 23 décembre, un grand libraire en ligne stoppé par une attaque DNS réussie (il n'avait qu'un seul hébergeur DNS). `http://www.bortzmeyer.org/noel-a-ultradns.html`

Sécurité et disponibilité

Sécurité et disponibilité

1. Il n'y a pas que des attaques, il y a aussi des pannes (ou des catastrophes naturelles),

Sécurité et disponibilité

1. Il n'y a pas que des attaques, il y a aussi des pannes (ou des catastrophes naturelles),
2. Certaines mesures de défense protègent aussi bien contre les pannes que contre les attaques (*anycast*).

Sécurité et disponibilité

1. Il n'y a pas que des attaques, il y a aussi des pannes (ou des catastrophes naturelles),
2. Certaines mesures de défense protègent aussi bien contre les pannes que contre les attaques (*anycast*).

Ces quelques transparents parlent donc uniquement de **disponibilité**. Mais j'espère que la discussion couvrira bien tout le spectre de la sécurité.

Assurer la disponibilité

Assurer la disponibilité

1. Avec le DNS, c'est facile, la redondance d'un service faisant autorité est prévue dès le début (contrairement à HTTP),

Assurer la disponibilité

1. Avec le DNS, c'est facile, la redondance d'un service faisant autorité est prévue dès le début (contrairement à HTTP),
2. Deux serveurs, ce n'est pas assez, mettez-en au moins quatre,

Assurer la disponibilité

1. Avec le DNS, c'est facile, la redondance d'un service faisant autorité est prévue dès le début (contrairement à HTTP),
2. Deux serveurs, ce n'est pas assez, mettez-en au moins quatre,
3. Sur-avitailler : machines et réseaux pouvant tenir trois à cinq fois la charge normale (pour les cas de dDoS),

Assurer la disponibilité

1. Avec le DNS, c'est facile, la redondance d'un service faisant autorité est prévue dès le début (contrairement à HTTP),
2. Deux serveurs, ce n'est pas assez, mettez-en au moins quatre,
3. Sur-avitailler : machines et réseaux pouvant tenir trois à cinq fois la charge normale (pour les cas de dDoS),
4. Et, surtout, évitez le SPOF (*Single Point of Failure*). Ayez plusieurs sites physiques et, si possible, plusieurs opérateurs, plusieurs systèmes d'exploitation, plusieurs logiciels...

Et en cas de sous-traitance ?

Certaines organisations, conscientes de ne pas être des professionnels du DNS, recourent à la sous-traitance (exemple : Google DNS pour le service de résolution de noms).

Et en cas de sous-traitance ?

Certaines organisations, conscientes de ne pas être des professionnels du DNS, recourent à la sous-traitance (exemple : Google DNS pour le service de résolution de noms).

Attention, tous les sous-traitants ne se valent pas et la sous-traitance ne garantit pas que vous pourrez dormir sur vos deux oreilles.

Tester la disponibilité

Tester la disponibilité

1. Certains tests de Zonecheck aident : nombre de serveurs, dans des réseaux différents, . . .

Tester la disponibilité

1. Certains tests de Zonecheck aident : nombre de serveurs, dans des réseaux différents, . . .
2. Outils de suivi (comme mon ou Nagios). Attention à avoir plusieurs sondes.

Disponibilité d'un service de résolution de noms

Quels résolveurs utilisez-vous ?

Comme l'exemple « Baofeng » l'a montré, la résolution de noms peut être vulnérable aussi.
Certains FAI grand public ont un service de résolution de noms plutôt faible.