SAN JUAN – Atelier de DNSSEC - Partie 1
Mercredi 14 mars 2018 – 9h00 à 10h15 AST
ICANN61 | San Juan, Porto Rico

JACQUES LATOUR: Bienvenus à cet atelier DNSSEC. Donc aujourd'hui, nous avons uniquement l'audio sur Adobe, toutes les diapositives sont disponibles sur le site de l'ICANN pour l'atelier DNSSEC.

Il y a une adresse email qui vous permet de répondre aux questions. Voilà ce qui va se passer pour aujourd'hui.

Donc bienvenus à cet atelier DNSSEC, vous avez ici le comité pour le programme d'aujourd'hui. Nous nous retrouvons toutes les semaines pour planifier des ateliers DNSSEC ? Nous essayons d'avoir un contenu pertinent et adéquat pour tous les participants du monde entier.

Donc merci aux participants au programme.

Nous avons aujourd'hui un déjeuner qui sera sponsorisé par Afilias, CIRA et SIDN. Jim, Christian merci beaucoup.

Mais il faut au moins avoir une réponse juste à l'interrogation pour pouvoir manger… Non, c'est une blague.

Donc l'interro, le test d'aujourd'hui c'est de ne pas oublier les questions de la réunion, et les réponses dans l'ordre. C'est ça le défi pour aujourd'hui.

Donc le déjeuner est sponsorisé, vous avez votre billet sur la table. Donc vous avez besoin de ce billet pour aller manger.

Donc le programme d'aujourd'hui a été organisé par ISOC et le SSAC. Et tout ce que nous faisons lors de ces ateliers en général est intégré au programme Deploy 360 Internet Society. Donc Dan York est chargé de ce projet, et pour l'instant il se débrouille très bien.

Alors pour ce qui est de l'ordre du jour d'aujourd'hui, la journée est bien remplie. Nous aurons un panel sur les activités DNSSEC, donc Comcast, CIRA ? Nic.BR, Fred etc. Donc une heure là-dessus. Ensuite l'après-midi il y aura plusieurs présentations, KSK, Sentinel, CZ.NIC avec des expériences de validation DNSSEC au CPE, CIRA sur HSM et le roulement de clef, et Joe sur NTA, ainsi que quelques points de vue par rapport à ça.

Et ensuite, l'interro, le test DNSSEC, le repas de midi, quelques présentations l'après-midi sur DANE, ça ce sera intéressant, il y aura des ateliers pratiques, donc je pense que ce sera intéressant. Et ensuite une discussion avec un panel sur le roulement de KSK.

Alors, c'est la tradition, donc regardons ce qu'il se passe dans le monde entier, en matière de déploiement de DNSSEC. Donc les statistiques.

Dan York fait le suivi de tout ce qui se passe en matière de DNSSEC. Il y a un rapport détaillé qui est disponible, sur le site ISOC, avec donc le déploiement jusqu'à 2016. Donc c'est le dernier rapport que nous avons là-dessus.

Alors pour ce qui est des statistiques, la tendance était en augmentation jusqu'en juillet de cette année. Et après, il y a eu un petit problème, je na sais plus quel est le nom…

NON IDENTIFIE: BNSL.

JACQUES LATOUR: BNSL s'est éteins, donc la validation DNSSEC BNNSL a été éteinte, on espère que ce sera rallumé, que se sera remis en route après le roulement, mais voilà donc l'impact que peut avoir un FSI sur la totalité, parce qu'en fait cela représente énormément d'utilisateurs. Donc c'est malheureux mais c'est comme ça.

En ce qui concerne les statistiques par région, vous les voyez. Donc en haut, 58 %, jusqu'à 2 %. Donc le DNSSEC n'est pas

universellement répandu, il y a certaines régions qui l'utilisent plus que d'autres, donc il y a encore du travail à faire pour que les FSI valident.

De l'autre côté, du côté TLD, déploiement TLD, on est à 90 % de TLD signés dans la racine et je crois que ce chiffre va rester à ce niveau-là pendant longtemps. Les 10 % qui restent vont prendre un certain temps, donc il nous reste encore du travail.

Donc nous avons 1544 TLD signés, donc c'est bien, on progresse.

Donc ces statistiques, ce sont des statistiques des domaines signés, c'est un pourcentage de domaines signés par TLD. C'est difficile à lire en fait. Vous voyez la diapositive. Donc davantage de statistiques. Vous avez le lien en dessous si vous voulez avoir les statistiques DNSSEC Stats, vous pouvez allez voir, ça peut être intéressant. Simplement parce que voilà, c'est intéressant.

Donc ce que nous avons c'est des cartes en fait, du monde, avec des couleurs, qui vous donnent le statut des différentes régions avec les couleurs. Donc vous voyez ici la carte DNSSEC du monde.

Il y a 7 ans, je me souviens que ces cartes étaient relativement vides, il n'y avait pas beaucoup de vert, beaucoup de mises en place partielles ou expérimentales. Alors il y a encore quelques

régions qui ont besoin de travailler, mais c'est quand même relativement positif, même s'il reste du travail.

Justement, en Afrique, il y a beaucoup de CC qui n'ont pas annoncé, qui n'en sont même pas au statut expérimental pour les ccTLD. Alors il peut y avoir deux raisons à ça. Si vous souhaitez mettre en place le DNSSEC, il faut informer Dan York, auquel cas dans la communauté, et à ce moment-là vous êtes sur la carte. Donc c'est un problème aussi d'information.

Là ça progresse, l'Asie Pacifique c'est beaucoup mieux. Il reste encore quelques pays et régions qui manquent mais ça commence à démarrer relativement bien.

Vous voyez des informations dans ce petit encadré.

L'Italie, enfin, par rapport à la question qui a été posée, c'est toujours coloré en vert, donc DS dans la racine. Donc pas d'acceptation des bureaux d'enregistrement. Je ne sais pas s'il y a des Italiens dans la salle… Non ? Alors je ne sais pas… Donc DS dans la racine, c'est l'hypothèse, c'est ce que nous avons imaginé, mais si le DS est accepté par le bureau d'enregistrement, il faut que l'on passe à une autre couleur, donc il faut qu'on soit informé de ça.

Ensuite, la région LAC, il en manque quelques-uns. Donc là aussi il faut sensibiliser. Donc je crois que LAC TLD est en train de travailler là-dessus.

Amérique du Nord et Groenland, on en est presque au vert partout, donc ça avance. Donc ça, ça permet de bien faire augmenter le pourcentage, ces couleurs.

NON IDENTIFIE: Est-ce que vous pouvez revenir en arrière, en Amérique Centrale ? Moi je voulais simplement mentionner le Panama, parce que c'est là qu'on va la prochaine fois, n'est-ce pas ?

JACQUES LATOUR: Oui, tout à fait. Effectivement peut-être qu'on devrait organiser quelque chose sur le DNSSEC là-bas.

D'accord… voilà l'Amérique du Nord… Donc les cartes sont disponibles en ligne, sur Deploy 360. Vous pouvez vous inscrire, je crois que vous recevez des informations tous les mois, ou deux fois par mois, avec toutes les informations, les fichiers JPEG, toutes les données, vous pouvez vous inscrire, tout est en ligne.

Ensuite, l'ISOC est en train de travailler à un projet sur l'historique du DNSSEC. Donc si vous avez des informations qui

ne sont pas sur ce site, n'hésitez pas à nous le dire, on pourra mettre à jour les informations sur tout l'historique du DNSSEC.

Et voilà, c'est tout ce que j'avais à vous dire. Y a-t-il des questions ?

ABDALMONEM GALILA: Je suis coach ICANN pour l'Égypte. Ma question est relative à la différence entre le DS dans la racine et le statut opérationnel. Donc DS dans la racine, ça veut dire qu'un bureau d'enregistrement peut ajouter au niveau du registre, ou est-ce que le bureau d'enregistrement peut proposer des sites DNSSEC pour le bureau d'enregistrement ?

JACQUES LATOUR: Alors, en vert clair, il y a une chaine de confiance. Alors en plus foncé, c'est difficile, mais c'est lorsqu'il y a acceptation du titulaire de nom de domaine, du DS, donc il peut signer la zone. Le bureau d'enregistrement Donc ils ont EPP et ils acceptent l'enregistrement dans le web.

ABDALMONEM GALILA: Alors l'Egypte doit changer de couleur?

JACQUES LATOUR: Donc DS dans la racine vous.

ABDALMONEM GALILA: J'avais parlé lors de réunions précédentes de l'ajout, de prendre en compte les ccTLD IDN pour l'Egypte. Mais peut-être qu'il faudrait identifier les IDN et ASCII ? Ca, c'est pour le .eg, pas pour l'IDN. Mais ça c'est pour l'IDN, c'est pas pour le .eg.

JACQUES LATOUR: Effectivement, vous avez raison. D'accord, je le note.

NON IDENTIFIE: c'est plus facile, si possible, surtout dans ce type de situation, d'envoyer des emails directement à Dan York ou au comité qui s'occupe du programme DNSSEC, parce que ça, ça nous intéresse ce type d'information.

NON IDENTIFIE: Petit commentaire, je n'ai pas trouvé de domaine signé en Italie. Donc s'ils le délèguent et bien ils le cachent bien. Mon serveur n'a pas trouvé un seul domaine signé en Italie. Donc je pense qu'ils ne délèguent ou alors ils cachent vraiment les premiers cas.

JACQUES LATOUR: C'est donc un secret. Très bien, merci. D'autres questions ?

MATS DUFBERG: Je me demande pourquoi le certificat de déploiement du .ORG, DNSSEC donc a expiré. En aout 2017.

JACQUES LATOUR: Dan York, est-ce que vous nous écoutez ? Alors, n'oubliez pas de donner votre nom avant de prendre la parole et j'aurais dû d'ailleurs mentionner sur quelle diapositive je suis, parce qu'en fait il y a des gens qui nous écoutent et qui écoutent uniquement l'audio.

MATS DUFBERG: Il y a un lien au déploiement du DNSSEC et à l'historique, j'essayais d'y accéder et le certificat a expiré.

JACQUES LATOUR: Merci, on va voir ce qu'on peut faire.

Très bien. Des questions ?

Alors, il nous reste encore une minute, et je ne sais s'il y a des personnes de la région africaine qui prévoient de mettre en place le DNSSEC dans la salle et qui pourraient nous mettre à jour ? Il n'y a rien qui se passe là-bas ?

Très bien, merci.

Donc la session suivante, c'est la discussion du panel sur les activités DNSSEC. Et notre premier intervenant, c'est Joe Crowe de Comcast.

JOSEPH CROWE: Bonjour à tous, je m'appelle Joe Crowe. Comme Jacques l'a dit, je suis de Comcast, je travaille à Comcast depuis 4 ans en tant que responsable ingénieur.

Comcast a mis en place le DNSSEC depuis 2012, nous avons non seulement fait la validation de toute notre empreinte, nous avons également effectué la signature de DNSSEC sur 5000 zones, plus de 5000 zones.

Nous validons pour plus de 20 millions de clients. Donc le DNSSEC est extensible. Il y a des problèmes opérationnels en cas d'échecs de la validation DNSSEC, on a des appels, et donc effectivement il y a un coût associé à ça. Et ça, c'est un des gros problèmes que nous avons, même si ce n'est pas nous en fait qui sommes responsables de l'interruption.

Excusez-moi, c'est la première fois que j'interviens, et en plus c'est vraiment très tôt. Donc vous m'excuserez.

Alors, du point de vue des problèmes opérationnels, alors premièrement la mise en place des DNSSEC sur toute notre empreinte, c'est-à-dire s'assurer que tous nos résolveurs sont à

jour, s'assurer que les numéros de version de nos résolveurs, les logiciels de nos distributeurs sont conformes avec tout ce que nous devons faire en matière d'automatisation.

L'automatisation, c'est vraiment la plus grande initiative au cours des 4 dernières années que nous avons mise en place. Il y a différents outils d'automatisation que nous avons mis en place, nous avons utilisé SaltStack récemment qui nous permet d'automatiser un endroit et jusqu'à plusieurs distributeurs. Du côté des résolveurs, DHCP.

Donc lorsque vous avez des centaines et des centaines de serveurs sur votre empreinte, il faut absolument utiliser cette méthode, parce que vous n'allez pas manuellement changer tout ceci. Le changement manuel, c'est forcé qu'à moment ou un autre, vous allez avoir un problème.

Donc nous avons récemment essayé de voir comment faire EDNS0 et nous avons essayé de le mettre en place avec un… En fait il y a un cout parce qu'il faut un CPU, une unité de traitement, donc étant donné le nombre de requêtes que nous avons par jour et même par seconde, il faut absolument s'assurer de faire les choses correctement pour les gens du CDN, pour qu'ils aient la bonne réponse par rapport à la géolocalisation, d'avoir la bonne réponse. Et l'idée c'est vraiment de s'assurer qu'il n'y a pas de problème de

performance pour nous et nos clients. Vous savez, ces petites millisecondes s'ajoutent et deviennent quelque chose d'énorme.

Alors depuis 2015 nous avons commencé à utiliser DANE pour les mails. Au début, c'était un problème du point de vue opérationnel, parce que nos serveurs faisant autorité à l'époque n'avaient pas d'enregistrement TLSA à utiliser. J'ai dû donc essayer de voir comment utiliser le R7 type 52, et donc j'ai dû utiliser nos résolveurs pour nous assurer qu'ils faisaient autorité et que le reste du monde pouvait utiliser ces enregistrements. Ensuite, le lancement n'a pas été problématique.

L'équipe avec laquelle je travaille s'en occupe depuis 2015 et nous avons donc lancé le programme, le test a eu lieu en 2014.

Alors, à l'avenir, dans notre infrastructure, nous allons utiliser de plus en plus DANE pour tous les enregistrements TLS. C'est en fait un CE interne, nous l'utilisons comme ceci. Il y a beaucoup de choses que nous auto-signons à l'interne, sans utiliser de CE externe, surtout étant donné les couts qui sont associés.

Vous savez peut-être, pour certains d'entre vous, que si vous utilisez plus de 5000 zones à l'interne, et si vous ajoutez à ça le nombre d'équipes qui sont dans la zone racine, et si vous souhaitez avoir propre TLS, votre propre certificat,, toutes ces équipes, c'est un cout énorme. Parce que si les gens disent on va passer à [inaudible] et s'ils dépensent quelques centaines de

dollars par an, c'est certes quelque chose qui n'est pas très adéquat. Donc voilà, il vaut mieux faire comme ça, à l'interne.

Alors du point de vue opérationnel, on essaye de voir comment faire notre roulement de clef DS. Comme je l'avais dit, c'est 5000 zones. Donc c'est énorme comme travail à effectuer. Donc lorsqu'on re-signe, il faut mettre à jour les enregistrements DS ? Il n'y a pas de processus automatique pour le faire, tout est manuel, il y a beaucoup de choses que l'on fait avec nos bureaux d'enregistrement là-dessus.

Et donc il y a plusieurs personnes dans l'équipe qui ont essayé de voir comment on peut automatiser le processus, de manière à faire un roulement sécurisé, mettre à jour notre DS, resigner quand c'est nécessaire.

Il y a eu des problèmes, il a fallu faire passer des zones d'un serveur faisant autorité à un autre, et il a fallu donc resigner.

Donc l'idée c'est vraiment de s'assurer que tout ce qui est opérationnel nous soit bénéfique. Nous sommes une grande société, je sais que tout le monde a ce type de problème, mais pour nous ceci est d'autant plus important parce que nous sommes une grande société. Et donc il faut absolument s'assurer que ça fonctionne correctement, sans problème, parce que ça coute cher. Même un tout petit problème peut nous

couter des dizaines de milliers de dollars. Et je parle là d'une période de 5 à 10 minutes. Et en plus tous les clients appellent.

Hier il y a eu un problème au STATE.GOC, avait un problème de DNSSEC. Donc on a reçu un email, en fait c'était un tweet de quelqu'un qui nous a dit : et dit donc, le State.Gov, donc le département d'État, a un problème de DNSSEC. En fait il y avait un problème de cache parce qu'ils avaient mis à jour des informations de leur côté.

Mais bon, ce sont de petites choses, et donc lorsqu'il y a des problèmes de DNSSEC, les gens s'adressent à notre équipe DNSSEC, et en fait le meilleur moyen de nous contacter, c'est tweeter, Tweeter Comcast, parce que vous arrivez directement sur un ingénieur de notre équipe.

Et donc on surveille notre tweeter 24 h sur 24 et 7 jours sur 7.

Voilà, c'est tout ce que j'avais là-dessus par rapport à notre travail à Comcast et le DNSSEC.

Je ne sais pas s'il y a des questions ?

JACQUES LATOUR: Russ ?

RUSS MUNDY: Merci beaucoup de nous avoir rejoints à cet atelier, c'est très positif. Nous avons très bien travaillé avec Comcast par le passé, et nous le ferons dans l'avenir.

Dans votre présentation, vous avez parlé de l'impact de l'EDNS. Et je suis sûr que vous faites des tests en interne et que vous avez publié des informations sur DNSSEC, l'impact du DNSSEC sur les serveurs faisant autorité.

Mais je ne suis pas sûr si vous avez des informations disponibles, par rapport aux résolveurs validants, et à la question de savoir si l'EDNS est utilisé ou pas.

J'aimerais donc que vous demandiez dans votre société si des informations en ce sens pourraient nous être fournies. Cela pourrait aider les autres et nous donnerait un point de référence que d'autres opérateurs pourraient regarder pour mettre en œuvre leurs tests.

JOSEPH CROWE: Je suis d'accord avec vous, je pense que ce type de données serait très utile pour la communauté DNSSEC dans son ensemble. Je vais bien sûr remonter cette information.

RUSS MUNDY: Ce serait très bien pour la publicité de Comcast.

NON IDENTIFIE: Russ, une question de clarification, quand vous avez parlé de EDNS, parliez-vous d'une extension spécifique de EDNS 0 ?

JOSEPH CROWE: Quand j'ai parlé de EDNS0, je parlais notamment des résolveurs.

NON IDENTIFIE: Oui, c'est ce que je disais.

Pour ce qui est des défaillances dans ce sens, il y a eu en 2016, en 2017, récemment on n'en a pas eu de ce type de défaillances, mais si on pense à 2016, il y en a eu 6 qui étaient chiffrées. Il y avait eu des données brutes qu'on avait reçues et c'est pour ça qu'on avait publié dans la zone. Je ne sais pas comment on avait fait, mais ce serait intéressant d'avoir des informations là-dessus.

JACQUES LATOUR: Jeff et puis Warren.

JIM: En général, quand on parle de DNSSEC, on parle des résolveurs et on sait qu'il faut du temps et beaucoup d'attention parce qu'on peut mettre en place des encres de confiance négatives.

Alors que dites-vous aux autres fournisseurs de service internet qui se penchent sur cette question des ancres de confiance négative ?

JOSEPH CROWE: Il faut valider DNSSEC, c'est ça la réponse. C'est très facile d'allumer, si vous voulez, ce type de solution. C'est une solution qui est un peu obscure, mais quand il y a une validation qui est mise en place, nous ne pensons plus à qu'est-ce qu'il va se passer.

Je vais parler plus tard sur cette question en particulier, donc je vais rentrer dans le détail après.

JACQUES LATOUR: Warren?

WARREN KUMARI: Je ne me sens pas très bien parce que nasa.gov a eu un petit problème à un moment donné, et state.gov également a trouvé des difficultés en signant le DNSSEC. Alors ce serait important que les gens arrêtent de casser DNSSEC, ce serait génial.

JOSEPH CROWE: Oui, nous recevons les appels, bien sûr, mais oui, je suis tout à fait d'accord. Notamment quand il y a des pannes qui se

produisent, HBO par exemple, quand le DNS est en panne, c'est nous qui sommes les coupables finalement aux yeux des gens.

JACQUES LATOUR: Vous avez dit que vous avez plus de 5000 zones que vous gérez, est-ce que vous vous êtes penché sur l'automatisation CDNS des clefs ?

JOSEPH CROWE: Nous ne sommes pas allés aussi loin parce que nous avons d'autres projets sur lesquels nous nous penchons, mais à chaque fois qu'on essaye d'examiner cela, il y a quelque chose d'autre qui se présente.

JACQUES LATOUR: Et la dernière remarque que j'ai est la suivante : alors l'utilisation de DANE, est-ce que vous avez trouvé que cela conduit à des bénéfices ? Si vous faites cela, vous pouvez avoir des effets positifs ?

JOSEPH CROWE: Oui, je suis d'accord avec vous. Nous testons cela et nous voyons que cela peut nous faire progresser parce qu'il y a un retour sur investissement qui est intéressant lorsqu'on parle de ce type de projet.

JACQUES LATOUR: Merci beaucoup. Est-ce qu'il y a d'autres questions ?

Très bien. Prochaine présentation, c'est Jacques Latour de CIRA, c'est-à-dire moi-même, activités DNSSEC au Canada et au .CA.

Alors, nous avons pu faire un suivi de l'application de DNSSEC au Canada pour identifier les tendances générales pour la validation de .CA au Canada. Il y a certains FSI qui ont décidé de ne pas mettre en place DNSSEC. Il n'y en a pas beaucoup, mais il y en a certains. Et donc la tendance change.

Heureusement, éventuellement, il y aura d'autres fournisseurs qui vont réactiver DNSSEC, et si vous avez des informations qui pourraient encourager ce type de fournisseurs pour qu'ils comprennent la valeur ajoutée que représente DNSSEC, ce serait intéressant de les recevoir.

Entre temps, nous essayons de faire des présentations auprès des FSI pour voir quels sont les bénéfices des DNSSEC. Nous avons mené des actions de sensibilisation, mais ça reste quand même assez difficile.

Ici, vous voyez [Telko], au canada, vous voyez qu'il y a Teksavvy, c'est le seul qui fait la validation DNSSEC, il y a un autre FSI qui s'occupe des échanges internet de Canada, et c'est l'un des plus modernes FSI.

Pour le reste, ils ne sont pas intéressés à mettre en place DNSSEC. Nous avons beaucoup travaillé affaires avec ces gens, pour qu'ils adoptent DNSSEC.

Activités dans .CA ; nous avons suffisamment de noms signés pour générer un schéma, ou un graphique, c'est bon signe déjà. Nous avons généré ce schéma ce mois-ci, nous avons 1256 domaines signés. En juillet 2017, on a fait l'intégration DNSSEC avec CIRA, et avant cela, nous n'avions pas GoDaddy avec nous. C'était dommage, mais maintenant ils sont là. Mais l'impact de cela n'a pas non plus créé beaucoup de demandes au niveau du trafic.

CIRA travaille à l'automatisation de CDS à travers le fichier de zone, pour essayer d'automatiser les opérations qui ont lieu à ce niveau-là. On essaye d'avoir CDS disponible dans le fichier de zone pour que tout cela fonctionne.

Alors l'adoption DNSSEC est plutôt lente, nous avons très peu de bureaux d'enregistrement qui ont adoptés DNSSEC, GoDaddy l'a adopté, mais les bureaux d'enregistrement ne sont pas intéressés à adopter DNSSEC avec les titulaires. Ils ne sont pas intéressés à ces clefs.

Et cela prouve qu'il y a un besoin d'automatisation CDS et des clefs CDNS.

Nous commençons à voir cette question de l'automatisation. Le problème c'est que nous n'en sommes pas au stade de production encore. Et même en interne nous essayons, nous avons des difficultés pour que l'on attribue une priorité à ce dossier. Il y a des nouvelles plateformes qui sont en préparation, mais d'ici 6 mois nous pourrions faire des progrès là-dessus. En interne, comme je vous ai dis, cela traine un peu. C'est triste, mais c'est la réalité.

Nous avons donc le DPA qui peut accepter la demande des opérateurs pour accepter ou éliminer les enregistrements DS, nous devons travailler sur le protocole pour que ce soit plus automatisé. Si nous voulons que les opérateurs fassent quelque chose par rapport au DPA, ça doit être dans leur zone, sans aucune mise à jour. Alors, je pense que le fait de scanner une zone assez large, c'est la meilleure façon de faire, mais on doit, il faut que certains opérateurs puissent travailler un peu plus sur la base de la réalité.

Et voilà tout ce que j'ai. Il ne se passe pas grand-chose au Canada au niveau du .CA.

Y a-t-il des questions ? Jacques ?

NON IDENTIFIE: En tant que l'un de vos bureaux d'enregistrement, et l'un des rares qui le font, j'ai des domaines signés, et je rencontre le problème habituel. Je suis un gestionnaire DNS, mais je n'utilise pas CDS encore. Donc quand est-ce que je vais pouvoir utiliser CDS ?

VIKTOR DUKHOVNI: J'ai un commentaire.

JACQUES LATOUR: Pouvez-vus dire votre nom s'il vous plait.

VIKTOR DUKHOVNI: Je l'ai fait.

JACQUES LATOUR: Excusez-moi.

VIKTOR DUKHOVNI: J'ai trouvé 24 domaines en .CA qui ont CDS, et CIRA Labs est l'un d'entre eux. Il parait que vous êtes en train de tester cela, c'est très bien. Voilà mon commentaire.

JACQUES LATOUR: Merci beaucoup. Russ?

RUSS MONDY: Avez-vous des plans pour essayer de faire en sorte que les bureaux d'enregistrement soient plus nombreux à adopter DNSSEC ? Ou qu'ils changent leur mentalité, penser qu'il n'y a pas de retour sur investissement à l'adoption de DNSSEC.

JACQUES LATOUR: L'idée c'est un petit peu de travailler avec eux pour essayer qu'ils arrêtent d'utiliser PowerDNS, et essayer d'échanger des informations. Je ne sais pas si ça donnera des résultats, mais on essaye de faire en sorte qu'ils puissent utiliser DANE pour la messagerie et en gros essayer de travailler avec eux. Mais le transfert des enregistrements DS, cela n'est pas possible.

RUSS MONDY: Donc la coopération en terme de soutien au DNSSEC, puisqu'il n'y a pas d'impact financier, ils mettent les registres, mais ils ne veulent pas investir de l'argent pour incorporer toutes les fonctionnalités du système, c'est bien ça ?

JACQUES LATOUR: Oui, exactement. Alors, nous avons organisé un atelier sur DNSSEC et le transfert des informations DNSSEC ne fait pas partie de l'enregistrement des noms de domaine. Ça ne fait donc

pas partie des informations d'enregistrement. Et il y a d'autres informations qui sont mises à jour automatiquement.

D'autres questions? Christian ?

CHRISTIAN HASSELMAN: Est-ce que vous parlez avec les FSI qu'on a vus sur la liste ?

JACQUES LATOUR: Oui. Je rencontre les différents FSI du Canada, je leur présente le DNSSEC, les DNSSEC, mais ils s'en fichent.

Par contre, les statistiques par rapport à l'IPv6 sont beaucoup plus encourageantes. Mais les DNSSEC, on a encore du travail là-dessus.

Y a-t-il d'autres questions ?

Alors, prochaine présentation, c'est Carlos Acosta de NICPR.

CARLOS ACOSTA: Bonjour, je m'appelle Carlos. Une brève histoire de .PR.

Tout d'abord on était un laboratoire de recherche, nous travaillions sur plusieurs dossiers, comme par exemple l'encrage numérique ou la clef cryptographique publique ou d'autres projets. Ensuite, c'était un centre de sciences informatiques, et nous nous penchions sur beaucoup de questions concernant le

chiffrement et c'est pour ça que nous nous sommes intéressés à la question de la sécurité du DNS.

En 2000, un site du gouvernement a été redirigé vers un site malveillant, au niveau du FSI, et cela aurait pu être évité si on avait eu DNSSEC.

Ensuite, la Suède a été le premier ccTLD qui a proposé DNSSEC, et on a compris que c'était le chemin à suivre.

En 2006, en juillet, nous avons commencé à signer des zones, mais ça n'a été qu'au mois d'aout de la même année que nous avons pu enregistrer ces enregistrements dans les serveurs publics.

Voilà les zones que nous avons déployées au niveau du DNSSEC, c'est une liste assez considérable. Et ensuite, nous avons créé une page web pour informer le public ou les parties intéressées, où on en était par rapport à la mise en œuvre du DNSSEC. Et à ce moment-là nous avons encouragé le gouvernement à signer le nom de domaine du gouvernement pour éviter les problèmes qu'ils avaient pu rencontrer auparavant.

Il y a quelques années, nous avons signé un programme d'encouragement pour commencer à signer d'autres clients.

Vous voyez ici un schéma qui correspond à décembre de l'année dernière, pour voir combien de zones signées nous avions et

combien de zones non signées. Nous avons un peu plus de 1 % à décembre de l'année dernière. Ici vous voyez ce que représente ce 1%, 9 % ont été signés par les bureaux d'enregistrements et le reste par nous.

Vous voyez ici un aperçu des détails par rapport à la façon dont nous gérons la signature DNSSEC. Nous avons des machines avec des serveurs Windows 2003, nous utilisons VBScript pour signer DNSSEC. Et nous vérifions que tout fonctionne correctement avec des résolveurs ouverts DNSSEC et en utilisant DNSViz.

Et c'est à peu près tout. Voilà un bref apercu. Avez-vous des questions ?

Très bien, s'il n'y a pas de question, je vais donner la parole à Jim.

JIM GALVIN: Merci beaucoup Carlos.

Je suis Jim Galin, d'Afilias, et je vais aller directement à cette diapositive.

Donc Afilias vient de faire la transition du .PR, nous sommes donc passés à nos services en janvier et c'était justement le moment de parler des processus de transition des TLD.

Je sais que nous avons beaucoup parlé de roulement de clef, mais vous savez, l'expérience a été bonne pour nous, nous avons pu travailler avec le .PR là-dessus, c'était un plaisir puisqu'ils ont adopté assez tôt les DNSSEC. Et donc on a pu un petit peu parler de tout ce processus.

Alors, je passe à la diapositive 7. Donc Afilias, comme le .PR, est impliqué dans le DNSSEC depuis très longtemps. Nous n'avons pas été premiers, mais nous avons commencé le DNSSEC en 2008, nous avons commencé à signer des TLD en 2009. Donc ça fait déjà un certain temps qu'on travaille là-dessus, et au fil du temps, nous avons fait la transition pour un certain nombre de TLD. Certains d'ailleurs nous ont quittés, malheureusement, mais nous avons fait la transition quand même d'un certain nombre de TLD.

Ensuite, diapositive 9, ce qui est intéressant, je crois, c'est qu'il y a beaucoup d'attention qui est prêtée au roulement de KSK de la racine, et de toute évidence, c'est important parce qu'il y a un certain risque. Il y a beaucoup de technologie qui s'occupe de ce roulement, mais ce qui est intéressant au niveau des TLD c'est que comme pour la racine, la proposition est en fait un risque et les conséquences et les effets, s'il y a quelque chose qui se passe mal, sont très importants. Donc au niveau du TLD, vous pouvez perdre tout un TLD et devenir invalide.

Je crois que nous le comprenons tous, nous tous qui travaillons dans la technologie. Et donc il faut vraiment réfléchir à tout ce processus et voir où sont les points difficiles.

Alors ensuite, diapositive 9. Ce qui est intéressant, à mon avis, c'est qu'il y a des étapes administratives qui ne sont pas sous notre contrôle. En tant que fournisseur de service, le problème qu'on a c'est qu'en fait il y a deux choses, deux parties. Il est facile de dire oui il faut que j'aille parler à l'autre fournisseur de service, là où se trouve le DNS, mais en fait il faut qu'il y ait quelque chose qui se passe avec l'IANA aussi. Parce qu'il faut avoir les nouveaux enregistrements DS à mettre dans la racine. Et donc c'est ce processus supplémentaire, ce processus que vous ne maitrisez pas.

Et donc il y a des étapes de validation IANA aussi qui sont effectuées pour s'assurer que cette interaction se passe.

Tout ceci doit être documenté.

Ensuite, l'étape suivante, c'est lorsque vous êtes prêt à lancer tout ceci, il y a encore un lien à avoir avec l'IANA, avec la transition, et donc lorsque vous roulez votre propre clef, votre propre zone, lorsque vous ajoutez un nouvel enregistrement de clef, lorsque vous déplacez votre serveur de noms, vous déplacez un serveur de noms mais il faut coordonner ceci avec la partie tierce, et donc le problème c'est le calendrier.

Le processus est assez clair, facile, si vous vous occupez de votre propre zone, dans votre propre environnement, parce que le délai en général est déterminé par plusieurs TTL, et votre gestion de ces TTL. Mais dans ce cas, lorsqu'on a ce roulement avec les TLD, le processus prend un certain nombre de semaines pour qu'il soit bien fait, pour s'assurer que toutes les étapes d'administration soient effectuées.

Alors en ce qui nous concerne, nous avons une double vérification à chaque fois que nous faisons quelque chose. On vérifie avant de passer à l'étape suivante que toutes les [inaudibles] sont là. Donc c'est un processus assez lourd du point de vue administratif pour s'assurer que tout se passe bien.

Ensuite, diapositive 14, je vais en parler un petit. Je parlais justement des problèmes que nous avons rencontrés. Le .PR a parlé des machines Windows qu'ils utilisaient pour tout ceci, même aujourd'hui. Nous avons eu ce type de problème avec des technologies très anciennes et de processus anciens. Surtout pour les petits TLD.

Un des avantages que nous avons, étant donné que nous sommes un FSI important, beaucoup de nos processus sont automatisés, comme la plupart des personnes qui sont présentes dans la salle. Mais le problème en fait c'est l'installation. Il nous faut absolument bien voir ce que font les

fournisseurs actuels, il faut trouver un moyen d'intégrer notre travail avec le leur, d'avoir les données de zone qui sont envoyées. Et également la question c'est de gérer ces étapes de changement des clefs.

Autres choses auxquelles nous sommes confrontés, c'est les différentes politiques. Alors, je sais qu'on se concentre énormément sur le côté technique, mais en terme de meilleures pratiques, on avait deux serveurs clients en fait, mais c'est assez surprenant lorsqu'on a des ccTLD, on avait un seul serveur de nom objet dans les systèmes. Et donc ça c'est un problème. Donc il faut à un moment s'occuper de ce problème. Et s'occuper des enregistrements dans le système. C'est pas uniquement les TLD, c'est aussi les données que l'on a, les domaines de deuxième niveau pour s'assurer que toutes les politiques sont à jour. Et donc ce type de chose ralentit le processus de transition, le transfert, parce que vous avez l'impact des données d'enregistrement.

Autre problème que nous avons eu, c'est les problèmes d'incohérence des données. Et pour nous, lorsqu'on a des problèmes de ce type, parfois, par exemple nous avons eu des problèmes de présence dans la zone, ça faisait partie d'une transition, on n'avait même pas fait attention à ça, donc il a fallu mettre à jour les processus pour ne pas avoir de problème à l'avenir.

Et donc le message que nous avons à vous transmettre, c'est que cela demande énormément de personnel ce roulement de TLD, donc un cout important ce roulement de KSK. Ce n'est pas uniquement la partie technique, de toute évidence on en a déjà parlé, mais c'est toutes les activités supplémentaires qui s'y ajoutent.

Nous avons une liste de contrôle que nous suivons de manière très prudente, il y a toujours des choses qui se produisent et il faut s'occuper de tous ces incidents.

Et donc nous avançons, nous commençons à mieux comprendre les DNSSEC, nous faisons vraiment le suivi de tout ce qu'il se passe en matière de pénétration des DNSSEC dans la communauté dans son ensemble, et je crois que ce type de question est important.

Ce n'est pas aussi facile en fait qu'on pourrait le penser.

Voilà, c'est tout ce que j'avais à vous présenter.

JACQUES LATOUR: Merci Jim. Des questions ?

JAROMIR TALIR: Je vois que vous utilisez l'algorithme 5 pour le DNSSEC. Est-ce que vous allez passer à autre chose pour le DNSSEC ?

JIM GALVIN: Nous ne prévoyons pas immédiatement de modifier ça, mais effectivement c'est quelque chose que nous surveillons de près. Nous n'avons pas encore décidé ce que nous allons faire et quel algorithme utiliser pour l'instant.

NON IDENTIFIE : C'est quoi cet algorithme 5 d'ailleurs ? Des questions ? Non ? Ça va ? Très bien, Carlos alors. Carlos et Jim merci. Nous avons Frederico Nevis avec le roulement d'algorithme DNSSEC pour le .BR.

FREDERICO NEVES: Alors, bonjour, je m'appelle Frederico, je travaille pour l'opérateur de registre .BR.

Deuxième diapositive. Donc un petit historique de l'opérateur de registre DNSSEC.

Nous avons commencé en 2007, en utilisant le RSASHA1. Et en 2009, avec l'arrivée de l'adoption nsec3 et du refus nsec3, nous avons pu signer des zones plus larges. Donc nous avons signé toutes les zones .BR à ce moment-là. Nous avions environ 75 zones et nous en avons maintenant 90, avec beaucoup d'ajouts

d'extensions géographiques, de domaines de deuxième niveau, les citées du Brésil donc ;

En 2010, un peu avant la signature de la zone, nous avons fait notre premier roulement de KSK et nous avons mis à jour le DPS avec taille de la clef de 1280 bytes, et nous avons également utilisé un nouveau plan pour la cérémonie avec un DHSM. Et donc voilà ce que nous utilisons depuis.

Nous avons réussi à arriver dans la racine avec le DS. En fait à mettre le DS dans la racine en juin. Et en 2015, suite à notre DPS, nous avons à nouveau roulé notre KSK. Et à l'époque nous avons utilisé la même taille de clef, donc 1535 bytes.

Actuellement, nous avons environs 3,9 millions de délégations qui, pour la majorité, sont au deuxième niveau, .COM .BR, et environ un million de délégations signées.

Alors, justement pour le sujet d'aujourd'hui, par rapport aux motivations, donc le roulement d'algorithmes, la plus grosse motivation en fait, c'est d'être prêt en cas de roulement d'algorithme en urgence. Donc de préparer le logiciel à ce type de situation

Nous avons notre propre signataire, donc le logiciel actuel n'a pas la possibilité, n'a pas des capacités d'agilité d'algorithmes. Donc en temps de paix, l'idée c'est d'être vraiment prêts.

Nous sommes passés à l'ECDSAP226SHA256, grâce à mes collègues qui sont à ma gauche, parce que eux, ils ont déjà été confrontés à un enjeu avec le ping IANA. Donc l'IANA est maintenant prêt, et nous ne devrions pas avoir de problème pour rouler l'algorithme à l'avenir.

Donc il y a un bénéfice pour nous, un avantage supplémentaire, parce que certaines de nos zones plus grandes utilisent le NSEC3 avec la preuve de non-existence, dans certains enregistrements, dans certains types. Et donc nous n'avons plus besoin d'avoir une clef séparée, étant donné l'historique du protocole, le roulement d'algorithmes que nous avons utilisés pour introduire le NSEC3.

Notre système d'avitaillement actuel commence à vieillir un peu. Il a été écrit en 2004, et à l'époque nous n'avions pas toute la bibliothèque DNS, donc on a dû écrire notre propre système pour entretenir les choses. Donc on aimerait s'en débarrasser. Donc c'est un autre avantage du changement de ce logiciel donc.

Diapositive 4.

Donc la méthode pour le roulement d'algorithme. Comme je l'avais dit, nous avons notre propre signataire, nous avons dû décider de la manière de reconstituer l'algorithme. Donc nous avons commencé à faire des recherches, quelles sont les

recommandations que nous avons, et donc 6781 recommandent que le roulement soit fait de manière conservatrice. Mais tous les signataires open source que nous avons pu obtenir en fait, font le bind avec des clefs gérées et avec OPENDNSSEC. Donc il y a une autre approche qui est l'approche libérale, et c'est ce qui est utilisé par ces signataires open source. Mais nous, nous souhaitions avoir une approche plus conservatrice.

Au cours de la semaine passée, lors de la réunion OARC, nous avons obtenu davantage d'informations là-dessus, et donc nous savons maintenant que le logiciel qui utilise cette démarche conservatrice a déjà 7 ans. Donc ça commence à vieillir. Et il y a 5 ans, nous avons eu une clarification sur le 6740 par rapport à ce langage 4035 qui n'est pas très clair.

Donc il y a une certaine controverse qui existe. Et donc le roulement d'algorithme du .SE a très bien marché, ils ont utilisé le OPENDNSSEC, tout a très bien fonctionné.

Donc en fait, nous allons tester les deux approches, les deux démarches, et nous verrons par la suite comment ça se passe.

Alors au cours des mois à venir, nous allons rouler, mais comme vous le savez, il y a beaucoup de procédures, c'est compliqué, il y a différentes étapes pour s'assurer que tout fonctionne correctement. Alors voilà ce que nous allons faire. Mi-mai, nous allons mettre à jour nos HSM et nous allons avoir un troisième

site qui sera mis en place dans un autre lieu, par rapport aux autres sites qui sont à Sao Paolo.

Nos HSM ont été mis en place en 2010, ils fonctionnent toujours bien, mais nous allons en fait en éliminer deux et les changer pour que l'on puisse être compatibles avec le nouvel algorithme. Et ensuite il y aura la cérémonie de roulement, c'est une cérémonie qui ira de aout 2018 à janvier 2019.

En ce qui concerne le roulement test, la cérémonie de roulement test, il y en aura une pour commencer, qui utilisera les deux méthodes.

Passons à la diapo suivante, nous sommes à la diapo 6 pour ceux qui nous écoutent à distance.

Donc nous aurons 6 zones. Sur 3 de ces zones, on va utiliser la méthode conservatrice, et avec les trois autres zones, on utilisera la méthode libérale.

La raison pour laquelle nous avons ces trois zones, c'est que dans la zone BR, nous avons des clefs partagées, et dans d'autres, nous avons une seule clef.

Donc voilà.

Et pour la majorité nous utilisons le NSEC, nous essayons de couvrir toutes les situations.

Nous devrions avoir le début de ce roulement sera en juin, le 19.

Pour ce qui est de la surveillance, nous allons suivre le .SE. Le SIDN Labs a publié un rapport détaillé sur la surveillance du roulement, et donc nous allons utiliser leur méthode pour surveiller les tests ainsi que le roulement. Donc je vous recommande de lire ce rapport.

La cérémonie de roulement aura lieu le 23, 24 juillet sur nos sites. Et nous allons mettre à jour tous les logiciels signés ainsi que le matériel. Nous allons nous préparer à l'exportation des clefs. Parce que lorsque nous avons de nouvelles clefs pour les cérémonies, il y a beaucoup d'étapes pour l'exportation de ces clefs, et pour l'importation des HSM.

Donc nous allons en fait modifier notre approche, nous avons un nouveau format qui nous permet de faire plus d'agrémentation par jour, parce qu'il y a augmentation de la publication de la zone à 5 minutes.

Pour terminer, dernière diapositive, donc les changements visibles qui pourront être observés au cours des mois à venir sont les suivants. Donc les roulements tests commenceront à se faire le 19 juin, ils se termineront le 22 juin. Le roulement d'algorithme, si tout va bien, devrait avoir lieu le 20 aout. Et si tout va comme nous le prévoyons, nous devrions le terminer le

27 aout pour la première fenêtre de clefs signées. Parce qu'il y a aussi la communication avec l'IANA.

Donc voilà, c'est tout ce que j'avais à présenter. Je ne sais pas s'il y a des questions.

VIKTOR DUKHOVNI: Félicitations d'avoir adopté DNSSEC de manière si importante. Il y a des petits problèmes que l'on retrouve dans certaines délégations, si vous pouvez m'aider à me mettre en contact avec eux.

FREDERICO NEVES: Excusez-moi, je n'ai pas compris ce que vous avez dit.

VIKTOR DUKHOVNI: Il y a certains petits nombres de domaines que vous avez délégués, dont la gestion DNSSEC n'est pas tout à fait parfaite, si vous pouvez m'aider à entrer en contact avec eux, ce serait génial. Merci.

JACQUES LATOUR: Y a-t-il d'autres questions ? J'ai une question. CZ essayait de migrer vers le ECDSA, est-ce que vous essayez de faire la même chose ou est-ce que vous êtes compatibles ?

FREDERICO NEVES: Oui, maintenant on est compatible, oui tout à fait.

JACQUES LATOUR: Très bien. 3, 2, 1… Pas de questions ?

NON IDENTIFIE: Oui, c'était par rapport à l'application que vous avez utilisée. Est-ce que vous avez une documentation sur les tests que vous avez effectués ? Et puis voilà, j'aimerais savoir comment en fait on peut transmettre les tests que vous avez effectués à une plus large communauté et notamment ceux issus des Caraibes francophones, comme la Guadeloupe dont je viens.

JACQUES LATOUR: La documentation, est-ce que vous allez la publier, est-ce que vous pouvez la partager avec la communauté des caraïbes.

FREDERICO NEVES: Oui, oui, nous prévoyons de publier ce rapport début du mois de juillet. Et nous allons publier également un blog par rapport à cela.

JACQUES LATOUR: Très bien. Merci beaucoup de cette traduction. D'autres questions ? S'il n'y en a pas, on passe à la pause. Très bien nous avons encore 5 minutes pour la pause et nous nous retrouvons ici à 10h30 pour la deuxième partie de cet atelier. Merci beaucoup.

[FIN DE LA TRANSCRIPTION]