JOHANNESBURG – Session du GAC sur le roulement KSK
Jeudi 29 juin 2017 – 12:00 à 12:30 JNB
ICANN59 | Johannesburg, Afrique du Sud

DAVID CONRAD : … c'est comment le DNSSEC a été mis en œuvre. En 2010, lorsque nous avons signé la clef pour la première fois, nous avons dit à la communauté qu'au bout de cinq ans, nous la changerions. C'est que l'on connaît sous le nom de roulement de clef. On est en 2017 et nous sommes dans ce processus, ce processus est en cours. Dès qu'AdobeConnect se mettra de mon côté, je vous montrerai une présentation.

Nous sommes censés tenir une conversation de haut niveau pour vous permettre de comprendre. Nous avons transmis une lettre aux responsables de la règlementation dans 180 pays, à des représentants du GAC lorsque c'était pertinent. Dans cette lettre, nous avons informé les responsables de règlementation que le roulement de la clef arrivait et qu'ils devaient se renseigner au sein de leurs opérateurs de réseaux s'ils étaient prêts pour ce changement.

Ici nous avons un aperçu. La zone racine a une clef de signature de clef pour les extensions de sécurité du DNS dans la zone racine, pour le DNS donc. Ce sont des clefs cryptographiques

utilisées pour sécuriser les données au premier niveau. Une partie des données qui sont privées sont gardées dans les installations de gestion clefs, on en a deux, une sur la côte Est et l'autre sur la côte Ouest des États-Unis. Ces deux centres ont été établis en 2009 lorsqu'on avait encore le contrat avec le Département du Commerce des États-Unis.

Ces deux installations ont un niveau de sécurité assez élevé, avec une salle sécurisé avec en son sein une cage sécurisée contenant un coffre contenant des modules de sécurité matériels qui sont des dispositifs spécialisés qui contiennent les informations cryptographiques, c'est-à-dire la clef privée pour la zone racine. Donc tout est conservé dans les installations sécurisées, dans la cage, dans la salle, dans le dispositif et tout accès est contrôlé.

La partie publique de cette paire de clefs privée est copiée dans chaque résolveur de DNS qui exécute la validation du DNS sur la planète. Nous avons environ 100 millions de résolveurs partout dans le monde dont un petit pourcentage valide le DNSSEC, alors qu'il s'agit de millions de résolveurs qui ont ces informations de configuration.

Le clef est utilisée dans le DNSSEC pour établir une chaîne de confiance de la racine du DNS jusqu'au chaînon final qui est le dernier nœud de la recherche, ce qui garantit que les données

signées par le DNSSEC par le propriétaire de la zone ne seront pas modifiées par des attaques par exemple.

Diapositive suivante. Pourquoi faisons-nous ce roulement ? Notre meilleure pratique est mise en œuvre parce que si l'on a un modèle de base, on a tendance à le modifier de temps à autre pour nous assurer qu'il n'y a pas de risques qu'il soit connu à notre insu et pour garantir que notre infrastructure d'élaboration de mots de passe fonctionne pour que si l'on était forcé de modifier le mot de passe pour quelque raison que ce soit, ce soit possible, pour vérifier qu'on est en mesure de le faire.

C'est pareil pour le DNSSEC. On pourrait considérer la clef de signature de clef comme un mot de passe pour le DNSSEC. C'est pourquoi il faut s'assurer que l'infrastructure existante de modification de la clef fonctionne si jamais on devait y avoir recours, ce qui pourrait arriver, par exemple en cas de problèmes de technologie permettant à des informations cryptographiques d'être factorisées ou si l'on avait des indices comme quoi la clef a été compromise d'une façon ou d'une autre.

Le problème est que vu la quantité de dispositifs qu'il faudrait mettre à jour, cela doit être fait lentement et prudemment. Nous préférons que l'Internet continue à fonctionner pendant que

nous faisons cela. Mais si nous nous trompons au moment du roulement, les résolveurs, les serveurs qui reçoivent les requêtes des utilisateurs finaux pour chercher des noms sur Internet cesseraient de fonctionner dans toutes les zones signées. Depuis que la zone racine est elle-même signée, ce serait une très mauvaise journée pour tout l'Internet donc on préfère ne pas le faire.

Par conséquent, nous avons adopté une approche prudente avec autant de tests que possible pour garantir qu'il n'y aura pas de risque substantiel provoquant un problème avec la validation du DNSSEC sur Internet. C'est donc un processus de deux ans et demi.

Diapositive suivante. Voilà certaines dates à venir en matière de roulement. Le 19 septembre, la taille de la clef a été augmentée parce que nous avons dû ajouter la nouvelle clef au DNS pour son utilisation dans les cérémonies de signature de clef ultérieures. Les cérémonies consistent à prendre la clef privée dans l'installation et à signer une nouvelle clef de signature de clef que Verisign nous donne pour signer la zone racine. C'est ce que nous faisons chaque trimestre, c'est-à-dire que pour toutes ces activités, nous avons ces procédures de cérémonies de clef.

Donc, le 19 septembre 2017, la taille de la clef DNS sera rallongée, nous allons ajouter des caractères et le 11 octobre de

cette année, nous utiliserons cette clef pour la première fois. Cette date est la date à laquelle il est le plus probable qu'il y ait des occurrences inattendues, donc s'il y a des résolveurs qui n'ont pas changé leur clef d'ici le 11 octobre, ils ne pourront plus valider leurs noms de domaines dans leurs recherches. Leurs recherches leur donneront ces résultats « 2.404. erreur, résultat introuvable ».

Le 11 janvier, nous prendrons la nouvelle clef et nous supprimerons l'ancienne KSK qui ne sera donc plus disponible.

Le 22 mai, nous supprimerons la clef directement de la zone racine.

En août, elle sera complètement détruite, cette ancienne clef, pour être tout à fait sûr que tout est sécurisé.

Diapositive suivante. Sur qui cela aura-t-il un impact ? Sur les résolveurs et sur les distributeurs de logiciel qui devront intégrer la nouvelle clef dans leurs logiciels et dans leur distribution.

Les personnes qui opèrent l'intégration des systèmes, ce sont ceux qui installent et déploient les logiciels, il faudra qu'ils s'assurent d'avoir la version la plus récente de la clef dans le système qu'ils intègrent.

Les opérateurs de réseaux, ce sont eux qui en général exploitent ces résolveurs, ils devrons s'assurer que leurs systèmes peuvent supporter ce changement de clef.

Les opérateurs de service racine doivent être au courant, nous avons été en contact avec toutes ces personnes, parce que ce sont eux qui connaîtront le plus probablement des problèmes s'ils ne changeaient pas leur clef. En général, ceci résulterait du fait qu'un résolveur pourrait faire plusieurs essais pour exécuter la validation, la résolution si le DNSSEC ne fonctionnait pas. Ils verraient alors une augmentation au niveau du travail.

Les fournisseurs de services Internet seraient ceux qui recevraient les appels des clients en cas de problèmes si les opérateurs de réseaux ne mettaient pas leur clef à jour. Ce sont les FSI qui recevraient les appels, donc, et les utilisateurs finaux sur qui cela aurait un impact si l'opérateur de réseau ne mettait pas la clef à jour, puisque ce sont eux qui ne pourraient plus accéder aux sites sur Internet.

Diapositive suivante. Il faut qu'on se prépare, bien évidemment. Nous avons demandé aux opérateurs de réseaux s'ils avaient mis en œuvre et habilité la validation DNSSEC. Le cas échéant, ils devaient s'assurer de la mise à jour de cette clef. Historiquement, les résolveurs fonctionnaient tout seuls, il n'était plus nécessaire d'y penser, les gens le déployaient et

avaient des fichiers en mode lecture uniquement et ça ne présentait aucun problème. Ce serait un problème maintenant puisqu'on ne pourrait plus modifier la clef dans le disque.

Diapositive suivante. Il faut que les opérateurs de résolveurs sachent si le DNSSEC est habilité. Ils doivent s'assurer de comprendre comment la confiance est évaluée dans leur système. Ils doivent tester et vérifier que leur résolveur peut supporter un changement au niveau de la clef. Ils doivent vérifier leurs fichiers de configuration et que tout est à sa place.

Si la validation de DNSSEC est habilitée ou prévue dans leur système, ils doivent alors avoir un plan pour prendre part au roulement de la KSK. Par exemple, vérifier ce qui se passe le 11 octobre. Ils devraient également savoir quelles seraient les défaillances à attendre, quelles seraient les contingences. Ils devraient par exemple connaître les erreurs symptomatiques d'un manquement à la mise à jour de clef, quelle serait la réponse en cas de manque de réponse du serveur, justement. Merci.

Diapositive suivante. Malheureusement, vous ne pouvez pas voir l'image. Ce que l'on a à droite est une image du texte que nous avons envoyé, c'est la lettre que nous avons envoyée aux responsables de la règlementation de différents pays et aux représentants du GAC pour leur suggérer de communiquer avec

leurs opérateurs de réseaux pour s'assurer qu'ils étaient au courant du roulement de la clef.

Diapositive suivante. Et voilà, je suis à la fin de ma présentation. Si vous avez des questions à me poser, je suis là pour y répondre. Je serais bien sûr ravi de vous fournir toute information que je pourrais vous donner pour vous aider à en discuter avec vos opérateurs de réseaux. Je suis David Conrad, mon adresse mail est david.conrad@icann.org. Merci.

THOMAS SCHNEIDER : Merci, David. Première question : est-ce qu'il y a une ligne analogue de téléphone à nous indiquer en cas de défaillances ou de problèmes ? Et est-ce qu'elle fonctionnera 24 heures sur 24.

Je crois que les États-Unis ont une question.

DAVID CONRAD : Le centre de soutien global de l'ICANN a des numéros que vous pouvez appeler en cas d'urgence et qui fonctionnent 24 heures sur 24.

ÉTATS-UNIS : Merci, David. C'est une présentation très intéressante. Nous avons reçu votre lettre et, pour être honnête avec vous, ma réaction initiale était qu'il fallait travailler avec nos FSI.

Mais, pour ce qui est des directives que nous pourrions recevoir, qu'est-ce que le gouvernement devrait faire pour s'assurer que les FSI font leur travail ? Et est-ce qu'il y a autre chose que nous pourrions faire en interne pour assurer la réussite de ce processus ?

DAVID CONRAD : Les réseaux internes du gouvernement ont des résolveurs quelque part. Ils peuvent être externes, par exemple Google peut fournir des résolveurs externes, 888, et ces services sont utilisés par d'autres organisations. Le résolveur doit s'assurer qu'il est capable de supporter le changement KSK.

Google, bien sûr, est capable de gérer ce changement. Pour ce qui est des autres FSI, au niveau des entreprises, c'est bien de poser la question, savoir s'ils sont au courant de ce changement de clef. Ensuite, il faudrait leur demander s'ils ont le service de validation DNSSEC. S'ils ne l'ont pas, il faudrait les encourager à l'avoir. Mais s'ils l'ont, essayez de vous assurer qu'ils sont prêts pour ce changement de KSK et encouragez-les à participer aux efforts pour le roulement de clef mis en place par l'ICANN.

Ce que nous faisons ici reflète ce que nous avons fait déjà dans d'autres forums, c'est-à-dire essayer de faire en sorte que le plus de gens possibles soient au courant de ce changement de clef et encourager les gouvernements à entamer des efforts pour que

leurs opérateurs de réseaux soient au courant de ce changement.

THOMAS SCHNEIDER : L'Iran.

IRAN : Merci pour cette présentation. Avons-nous un canal de feedback pour nous assurer que les actions que vous avez indiquées sont dûment mise en œuvre avant qu'il y ait des défaillances, parce que nous ne sommes pas familiarisés avec ce type de dossier. C'est une question de feedback. On a reçu votre lettre et nous sommes en train de mettre en œuvre des mesures pour nous assurer que ce soit respecté. Avez-vous un système de retours où nous pourrions communiquer d'éventuelles difficultés ?

DAVID CONRAD : De manière générale, nous avons encouragé les gens à nous contacter s'ils ont des questions ou s'il y a des problèmes dont ils veulent nous faire part. Nous n'avons pas de mécanismes explicites pour recevoir les commentaires des gens mais nous travaillons avec des groupes d'opérateurs de réseaux, avec plusieurs organisations de TLDs afin d'établir un canal et cette communication avec eux, pour recevoir leurs commentaires et leurs retours.

THOMAS SCHNEIDER : J'ai l'Égypte, les Pays-Bas et le Royaume-Uni.

ÉGYPTE : Merci, Thomas. Et merci, David, pour cette présentation. J'ai une question sur la diapo numéro 5, mais entre temps, si j'ai bien compris, il y a un outil pour tester si l'opérateur est prêt ou non ?

DAVID CONRAD : Oui. Nous avons créé une plateforme de test qui permet aux opérateurs de résolveurs de participer à un essai en temps réel sur le roulement de la clef KSK. Cette plateforme de test ne figure pas dans ma diapo parce que c'est un peu plus technique, mais je peux vous fournir cette information si ça vous intéresse afin que les membres du GAC donnent ces informations à leur gouvernement.

ÉGYPTE : C'est très utile. Ma question concerne la diapo numéro 5. Je voulais m'assurer pour cet impact sur les opérateurs de résolveurs, je ne vois pas ici les opérateurs de registre TLD, est-ce qu'ils sont compris dans la case résolveurs ?

DAVID CONRAD : L'impact concerne le côté qui recueillit des informations des opérateurs TLD, donc les TLDs, ccTLDs, gTLDs ne seront pas directement affectés par le roulement de clef. Ils n'ont aucune action à mettre en place, c'est pour ça qu'ils ne figurent pas ici. Bien sûr, ensuite, ce sont les résolveurs qui doivent mettre en place des actions au niveau de leurs systèmes internes.

THOMAS SCHNEIDER : Merci. Les Pays-Bas.

PAYS-BAS : Merci, David, pour ces explications. Pour vérifier à nouveau certaines informations, je pense que les gouvernements n'ont pas de responsabilité formelle dans ce domaine, nous sommes plutôt un canal de sensibilisation. Je veux dire qu'il n'y a pas de responsabilité gouvernementale.

DAVID CONRAD : Bien sûr, tout à fait.

PAYS-BAS : Ensuite, il y avait une liste de résolveurs de DNS récursifs qui mettent en place la validation DNSSEC. Dans chaque lettre, il y en avait sept ou huit, je crois que nous les avons contactés

directement, mais y-a-t-il d'autres impacts pour les parties prenantes ? Doivent-ils changer leur système ?

DAVID CONRAD : Le changement de clef se produira de manière automatique, c'est-à-dire qu'un logiciel sera incorporé et permettra de faire des mises à jour au niveau de la clef. Ce serait prudent peut-être de participer aux tests qui sont mis en place pour s'assurer qu'au moment du roulement de la clef, tout est prêt. Mais en définitive, il s'agit d'un système automatique qui est introduit dans les systèmes pour que ce changement se fasse automatiquement.

Si les opérateurs n'ont pas mis en place le roulement automatique, à ce moment-là, ils devraient modifier la configuration de leurs données et cela concernera la clef publique associée au DNSSEC, cette nouvelle clef devrait être copiée dans leur configuration. C'est la façon manuelle dont les opérateurs devraient prendre en charge ce changement de clef.

ROYAUME-UNI : Merci, David, d'être venu nous expliquer cette question.

Je n'ai pas discuté avec les membres britanniques de l'unité constitutive des FSI qui s'occupent de la connectivité, je vais le faire. Mais j'imagine que ce sont eux les parties prenantes qui

sont impactées par ce changement et ce sont eux que vous souhaitez que nous contactions pour nous assurer que tout est prêt. Je n'ai pas vu la lettre non plus, alors il faudrait que je vérifie l'avoir reçue.

Si j'ai bien compris, vous avez dit qu'il faudrait vérifier au niveau des FSI au gouvernement, vérifier que eux aussi sont prêts à mettre ce changement en place.

Que faites-vous le 11 octobre ? Si quelque chose se passe mal parce que les gens n'ont pas pris les mesures nécessaires pour supporter ce changement, est-ce que cela pourrait avoir des conséquences pour les gouvernements par rapport à la manière dont les choses se passent ? Comment pourrait-on gérer un dysfonctionnement important ?

DAVID CONRAD : Nous avons été en contact avec les FSI et avec les unités constitutives qui regroupent les FSI, ainsi que les opérateurs de réseaux.

Pour ce qui est d'une défaillance possible ou que ça se passe mal, nous avons établi un système de veille ou d'observation assez performant pour voir comment la racine serait affectée. À ce moment-là, nous pourrions voir comment se passent les choses et nous avons des plans de secours, bien sûr, que nous

mettrions en place si nous identifions qu'il y a des défaillances majeures au niveau du fonctionnement des résolveurs après le roulement de clef.

Bien sûr que les gouvernements devront supporter la rage des utilisateurs finaux si les systèmes ne fonctionnent pas correctement, et moi-même, je serais la cible de ces critiques si les choses se passaient mal. Mais l'important c'est de pouvoir mettre à jour les informations et que les gens soient au courant.

THOMAS SCHNEIDER : J'ai une annonce importante à vous communiquer. Le représentant du Nigéria, s'il vous plaît. Ne partez pas, c'est la dernière intervention que nous allons accepter puis nous devrons arrêter.

NIGÉRIA : Merci beaucoup pour ces explications. Ma question est la suivante : pour les FSI qui n'ont pas mis en place la validation DNSSEC, que se passe-t-il avec eux ? Les FSI qui n'ont pas la validation DNSSEC dans leur système.

DAVID CONRAD : Il n'y aura pas de changement pour eux. S'ils ne proposaient pas ce service de validation DNSSEC, le roulement de la clef n'aura

aucun impact sur eux. Si, à l'avenir, ils souhaitaient valider le DNSSEC dans leur système, alors il faudrait s'assurer de posséder la clef la plus récente. Autrement, la validation ne pourra pas se faire et il y aurait des confusions. Ils devraient alors s'assurer qu'ils ont le dernier logiciel ou la dernière clef à jour.

THOMAS SCHNEIDER : Nous devons nous arrêter ici parce que nous avons une annonce importante à vous faire.

Comme vous le savez, c'est notre dernier déjeuner ensemble, dans cette réunion, ce qui veut dire que c'est le dernier déjeuner d'Olof dans sa fonction – quelle est votre fonction, en réalité ? - en tant que soutien du GAC. C'est grâce à lui qu'on fait toujours des blagues, et son soutien est toujours nécessaire.

Julia, elle se cache, comme d'habitude, quelque part. Est-ce que vous pourriez venir, Julia, pour nous aider à organiser ce petit cadeau pour Olof ?

Nous allons vérifier avec les gens de la technique pour voir comment vous pourrez ramener ça chez vous. Il y a une carte, aussi. Voilà le cadeau. Ce n'est pas très lourd donc ça devrait le faire.

Donc, avec ce petit présent, on tient à remercier Olof. Il y a des verres un peu cachés au fond de la salle. Nous voulions donc fêter ce dernier déjeuner que nous partageons avec vous, Olof. Merci beaucoup.

OLOF NORDLING : Merci beaucoup à tous.

J'ai toujours aimé les cadeaux aussi grands. Je vous remercie du fond du cœur. J'espère que nous resterons en contact, même si je prends ma retraite. Je serai là jusqu'à la fin du mois de juillet. Vous n'allez pas vous débarrasser de moi complètement.

Merci beaucoup.

THOMAS SCHNEIDER : Très bien.

BRÉSIL : Pour ce qui est des séances après le déjeuner, nous nous réunissons ici, si j'ai bien compris. Mais quel est l'objectif ? Parce qu'il faudra rediscuter du communiqué à un moment donné ou est-ce que ce ne sera pas nécessaire ? Quel est le plan ? Hier, vous avez dit que nous devrions nous réunir à un moment donné.

THOMAS SCHNEIDER : Nous allons voir si le texte préparé nous convient. Nous allons essayer de le lire pendant la pause déjeuner. L'idée, c'est de l'avoir prêt avant 15 heures et de passer quelques minutes à faire une lecture finale.

Ne partez pas encore, on n'a pas fini. Mais tout d'abord, on va faire un toast pour Olof. Merci beaucoup.

[FIN DE LA TRANSCRIPTION]