ABOU DABI – Atelier sur les DNSSEC - 1e partie
Mercredi 1 novembre 2017 – 09h00 à 10h15 GST
ICANN60 | Abou Dabi, Émirats arabes unis

RUSS MUNDY : Bonjour à tous. Bienvenue à cet atelier du déploiement du DNSSEC. Je suis Russ Mundy. Ici, vous avez Jacques Latour qui travaille avec les registres.

Est-ce que vous m'entendez ? Ah, d'accord.

Bien. Donc nous allons avoir aujourd'hui cette séance. Je crois qu'il y a des nouveaux, des gens que je n'avais jamais vus dans cet atelier. Nous voudrions que cet atelier soit une activité interactive, dans la mesure du possible. Donc tout le monde devrait avoir son programme et à l'arrière du programme, vous avez un ticket pour votre déjeûner, si vous voulez déjeûner ici. Ce ticket de repas nous est offert par le sponsor, notre sponsor. Nous allons vous le présenter bientôt. Voilà, le voilà. Voilà notre sponsor ou nos sponsors : Afilias, CIRA et SIDN, nos trois sponsors, plus .ca. En tout cas, ça, c'est la partie importante : nous allons applaudir nos sponsors qui nous ont offert ce déjeûner pour cet atelier. Bien.

Aujourd'hui, nous allons travailler, donc Russ, c'est moi, et Jacques et Dan qui vont être aussi parmi nous. Donc Jacques va

faire une présentation. Dan va faire la première partie. Donc nous allons commencer par Jacques d'abord.

JACQUES LATOUR : Nous allons regarder l'ordre du jour d'abord. Parfait. Donc aujourd'hui, nous aurons une introduction des normes dans le monde entier. Ensuite, on parlera du DNSSEC, des activités du DNSSEC qui vont se focaliser sur les régions. La deuxième partie de cet atelier va porter sur l'état actuel du roulement de clés de signature de clés. Nous en parlerons. Ensuite, nous aurons le quiz du DNSSEC. Je sais qu'il y a beaucoup de gens qui viennent seulement pour participer à ce quiz. Après le repas, nous aurons plusieurs présentations sur différents points liés au DNSSEC. Bien, donc une bonne journée de travail. Commençons par l'état du DNSSEC dans le monde.

Donc l'état du déploiement du DNSSEC, un rapport correspondant à l'année 2016. Si vous regardez ce lien, vous allez trouver un rapport assez étendu sur l'état du DNSSEC qui correspond donc au déploiement de 2016. On a fait un bon travail pour réunir tout ce matériel. Donc si vous voulez un petit peu en savoir plus sur le DNSSEC, c'est là qu'il vous faut commencer. Il y a beaucoup de références, beaucoup d'informations pour comprendre un peu davantage ce qu'est le DNSSEC. Bien.

Alors qui est ici pour la première fois ? Qui sont les personnes pour qui cet atelier du DNSSEC est le premier ? Bien, parfait. C'est bien de le savoir. Je vais voir si vous avez déjà vu cela auparavant ou pas. Donc je ne vais pas aller trop vite.

Ici, vous voyez donc, ce sont des données fournies par APNIC, le lab d'APNIC, concernant la validation du DNSSEC et son utilisation. Lorsque j'ai vu ce graphique pour la première fois, j'ai remarqué qu'il y avait un creux au niveau du mois de juillet et je pense que vous aurez peut-être des commentaires à faire là-dessus.

JEFF HOUSTON : En Inde, nous avons beaucoup de clients. Au mois de juillet, ils ont arrêté et c'est pour cela qu'on a cette baisse. Il y a deux raisons possibles à cela ; je n'aurais pas posé la question mais deux raisons. La première, c'est qu'ils ne s'étaient pas rendus compte que ça s'était interrompu. C'est déjà arrivé au Yémen. Et l'autre explication, c'est qu'ils ont décidé qu'ils n'allaient pas le faire, qu'ils n'allaient pas l'utiliser. Donc je ne sais pas quelle est la bonne explication. Est-ce que quelqu'un d'Inde peut nous donner davantage de précisions là-dessus ? En tout cas, c'est tout ce que je sais personnellement.

JACQUES LATOUR : Merci. Est-ce qu'il y a quelqu'un de l'Inde qui peut nous donner quelques précisions ici ?

ORATEUR NON-IDENTIFIÉ : Oui. Bonjour, je suis d'Inde mais je ne sais pas. Nous allons essayer d'obtenir davantage de renseignements et nous vous donnerons ces informations.

JACQUES LATOUR : Très bien, donc une action à suivre. Envoyez un courriel. Nous voulons savoir quelle a été la raison pour laquelle... l'une des deux raisons, c'est-à-dire on l'a arrêté ou on ne s'était pas rendu compte que cela ne marchait pas. Bien. En tout cas, si hormis cela, vous voyez qu'il y a une tendance à la croissance, en général, assez régulière.

Dans la région maintenant. Donc en premier lieu, l'Afrique du Sud avec 38 % de DNSSEC et ensuite, on arrive jusqu'à 2 %. Les bonnes choses, ce sont les chiffres publiés par Google, le PDNS. Donc cela veut dire que vous avez votre propre infrastructure dans la région, que vous comptez complètement sur Google pour faire votre DNS. Donc c'est positif.

En termes de validation du DNSSEC pour l'Asie, nous avons l'Irak avec 57 % et 25 % sur Google, et c'est assez positif. Et on arrive jusqu'à 0,50 % pour le Koweït. Donc il y a du travail à faire, avant

ou après le roulement de clés. Mais il va falloir s'en occuper. C'est une bonne occasion de le faire.

En termes de déploiement de TLD dans le monde entier, nous en sommes encore à 90 % de tous les TLD dans la zone racine qui sont signés, et à peu près 4 % du domaine de deuxième niveau qui sont signés. Et en général, 30 % d'utilisateurs sont validés.

Donc ce sont des nombres clés. Il faut s'en souvenir. Cela est basé sur Rick Lamb, qui est un centre de recherche de DNSSEC Stat. Donc je pense qu'il faudra un bon moment pour arriver jusqu'à 10 % mais bon, c'est un travail que nous devons réaliser.

Maintenant, les TLD de premier niveau et dans les nombres de domaines signés. Donc .nl avec 48 % de domaines signés, 2,8 millions de domaines, suivi par le Brésil, 23 %. C'est un nombre total de domaines signés. Et ensuite, on a .te en dernier.

Donc maintenant, Rick est train de chercher le nombre de domaines qui utilisent le système DNSSEC spécifique. Donc si ça vous intéresse, vous pouvez rentrer sur le site et regarder. Ils ont ce type de données. Si vous voulez parler à Rick, il est là-bas.

Alors maintenant, on regarde l'implémentation du TLD dans la région. Donc nous avons cinq états différents et Dan a fait un suivi de chaque TLD en se basant sur leur niveau, s'ils étaient en train de faire des expériences, s'il y avait un engagement public

pour déployer le DNSSEC dans leur région, où est-ce que c'était signé, s'ils avaient la technologie pour le faire, est-ce que DS était dans la racine, ce qui veut dire qu'il y a une chaîne au repos mais aucun des bureaux d'enregistrement n'accepte les enregistrements DS, et opérationnel signifie qu'ils acceptent des délégations signées. Donc tout cela est fait de manière manuelle parce que ce n'est pas quelque chose que nous pouvons faire sur les réseaux. Donc c'est basé sur les discussions, sur les commentaires. Lorsque le TLD planifie de faire quelque chose, on est au courant et on met ce type de statistiques à jour. Voilà, c'est comme cela que cela marche.

Donc nous avons fait cette carte du monde en nous basant sur ces données pour voir quel était l'état actuel. Nous avons fait de gros progrès. On pourrait comparer la situation à il y a un ou deux mais en tout cas, je peux vous dire qu'on fait de gros progrès. Avant, il y avait beaucoup de jaune et de rouge sur cette carte, donc vous voyez que cela évolue.

Il faut remarquer qu'il y a 46 DS en racine, ce qui veut qu'il y a beaucoup de bureaux d'enregistrement qui acceptent le DNSSEC. La clé semble être un problème, un défi pour certains TLD. C'est quelque chose que nous devons analyser.

Dans la région de l'Afrique, nous avons montré l'état actuel de la région avec ces couleurs. Donc la Guinée-Bissau, .gw, a signé au

mois d'octobre. Et l'Afrique du Sud, .za, est en état opérationnel, ce qu'on appelle opérationnel donc c'est positif. Ce sont des bonnes choses.

En Asie, .sa est devenu opérationnel, donc pour l'Arabie Saoudite ; on peut les applaudir. C'est une bonne chose. Et on a plus ou moins le même scénario, 24 opérationnels, 17 DS en racine.

Qu'est-ce qui vous empêche de devenir complètement opérationnel ? Les personnes qui sont de cette région, est-ce que vous pouvez nous expliquer un petit peu, les personnes qui sont de ce ccTLD ? Ou bien est-ce que c'est une question de mise à jour dans vos opérations ? Bien, je reposerai cette question un petit peu plus tard.

En Europe maintenant, nous avons les îles Åland, .ax, au mois d'août. Alors l'Italie nous manque. Donc on voit qu'il y a des progrès aussi.

Alors l'Amérique du Sud : en Argentine, il manque un petit peu de travail à faire ; Bermuda, .bm, au mois de juin mais il y a encore du travail à faire dans cette région.

Et le Groenland, donc deux DS dans la racine. Nous avons rencontré quelqu'un du Groenland, nous savons que cela existe.

Si ce type de choses vous intéressent, cette carte et toutes ces images, si vous souscrivez à cette liste, vous pouvez les recevoir, recevoir du matériel tous les mois avec toutes les modifications qui ont lieu. Comme cela, si vous faires des recherches sur le DNSSEC, vous pouvez utiliser cette information. Cela peut être utile. Et elle est basée sur les mises à jour que Dan effectue. Voilà.

Donc il y a un projet d'histoire du DNSSEC qui est en cours de réalisation. Vous pouvez aller voir l'état actuel de ce projet. Vous avez ici l'URL. Et vous pouvez voir où est-ce que nous en sommes. Si vous avez besoin de contenu ou si vous pouvez nous fournir des informations aussi qui pourraient nous être utiles, si vous avez besoin d'information pour le déploiement du DNSSEC aussi dans votre région, vous pouvez vous rendre donc sur ce site et vous trouverez du matériel.

Est-ce que vous avez des questions ?

JULIE HEDLUND : Nous avons un commentaire dans la salle Adobe Connect. Ce commentaire est de Abdalmonem Galila. Donc c'est un commentaire, premier commentaire concernant les données et la carte : « Est-ce que vous pourriez tenir compte des TLD d'IDN ? » Et le deuxième commentaire : « Je pense que ces cartes sont pour des ASCII et pour des TLD IDN. Est-ce que vous

pourriez faire une différence entre les ASCII et les DNSSEC avec IDN, les TLD signés sur la carte ? »

JACQUES LATOUR : Je crois que je vais demander à la personne qui a fait ce travail parce que ce travail se fait manuellement. Il dépend de la communauté. Donc s'il a ces informations, je pense qu'il peut le faire. Donc s'il me faire part de ces informations, je pourrai le faire.

ORATEUR NON-IDENTIFIÉ: Je suis [inintelligible]. Je viens du registre d'Indonésie .id. Vous avez parlé de ce qui est en vert, DS dans la racine. Quel est le critère que vous avez utilisé pour le DS dans la racine ?

JACQUES LATOUR : Cela veut dire que vous avez signé votre zone avec le DNSSEC et vous donnez à IANA les enregistrements DS pour mettre dans la zone racine. Mais si vous êtes un titulaire de registre, vous pouvez mettre les enregistrements DS dans votre zone parce que vous êtes supporté, vous ne faites pas l'EPP pour supporter le DNSSEC ou autre, vous n'utilisez pas notre système pour faire cela.

ORATEUR NON-IDENTIFIÉ : D'accord. Je peux vous donner... Est-ce que vous pouvez nous donner une URL pour supporter cela ?

JACQUES LATOUR : Dans le registre pour savoir comment supporter cela ? Vous avez votre propre registre ou vous utilisez une tierce partie ?

ORATEUR NON-IDENTIFIÉ : Nous utilisons une tierce partie mais nous avons aussi développé le DNSSEC dans l'état de développement. Il n'est pas encore complètement opérationnel. Nous utilisons un registre de tierce partie.

JACQUES LATOUR : Donc vous nous demandez de vous fournir un soutien ?

ORATEUR NON-IDENTIFIÉ : Oui.

JACQUES LATOUR : Et ensuite ?

ORATEUR NON-IDENTIFIÉ : Nous avons demandé au bureau d'enregistrement de supporter le DNSSEC mais il n'est pas entièrement supporté.

JACQUES LATOUR : Donc vous supportez le EPP DNSSEC ? Donc techniquement, vous devriez être opérationnel. Si votre bureau d'enregistrement ne le supporte pas, c'est un autre problème. Les clés DS, si vous avez cela, vous devriez être opérationnel.

ORATEUR NON-IDENTIFIÉ : Nous avons environ 15 bureaux d'enregistrement mais actuellement, il y en a seulement huit qui supportent entièrement le DNSSEC.

JACQUES LATOUR : Quel est votre TLD ?

ORATEUR NON-IDENTIFIÉ : D'Indonésie, .id.

JACQUES LATOUR : Vous êtes en vert, d'accord. Donc on devrait avoir une couleur différente lorsque tous vos bureaux d'enregistrement supportent le DNSSEC. C'est cela ? Ou alors, mettre des petites étoiles.

Est-ce qu'il y a d'autres questions ? C'est une séance interactive. Plus vous poserez des questions, plus vous en apprendrez. Merci.

Nous avons maintenant l'atelier numéro 1. Il s'agit d'une discussion du panel sur les activités du DNSSEC, et c'est moi qui modérera la séance. Et puis nous avons Raed Alfayez qui va parler de la mise en œuvre du DNSSEC et des noms de domaines. Bienvenue.

RAED ALFAYEZ : Bonjour à tous. Je m'appelle Raed Alfayez.

Cette présentation, je l'ai déjà faite dans la journée technique donc j'espère que ce ne sera pas ennuyeux pour vous. J'ai enlevé quelques diapositives pour aller un peu plus vite. Je suis du NIC d'Arabie Saoudite où nous avons récemment déployé le DNSSEC dans notre TLD, .saudia et l'IDN, et donc le .sa est dans notre IDN. Pardon, c'est mal écrit en arabe, je ne sais pas pourquoi on ne le voit pas correctement. Mais pourtant, je vais également ajouter un onglet, donc pas de problème. Les lettres sont séparées, je ne sais pas pourquoi. Je vous enverrai une version mise à jour par la suite.

Alors nous avons commencé à gérer le DNSSEC en trois étapes. Donc notre méthodologie était de diviser en étapes. D'abord, on

avait une étape de suivi. Nous avons contrôlé les RFC, les outils et les logiciels, en attendant à ce qu'ils soient suffisamment mûrs pour que l'on puisse les mettre à jour sans de modification radicale dans l'avenir. On voulait donc que le déploiement se fasse en douceur en Arabie Saoudite.

En 2015, nous avons commencé avec le travail préliminaire. Nous avons commencé par une étude complète. Il y a eu beaucoup de pays qui ont été ajoutés à notre référence, des pays leaders en matière de DNSSEC. Nous avons lu le RFC puis nous avons fini par élaborer un plan de déploiement pour savoir quels seraient les détails. Et puis, nous sommes passés à une étape de mise en œuvre qui était divisée en trois étapes à la fois, donc on a commencé l'année dernière. Et la deuxième étape était cette année. Donc cela a été complété.

Notre méthodologie, elle est au pas à pas. Nous nous sommes plutôt concentrés sur ce que nous avions écrit et on avait fait énormément de tests, on avait des laboratoires d'essais. Donc lorsqu'on voyait des textes et du ASCII, on essayait de l'essayer pour voir ce que ça donnait. Nous avons donc fait l'étude et suite à l'étude, nous avons fini par déployer le DNSSEC en trois étapes. Donc d'abord, en obtenant l'expérience locale sur le DNSSEC au niveau local, dans notre organisation avec le DNSSEC et avec les fournisseurs de télécommunications. La deuxième étape était l'élaboration d'un prototype. Donc nous

avons commencé par essayer de signer dans une petite zone. On a demandé à nos clients de faire signer leur bloc pour qu'ils essaient de l'essayer et qu'ils comprennent les informations. À ce moment-là, ils allaient être en mesure de bien le mettre en œuvre dans tous leurs noms de domaine et dans les noms de domaine de tous leurs clients aussi. Nous avons créé une liste d'échange interne pour notre équipe de travail. Donc si on voulait discuter d'un sujet, on le mettait sur la liste, on demandait à tout le monde de le lire et c'était comme cela également que nous avons pris les décisions pour le GSK, pour tout ce qui était technique, comme le KSK aussi. Et puis nous sommes passés aux aspects opérationnels des techniques pour que tous nos clients puissent mettre en ligne ce système.

Nous avons organisé des séances de formation, qui est un aspect clé pour le succès du DNSSEC. Nous avons commencé par un cours de trois journées qui a compté 25 participants de 11 organismes gouvernementaux et d'opérateurs de TIC en octobre 2015. Un deuxième cours a été tenu en mai cette année où nous avons expliqué un peu plus de détails et nous avons eu 41 participants de 29 agences gouvernementales, des opérateurs de TIC et de quelques banques. Et puis en mai, nous avons organisé un évènement d'un jour après la formation, où nous avons eu 120 participants d'Arabie Saoudite dont la plupart sont soit des chefs de département d'informatique ou de

département de sécurité, des FSI. Donc c'était un évènement ouvert à tous ceux qui étaient intéressés par le DNSSEC. Toutes ces séances de formation ont été organisées en coordination entre RIPE, MENOG et l'ICANN.

J'ai ajouté ici quelques photos de notre séance d'information. Sur la droite, vous avez la première séance, sur la gauche, la deuxième. Ici, on a des photos de notre évènement public. Et nous avons remis des attestations, des certificats, des diplômes pour qu'ils se sentent fiers d'avoir cette connaissance du DNSSEC, nos participants.

Ici, on a quelques livrables attendus. Donc on a une déclaration pratique du DNSSEC. Nous étions les premiers à élaborer ce document, tant en anglais qu'en arabe. Tout est compatible avec la déclaration RFC 6841. Nous avons également travaillé sur la mise en œuvre de beaucoup de procédures que nous avons développées pour la gestion du DNSSEC, pour la cérémonie de signature de clés, pour l'installation de clés, pour développer de nouvelles mesures de sauvegarde lorsqu'il y a des désastres comme on dit. Et puis si quelqu'un qui gère les mots de passe ou les modèles de matériel avait des problèmes, que ferait-on si cette personne avait un accident ? Ou si on avait des problèmes à un autre niveau, que faire aussi ?

Donc on avait un tableau de gestion de risque qui nous montrait clairement ce qu'il fallait faire. C'est ce que nous avons élaboré nous-même. Puis nous avons publié un site web avec des outils. Tout cela est disponible en arabe et en anglais. Et puis tout est complètement opérationnel. C'est ce que j'ai dit tout à l'heure.

Ici, vous voyez notre infrastructure. Donc sur la droite, on a la salle du DNSSEC où nous faisons les travaux de génération de clés. Tout est sécurisé. Donc le système et les cartes sont gardés dans un coffre à la fin de la cérémonie et personne ne peut quitter la salle, à moins qu'ils aient suivi la procédure spécifique. Nous avons également une salle de backup et puis nous avons deux centres, centre de données 1 et centre de données 2, qui ont des serveurs publics.

Ici, vous avez les procédures de configuration que nous avons élaborées. Nous avons lancé les opérations du DNSSEC en Arabie Saoudite en 2016 et nous avions été le premier pays DCC à habiliter le DNSSEC et nous avons, comme je l'ai dit tout à l'heure, invité les FSI et les fournisseurs de services de données à participer au DNSSEC. Le lancement officiel de .saudia, du .sa et de l'IDN était lancé le 22 juin 2017 et nous avons été le premier pays du Moyen-Orient et de l'Afrique du Nord à ouvrir le service à tous nos clients. Nous avons fait la cérémonie, nous avons publié la zone, nous avons publié la clé publique avec l'IANA, nous avons commencé à signer les ccTLD et l'IDN, nous

avons mis à jour les systèmes d'enregistrement pour nous préparer à la fourniture de services du DNSSEC, nous avons fait des séances de sensibilisation et de promotion, et nous avons également publié un site web qui est le dnssec.sa, qui est disponible en arabe comme en anglais.

Ici, vous avez la carte de déploiement du DNSSEC et vous voyez les pays qui sont opérationnels qui sont en vert. Nous, on est en vert foncé heureusement. Ici, on a des images de la cérémonie de génération de clés. Toutes ces personnes étaient des participants à la cérémonie pour signer. On a également un auditeur, on a des personnes du gouvernement et des experts en DNSSEC qui nous ont accompagnés.

Voici le site web. Vous voyez ici la version en arabe. Il y a des images pour montrer aux personnes que le DNSSEC est facile à comprendre. C'est pourquoi nous diffusons des connaissances en leur propre langue. Ce serait difficile pour eux de le comprendre en anglais. Donc si les personnes ne le comprennent pas en anglais mais qu'ils ont recours à ce site en leur propre langue, ce sera plus facile pour eux de le comprendre.

Ici, vous avez le vérificateur de registre DS. Et donc si vous utilisez des informations là-dessus, vous pourrez vérifier si vous avez une coïncidence ou pas sur le site web. Si vous saisissez vos

informations, l'outil va chercher le registre DS dans la zone racine – dans le fichier de zone – et puis vous allez vérifier que tout est correct.

Nous avions jusqu'à la fin de septembre. À la fin de septembre, nous avions plus de 50 000 noms de domaines et jusqu'à hier, on avait 55 domaines au total : 33 sur le .sa, 8 sur .saudia qui est notre IDN, 6 sur .com.sa, 6 sur le .net.sa, 1 au .org.sa et 1 au gov.sa. Il faut que l'on fasse de notre mieux pour que le .sa soit complètement compatible avec le DNSSEC dès que possible, donc il faut faire davantage d'activités au niveau de la sensibilisation et de la promotion. Donc nous continuerons de travailler. Nous augmenterons nos activités dans l'avenir. Nous allons également faire le suivi de nouvelles améliorations au protocole DNSSEC et aux mises à jour des clés par exemple de DNSSEC. Et il faut également que l'on contrôle les roulements de clés. Celle du ZSK dure six moi. Donc cette clé change tous les six mois. Il faut que l'on suive ces changements.

Les leçons que nous avons tirées que je veux partager avec vous, c'est qu'il faut absolument avoir des connaissances locales et vous devez avoir un laboratoire à essais.

Attendez, on a un petit problème ici dans la salle. Aucun problème.

Donc vous devez lancer un laboratoire de tests pour tester les systèmes, pour faire des tests et permettre la configuration du DNSSEC. Vous devez également faire le suivi des tests, des outils pour le système DNSSEC. Donc vous voyez que ce n'est pas simplement question d'élaborer un fichier de zones et de le publier. Il faut le vérifier avant de le publier, contrôler que les crédentiels soient valides. Il faut ajouter quelques domaines importants et voir quelles sont les priorités pour ne pas publier le fichier s'il y a ces informations qui ne sont pas compatibles. Et puis, il faut voir comment faire l'automatisation, surtout pour la cérémonie de signature de clés. On a beaucoup de marge à erreur humaine donc on ne peut pas dépendre des personnes. Les personnes pourraient avoir du mal à suivre. Et puis, on doit fournir du soutien à la clientèle à l'aide des outils pour valider l'efficacité d'exactitude des clés. Voilà. Nous voilà à la fin.

JACQUES LATOUR : Merci. Y a-t-il des questions ? Oui, moi, j'en ai une.

JOHN LEVINE : C'est vraiment impressionnant. Merci.

Quel est le processus utilisé par rapport les titulaires de noms de domaine pour mettre à jour les clés qui correspondent à leur nom de domaine ?

RAED ALFAYEZ : Ils peuvent voir notre registre et puis mettre à jour leur DNSSEC.

JOHN LAPRISE : Est-ce qu'il y a des API ou c'est manuel ?

RAED ALFAYEZ : Non, c'est manuel. Vous complétez tout et puis...

JOHN LEVINE: Non mais attendez. Moi, ce que je veux savoir, si je suis un titulaire de nom de domaine avec 20 noms, est-ce qu'il faut que je saisisse chaque nom individuellement ?

RAED ALFAYEZ : Oui.

JACQUES LATOUR : C'était la même question que j'avais à poser.

Y a-t-il d'autres questions ? Russ ?

RUSS MUNDY : Voilà. Merci de cette présentation. Le travail que vous avez fait est véritablement impressionnant.

Je sais que vous êtes censé présenter le DNSSEC ici mais je voulais savoir si vous avez vu des procédures de gestion de risque similaires et si vous avez considéré la démarche pour les contenus lorsque les titulaires de noms de domaine fournissent des informations pour le registre des DNS par exemple. Est-ce que vous avez des processus de procédures similaires pour gérer les contenus de fichiers de zone eux-mêmes ? Parce que c'est en fait ça ce que fait le DNSSEC ; c'est de conserver, de protéger les contenus de la zone. Donc je voudrais savoir si vous avez également évalué ce type d'activités pour les contenus qui sont publiés dans la zone.

RAED ALFAYEZ : Si quelqu'un voulait mettre à jour leur registre DS, notre système vérifierait que le DS corresponde à la clé de la zone. C'est la seule vérification que nous faisons. Nous allons leur envoyer une alerte si ce n'est pas compatible. Si les personnes ignorent cet avis qui dit « Votre fichier de zone ne sera pas correct. », peut-être que les personnes ne vont pas pouvoir rejoindre votre nom de domaine si vous avez des données qui ne sont pas les bonnes. Et dans l'avenir, il se pourrait qu'on vérifie si les signatures sont ou pas valides mais ce n'est pas fait à l'heure actuelle.

J'espère avoir répondu à vos questions.

RUSS MUNDY : Oui, à peu près. Mais je sais qu'il faut avancer. J'ai d'autres questions à vous poser plus tard.

JULIE HEDLUND : Nous avons une question sur le chat et un commentaire. La question... Pardon, je ne sais plus où elle est. La question a été envoyée par Zainab Al Farsi qui demande : « Quels sont les défis auxquels vous êtes confrontés ? »

RAED ALFAYEZ : Le plus difficile, c'est de créer une équipe, de former des spécialistes en DNSSEC, de trouver des spécialistes même. C'était ça l'obstacle principale pour nous parce qu'on avait l'outil, tout y était. Mais il fallait lire les RFC et comprendre qu'est-ce que c'était ce dont on avait besoin. Au moment de créer des équipes, il faut comprendre les différents temps, les différents paramètres du DNSSEC parce qu'ils sont liés entre eux. Et nous consacrons quatre mois à déchiffrer, par exemple, que les clés TTL sont liées avec d'autres paramètre puis qu'il y a un deuxième paramètre qui est lié à un troisième. Donc cela aurait été plus facile si quelqu'un avait établi la relation entre les différents paramètres du DNSSEC, comme une formule que si on met DS3, alors il va falloir doubler le TLL et puis qu'il faudrait

qu'on ait le triple sur une autre valeur. Ce serait plus simple si on avait cela comme une formule. On l'a maintenant, on espère pouvoir faire quelque chose qui soit utile pour aider les autres aussi. Mais le défi principal pour nous, c'était de trouver des experts au niveau local.

JULIE HEDLUND : On a reçu un commentaire d'Abdalmonem Galila : « Merci Raed d'avoir maintenu cette identité arabe. Vous avez utilisé la langue arabe sur votre présentation, et merci de pouvoir faire la sensibilisation à travers votre propre langue maternelle. »

JACQUES LATOUR : Merci.

Maintenant, nous avons Kadir Erdogan de la Turquie qui va nous parler des activités du DNSSEC en Turquie.

KADIR ERDOGAN : Bonjour. J'attends mes diapositives. On ne voit pas très bien mais peu importe. On ne voit pas bien. Je m'appelle Kadir Erdogan. Je représente .tr, je suis le gérant technique de ce ccTLD. Alors je viens de la Turquie et je vous donnerai une présentation rapide sur les activités au niveau du DNSSEC en

Turquie. Comme vous le voyez, notre pays est très coloré. Il faudrait que vous le visitiez si vous n'y êtes jamais allé.

La Turquie est l'un des pays les plus conscients du DNSSEC. Est-ce qu'il y a quelqu'un qui ne sait pas ce qu'est 8.8.8.8 ? Comme vous voyez, cette configuration a été écrite sur un graffiti dans un appartement. Cette photo a été prise il y a quelques années lorsque le gouvernement s'occupait de faire le filtrage de DNS pour les réseaux sociaux. Et tout le monde a appris à configurer leur DNS.

Je sais que nous sommes là pour faire des présentations de DNSSEC mais en Turquie, il n'y a pas de FSI qui signe ou qui valide le DNSSEC, donc il est très important pour nous de travailler sur les DNS. Et le gouvernement nous a aidé à ce niveau-là parce que grâce à eux, à la censure, les personnes connaissent le DNS.

Je partage avec vous une petite histoire de nic.tr, notre ccTLD. On a établi la première connexion internet à l'Université technique du Moyen-Orient en 1991. En 1995, on a monétisé le .tr. En 1998, nous avons créé le groupe de travail du DNS. Il s'agit d'un modèle de gouvernance multipartite précoce. C'est le modèle que l'on suivait. On avait différents acteurs qui partageaient le besoin de sentir cette nécessité de réglementation. En 2003, on a vu l'automatisation du web pour

des applications, pour faire des paiements, pour traiter des documents, etc. En 2006, nous avons mis en œuvre des IDN. Nous avons six lettres qui ne sont pas des caractères ASCII, donc c'était facile pour nous. Ce n'est pas comme dans le cas de l'arabe. En 2008, nous avons mis en œuvre un système d'opérateurs de registre et de bureaux d'enregistrement. Ce n'est pas EPP, c'était un système API. Et en 2010, le gouvernement a publié des statuts constitutifs. Il y a eu un conflit entre le ministre des transports et des communications et nic.tr. Nous sommes toujours en train de négocier avec eux.

Alors par rapport au DNSSEC en Turquie, personne ne sait ce que c'est et cela n'intéresse personne. C'est un peu un cliché mais nous ne sommes pas personne. Nous travaillons beaucoup, il y a beaucoup de personnes qui travaillent.

Alors l'état des lieux actuel, malheureusement, le .tr n'est pas signé pour l'instant. Les grands opérateurs ne valident aucun, et aucun des opérateurs en fait ; je ne pense pas que ce soit que les grands opérateurs qui ne valident pas. Par conséquent, nous n'avons pas de problème de roulement de KSK en Turquie. Et les décideurs, donc, ne sont pas au courant du DNSSEC.

Pourtant, on a des aspects positifs. Nous voulons signer le ccTLD. La communauté technique en discute. Nous recevons d'ailleurs quelques demandes des titulaires des noms de

domaine pour pouvoir signer leur nom de domaine, ce qui est bien. Et nous organisons des séances d'information et des ateliers dans le pays.

Ce que nous avons fait jusqu'à présent, en 2014, nous avons tenu une formation ; c'était le début de nos activités. Cela a été organisé ensemble avec l'ICANN et NSRC. Nous avions, là, différentes personnes qui y ont participé : il y avait des étudiants, des stagiaires. Les formateurs étaient Richard Lamb de l'ICANN et puis un autre de NSRC. En 2016, en mars, nous avons tenu un atelier à Istanbul. Cet atelier a été organisé à l'aide de RIPE. Et encore une fois, moi-même, j'ai été formateur au nom de nic.tr. L'ICANN nous a encore envoyé Richard Lamb. En 2016, on a tenu un nouvel atelier national. Ce sont des ateliers de cinq jours. Ce sont des formations très complexes, très techniques et elles ne sont pas faciles à organiser. Il n'est pas facile de trouver des personnes pour faire la formation parce que le DNSSEC est un sujet très étroit et les personnes ne connaissent pas cela à la profondeur suffisante. Nous avons organisé un autre atelier en 2017. Il s'agissait du forum du DNS de la Turquie. C'était le troisième. C'était un atelier de quatre jours. Vous voyez ici des photos de cet atelier. Et vous voyez ici Rick qui donne le cours, qui participe donc comme formateur.

Alors qui est-ce que nous avons formés ? Jusqu'à maintenant, nous avons formé une cinquantaine de techniciens. La plupart

sont responsables du DNS dans des organisations. Vingt d'entre aux appartenaient aux gouvernements, aux ministères, à l'armée, 10 à des universités, 10 à des bureaux d'enregistrement et 10 à des opérateurs de réseaux. Comme je l'ai dit, c'est très difficile d'identifier en général les personnes que nous formons mais nous avons un bon groupe.

Nous devons organiser davantage de formations parce que le DNSSEC est un point important et il faut être formé. Donc on a besoin de davantage d'experts, d'ateliers, et on a besoin de commentaires. Je dis commentaires parce qu'on a besoin de former des gens qui s'y connaissent. Et si on parle de manière trop technique, les gens ne comprennent pas. Donc je pense que finalement, les commentaires seraient un bon système.

Alors qu'est-ce qu'il nous attend dans le futur ? Nous allons le signer. Merci. C'était ma voix.

JACQUES LATOUR : Merci beaucoup. Est-ce qu'il y a des questions pour Kadir ?

CHRISTIAN : Je suis Christian. J'appartiens au registre pour les Pays-Bas. Qu'en pensez-vous : est-ce que le DNSSEC va commencer ? Est-ce que vous pensez que ça va commencer au niveau des registres ?

KADIR ERDOGAN : Je pense que ça va commencer par le ccTLD. Nous allons devoir le signer d'abord.

CHRISTIAN : Nous avons commencé la même façon. Il faut commencer à un moment donné et nous avons commencé au niveau des registres.

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

JEFF HOUSTON : J'ai remarqué que l'utilisation du DNS public de Google avait diminué en Turquie de 7 %. Est-ce que c'est parce que vous avez arrêté d'utiliser Google ou est-ce que c'est parce que votre fournisseur ISP, votre ISP, a cessé de l'utiliser ?

KADIR ERDOGAN : Je n'ai pas de réponse mais je peux vous dire ce que j'en pense. Je pense qu'on est en train d'intercepter certaines choses. Le gouvernement est en train d'intercepter certaines choses. Je ne sais pas lesquelles.

JEFF HOUSTON : Est-ce que l'on peut essayer de prévenir cela d'une certaine façon pour résoudre ce problème ?

KADIR ERDOGAN : Je ne sais pas quoi vous dire.

JACQUES LATOUR : D'autres questions ?

Notre prochain intervenant est Rajiv Kumar. Le registre de .in, la mise à jour du DNSSEC dans le registre de .in.

RAJIV KUMAR : Bonjour à tous. Je suis Rajiv Kumar. C'est une bonne occasion pour moi de vous faire une mise à jour sur ce qu'il se passe au niveau du DNSSEC en Inde.

Mon ordre du jour va être donc : présentation du DNSSEC et du registre .in ; participation des bureaux d'enregistrement ; efforts des registres ; et ressources pour les bureaux d'enregistrement.

Donc .in, ce registre, quelqu'un a adopté de manière précoce ce DNSSEC ; .in a été signé en novembre 2010. Dans ce programme, nous avons un programme dans lequel nous permettons aux FSI, aux bureaux d'enregistrement, d'utiliser ce système dans leur environnement de façon à ce qu'ils le connaissent. En 2011, le DNSSEC a été introduit dans l'environnement de tests. Nous

avons testé les bureaux d'enregistrement, testé l'environnement et cela a permis de signer ces enregistrements. En novembre 2011, nous avons accepté les enregistrements DS.

Et la participation des bureaux d'enregistrement : nous avons 121 bureaux d'enregistrement accrédités sur lesquels 39 utilisent le DNSSEC, y compris 10 bureaux d'enregistrement pour le registre. Ils offrent des services DNS aux bureaux d'enregistrement. Nous avons 2 millions de noms de domaines enregistrés parmi lesquels 1287 sont signés. Donc je parle de date, à partir de septembre 2017.

Nous avons une série de bureaux d'enregistrement que nous encourageons à déployer le DNSSEC et pour cela, nous faisons des réunions présentielles. Nous faisons des présentations pour eux, nous organisons des formations, des ateliers, des programmes pour la communauté technique, pour les FSI, pour les bureaux d'enregistrement avec l'aide d'ICANN et de APNIC, et nous organisons donc ce type d'ateliers. Nous avons organisé un atelier de cinq jours par exemple. Il y a des ressources pour les bureaux d'enregistrement qui sont disponibles sur notre site internet. Ici, vous avez le lien. Nous faisons aussi de la mise à jour de clients EPP pour déployer les commandes du DNSSEC.

En ce qui concerne la partie de la validation, nous avons fait des recherches et nous avons partagé certaines données avec des

chercheurs. Ces résultats sont : nous avons 34 serveurs de noms qui peuvent valider le DNSSEC ; nous avons 144 serveurs de noms qui connaissent le DNSSEC mais qui ne le valident pas ; nous avons 299 serveurs de noms qui ne mettent pas en œuvre le DNSSEC. Et nous prenons aussi en charge certains noms de domaine internationaux qui ont été signés.

Je vous remercie

JACQUES LATOUR : Merci.

Est-ce qu'il y a des question ? Russ, allez-y.

RUSS MUNDY : Je vous remercie pour votre présentation.

Je serais curieux, si on pouvait revenir à la diapositive de validation s'il vous plaît. Je voudrais vous demander comment est-ce que vous identifiez les chiffres de validation ?

RAJIV KUMAR : Notre université a mis en place ce type de recherches auprès de la communauté en Inde et ils ont fourni donc le statut de validateur de DNS.

JACQUES LATOUR : Donc vous pensez qu'il y a davantage de résolveurs ouverts ?

RAJIV KUMAR : C'est possible, c'est possible. Je vais demander au responsable de cette recherche à l'université, et je vous donnerai la réponse.

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

RUSS MUNDY : Je crois qu'il y a une question en ligne.

JULIE HEDLUND : Il y a une question que l'on attend en ligne. Et on me dit qu'il y a une personne qui n'a pas pu venir ici mais qu'il va faire sa présentation qui a été enregistrée en vidéo. Donc cette personne sera ici de manière virtuelle mais cette personne viendra plus tard pour répondre à vos questions.

RAJIV KUMAR : Je n'ai pas vraiment compris ce que vous disiez.

ABDAMMONEM GALILA : Je suis le gestionnaire de ccTLD de IDN. Je suis un boursier d'ICANN et j'appartiens aussi au nom de domaine... au groupe

de travail sur le nom de domaine. Je vais vous faire une présentation sur les défis que nous avons eus pour déployer le DNSSEC. Et je suis Abdalmonem Galila. Je vais vous parler aussi de la période après le déploiement et je vous parlerai aussi des scripts de DNSSEC.

Nous utilisons des systèmes de signatures. Nous déployons le DNSSEC pour plusieurs ccTLD et avant le déploiement du DNSSEC, nous n'avions aucune idée de ce que c'était le DNSSEC. Je pense qu'il est important de savoir ce que c'est que le DNSSEC et de savoir comment il fonctionne. Nous avons entendu parlé du DNSSEC à Djibouti en 2014 lors d'un forum internet et nous avons commencé à réfléchir à ce qu'était le DNSSEC et nous avons voulu savoir qu'est-ce que c'était que le DNSSEC, obtenir des informations.

Nous avons assisté à l'atelier du DNSSEC. Nous avions un premier environnement et ensuite, nous avons utilisé ce système pour le tester. Nous avions un système avec le registre, une base de données, un système WHOIS. Nous voulions des informations sur la façon dont le DNSSEC va fonctionner. Donc nous avons dû avoir un système de résolveur qui nous a permis de tester notre environnement. Nous avons fait cela et nous avons obtenu les informations requises pour commencer le déploiement du DNSSEC dans notre environnement de production.

Et lors de notre environnement de tests, nous avons signé et nous avons eu notre propre version des registres qui étaient d'accord pour utiliser ce DNSSEC pour les domaines enfants. Pour les interfaces de registre, nous avons utilisé un logiciel de registre qui s'appelle CoCCA et nous pensons que cela a bien fonctionné. Un de nos systèmes de tests des serveurs DNSSEC a été reporté de plusieurs minutes et nous avons dû adapter notre système, et nous avons construit un serveur de temps et nous avons rendu notre serveur client de cet autre serveur. Nous avons une communication entre le serveur de DNS maître-esclave. Donc nous avons utilisé des signatures de transaction pour répondre à ce problème dans notre environnement de tests, et nous avons essayé de mieux comprendre les problèmes qui pouvaient surgir dans le DNSSEC avant d'entrer en ligne avec le DNSSEC. Après le test, nous avons voulu reprendre, refaire ce que nous avions fait dans notre environnement et l'appliquer à notre environnement de production.

Nous avons dû reconfigurer cela pendant 15 minutes. La plupart des problèmes que nous avions eus étaient liés aux protections. Donc assurez-vous de travailler avec votre réseau et votre administrateur de sécurité de façon à ce qu'ils puissent changer leurs prérequis avant de déployer le DNSSEC et modifier les pare-feux.

Il y a deux types de problèmes de pare-feu qui sont les plus courants. Le premier comprend le TCP, le protocole de contrôle de transmission. Il y a une mauvaise compréhension concernant les pare-feux et les administrateurs de sécurité à ce propos. L'UDP, le protocole d'utilisateur... parce que nous utilisons l'UDP et hélas, on pense cela mais ce n'est pas tout à fait exact. Donc on est revenu au TCP si cela n'est pas reçu lorsqu'il y a une requête ou lorsque certaines informations importantes sont coupées.

Donc la possibilité d'avoir quelque chose qui bloque sur le passage et qui bloque la demande ou la requête initiale fait que pour le DNSSEC, pour que le DNSSEC fonctionne correctement, vous devez ouvrir votre pare-feu ; c'est obligatoire. Et vous devez ouvrir votre pare-feu pour les TCP ou pour les UDP, dans les deux cas pour 53.

Le deuxième type de problème concerne la taille d'assemblée. Les autres normes de DNSSEC ont constaté que ce type de problème pouvait arriver et le TCP s'occupe de ce type de problème sur les serveurs DNS. Et de façon à éviter d'avoir trop de trafic TCP, on a un système d'EDNS(0) qui fonctionne avec le DNSSEC. Ce EDNS(0) est un mécanisme d'extension pour le DNSSEC et un système qui permet de signaler qu'il peut recevoir cela sur l'UDP. Ils sont plus grands que les limites préalables de 500 et quelques bits. Certains pare-feux ne savent pas que le

EDNS(0) et les normes du EDNS(0) permettent d'avoir des paquets plus grands, de plus grandes tailles, et que ces paquets EDNS peuvent utiliser EDNS(0) ou bloquer des paquets qui sont plus grands que 515 bits, sans tenir compte du fait qu'EDNS(0) le signale. D'autres pare-feux permettent d'avoir des paquets plus grands par défaut et plusieurs fournisseurs requièrent à ces pare-feux d'être configurés manuellement. Pour ce faire, il faut savoir que l'EDNS(0) et les normes de l'EDNS(0) existent pour pouvoir prendre des décisions correctes concernant la possibilité de retransmettre ces paquets.

Vous devez aussi tester cela et il y a une source externe qui peut recevoir des réponses DNS plus grandes que votre serveur DNS envoie. Et une façon de faire cela, est d'utiliser le résolveur de DNSSEC ouvert. Et donc vous devez tester et configurer votre pare-feu pour vous permettre d'utiliser l'EDNS(0) et les paquets d'EDNS qui sont plus grands que 515 bytes UDP. Et nous demandons aussi des contacts d'administration pour soumettre tout cela à ICANN pour vérifier tout cela et ajouter ces données dans la zone racine.

Prochaine diapo. Après le déploiement de DNSSEC, il faut savoir comment conserver notre système en ligne en permanence sans problème de signature. Donc nous avons fait un script pour la resignature de la zone après la génération d'une nouvelle zone par le système de registre, qui soit capable de contrôle tout cela.

Le DNSSEC introduit aussi de nouvelles tâches opérationnelles, comme par exemple le roulement de clés. Et cette tâche doit être réalisée de manière régulière. Et nous n'avons pas fait de roulement de clés jusqu'à maintenant mais nous allons le faire cette année. Et de nouveau, vous devez préparer votre pare-feu pour DNSSEC. Je le répète, la plupart de problèmes du DNSSEC sont liés au pare-feu donc faites attention. Vous devez vous assurez que vous en avez parlé à votre système de sécurité, à vos administrateurs.

Notre mission maintenant est de parler du DNSSEC à nos bureaux d'enregistrement locaux. E t nous avons aussi constaté que certains serveurs DNS ne répondent pas aux requêtes CB. Et les problèmes que nous constatons répondent à un excès de taille de 1500. Et le DNSSEC introduit aussi de nouvelles tâches opérationnelles qui peuvent faire que cette taille soit supérieure. La plupart de nos FSI n'ont pas de validation de DNSSEC, donc même si c'est seulement une ligne de configuration. Prochaine diapositive.

En tant que bureaux d'enregistrement, la plupart de nos bureaux d'enregistrement sont des FSI. Alors nos clients n'ont aucune idée du DNSSEC, ils ne savent pas comment le faire et ils ont la sensation que leurs systèmes sont stables. Donc il n'y a pas besoins de changer leurs systèmes actuels parce qu'ils semblent stables.

Alors la résolution des noms de domaine, il semble, prendra plus de temps pour les bureaux d'enregistrement. Les noms de domaine qui ont des signatures invalides seront bloqués. Ils auront toujours des attaques mais ils pourront les mitiger s'ils mettent en œuvre le DNSSEC. À certaines phases, les bureaux d'enregistrement n'ont pas la capacité d'envoyer des registres au DNSSEC au système, et ils n'ont pas suffisamment de personnel pour faire le suivi et [inintelligible] du DNSSEC.

Maintenant, je vais vous montrer la structure des signatures en vrac et le script d'automatisation de la signature de la zone DNSSEC. Ce script était développé pour la zone numéro 5 et il était également conçu pour pouvoir gérer la signature DNSSEC. Alors la structure des scripts commence par des variables qui sont initialisées tel que la directive des fichiers de zones pour les registres qui sont générés.

INTERPRÈTE : Nos excuses, la cabine ne reçoit pas de son.

JACQUES LATOUR : Voilà, c'est la fin. Merci. Y a-t-il des questions ?

Autrement, on est juste à l'heure pour la pause. On se voit d'ici 15 minutes.

JULIE HEDLUND : Je savais d'Abdalmonem voulait venir pour les questions et réponses. Je ne sais pas s'il est là... Ah ! Il est là si vous avez des questions.

INTERPRÈTE : L'intervenant est en train de parler sans microphone. L'interprète s'excuse.

ABDALMONEM GALILA : Alors notre script commence par la saisie de certaines informations dans le fichier de zones. Puis on génère, à travers un processus automatisé, le script. On vérifie les nouveaux fichiers de zone pour voir si tout est correctement généré pour appliquer les informations du DNSSEC. Après, nous décompressons les zones générées par le registre. Donc si vous avez beaucoup de zones que vous voulez signer à l'aide du DNSSEC avec notre script, c'est acceptable. Puis, les zones sont signées et après tout cela, nous utilisons notre redémarrage RNDC au cas où vous voudriez relancer, si vous avez beaucoup de noms de domaine comme registres ne recommandant pas d'utiliser le système actuel. Nous n'avons que 800 noms de domaine IDN, c'est pour cela que nous les utilisions.

Ici, vous voyez des captures d'écran de notre script d'automatisation qui commence par certaines variables, comme vous voyez, qui sont automatiquement générées. Puis on voit ici le fichier de zones qui est automatisé ou pas. Puis on cherche dans la zone – si on a plusieurs zones, dans les zones – comment faire la signature DNSSEC, voir si elles ont été signées et puis voilà. C'est tout. Merci.

JACQUES LATOUR : Merci. Y a-t-il des questions ? Oui ?

RAED ALFAYEZ : Merci Abdalmonem par cette présentation que vous avez faite en deux parties, à distance et en personnes.

Je voudrais savoir si vous avez commencé à accepter des registres DNSSEC pour vos clients et si vous avez des outils pour valider leur DS ou pas.

ABDALMONEM GALILA : Nous acceptons des registres DS de nos bureaux d'enregistrement, mais le problème est que les bureaux d'enregistrement ne connaissent pas bien le DNSSEC. C'est pareil pour nos clients. Nous sommes un opérateur de registres, pas un bureau d'enregistrement, donc nous acceptons les

registres des bureaux d'enregistrement. On n'a que huit qui ont signé le DNSSEC. Merci.

JACQUES LATOUR : Merci. Y a-t-il d'autres questions ? Très.

Dans ce cas là alors, on est officiellement en pause. On reprend à 10:30, d'accord ?

[FIN DE LA TRANSCRIPTION]