BARCELONE – Atelier sur les DNSSEC - (1 sur 3)
Mercredi 24 octobre 2018 – 09h00 à 10h15 CEST
ICANN63 | Barcelone, Espagne

RUSS MUNDY: Bonjour à tous. Il n'est pas tout à fait 9 heures, mais nous avons un panel assez nombreux. J'ai essayé de parler à tout le monde à l'entrée de la salle, mais il est possible que j'ai raté quelqu'un parce que nous avons beaucoup de personnes à ce panel.

Donc s'il y a des personnes qui font partie du premier panel et que je n'ai pas encore salué, et bien il reste des places à la table. Et donc c'est là que nous vous demandons de prendre place.

Nous allons commencer dans un petit instant, mais avant que nous ne commencions, et je le répèterai, vous voyez le déjeuner ici, ce n'est pas pour vous. Notre déjeuner sera en haut. Donc il faudra prendre deux escalators, parce que ça, ce repas qui sera préparé au déjeuner, ce sera pour un autre groupe. Il nous faudra donc sortir de la salle au moment du déjeuner.

Alors, voyons, voyons... Alors Steve est avec nous au téléphone. Bonjour Steve, ici Russ, tu es avec nous dans la salle.

Il est désormais 9 h, et je pense que pratiquement tout le monde est là. Nous avons 9 personnes pour ce premier panel.

Je suis Russ Mondy, je souhaite souhaiter la bienvenue à vous tous qui êtes présents pour cet atelier DNSSEC à l'ICANN 63. Nous avons beaucoup de choses à faire aujourd'hui.

Je ne vais pas m'étendre pour l'introduction, je voudrais simplement vous redire que le déjeuner qui est là à côté n'est pas pour nous, nous allons monter en haut. Nous avons une salle de banquet qui est très sympathique de toute façon. Nous devrons tous quitter la salle à midi pour le déjeuner et revenir ensuite ;

Alors, ceci étant nous allons commencer. Ma première personne qui va faire la présentation c'est Erwin Lansing. Et je ne sais pas comment prononcer son nom de famille.

ERWIN LANSING: Très bien. Bonjour à tous. Erwin Lansing au micro.

Alors, tout d'abord, est-ce que vous avez tous poussé un soupir de soulagement ? Oui ?

Très bien, on a roulé la clef et l'internet ne s'est pas arrêté de fonctionner, nous n'avons pas cassé l'internet.

Alors pour aujourd'hui, c'est bon, tout le monde est prêt ? Levez la main si vous êtes prêts, oui. Ceux qui font partie du comité et du programme ? Oui, c'est vous ? Très bien.

Alors je remercie tous les sponsors pour le repas : Affilias, SIDN, CIRA, merci beaucoup.

Ensuite.

Alors cet atelier est organisé par le SSAC et par l'Internet Societéy Deploy360. Mais je suis là pour les représenter. Diapositive suivante.

Alors, nous avons pas mal de choses à faire, n'est-ce pas ? Alors, passons à la suite.

Et ensuite beaucoup de chiffres, et je vous donnerai des chiffres sur le Danemark tout à l'heure, mais voilà les chiffres pour le monde. Donc ceci est basé sur le travail de Jeff pour APNIC. Il a collecté des statistiques DNSSEC pour Google Up et donc nous voyons une petite augmentation toujours, 14 % à peu près pour le monde entier. Il faudrait que ce soit plus élevé, n'est-ce pas ?

Ensuite, donc les régions. Vous en voyez un certain nombre. J'utilise Google beaucoup, parce qu'il y a le résolveur ouvert qui fait sa validation de DNS. Donc premièrement Micronésie à 62 %. Les statistiques Google, donc avec le soutien des FSI.

Diapositive suivante.

Donc voilà certains des chiffres sur les domaines signés.

Est-ce que Christian c'est juste ça ? 62 000 ? C'est ça pour les Pays-Bas ? 62240, de domaines signés, c'est ça ?

Alors je ne sais pas comment on a fait pour collecter ces chiffres, mais... Le .COM est le premier, le .SE numéro 2, ensuite .NU, .NL, .CZ.

Je me demandais pourquoi on avait ce chiffre pour la Hollande. Il me semblait que c'était plus élevé.

Ensuite, donc en ce qui concerne les TLD, en tout cas les ccTLD qui sont signés, le programme DEPLOY360 fait beaucoup de travail pour le WHOIS signé sur les 5 niveaux. Donc une expérience... Donc il va falloir avancer.

En bleu la zone signée, mais le DS n'est pas dans la racine, donc ça veut dire que la validation ne fonctionne pas encore.

Ensuite en vert, le DS est dans la racine, mais n'accepte pas les enregistrements DS encore.

Et ensuite, opérationnel avec acceptation de délégation signée.

Le monde entier qui donc devient de plus en plus vert, donc c'est très bien. Il y a quelques points compliqués... Ha.

Ensuite on a l'Afrique, normalement sur la diapositive suivante. Donc pas beaucoup de signature, c'est assez blanc mais on continue d'avancer.

Voilà.

Donc en Afrique du Sud ça va bien. Enfin dans le sud de l'Afrique ça va bien, mais au centre, ce n'est pas génial.

Ensuite, l'Asie de plus en plus vert. Encore quelques zones en attente u Moyen-Orient principalement.

Pratiquement tout vert, bravo pour l'Europe. La Biélorussie et l'Italie sont opérationnelles apparemment.

Ensuite, l'Amérique latine, c'est pas mal, ça avance.

Ensuite, le Groenland, ça avance.

Les TLD en Amérique du Nord c'est bien.

Donc ces cartes sont mises à jour toutes les semaines. Et vous pouvez avoir davantage d'informations sur ce lien.

Voilà, je crois que c'est la dernière diapositive. Voilà le rapport. Nous l'avons programmé en 2016, il est un petit peu ancien, mais il y a quand même des chiffres intéressants, donc vous pouvez aller le consulter.

Et ensuite... Ceci étant je vais passer la parole au panel.

RUSS MONDY: Étant donné que nous avons beaucoup de monde au panel, nous allons prendre les questions après la partie des cartes, comme nous le faisons... Nous n'allons pas prendre les questions maintenant, nous le ferons un petit peu plus tard. Mais merci pour cette présentation.

Nous allons directement passer maintenant à notre panel. Et notre premier intervenant, c'est justement Erwin, qui va nous parler de ce qu'il se passe au Danemark, dans le point DK.

ERWIN LANSING: Le .DK. Alors vous voyez, ça a l'air de marcher, mais en fait je n'ai pas toute la diapo.

Alors voilà les chiffres pour le .DK. Donc augmentation lente, 24 000 domaines signés. Je crois que c'est 2 % pratiquement. Nous allons convaincre nos bureaux d'enregistrement d'avancer, de continuer de signer.

Alors, pour ce qui est en bleu, algorithmes 13, ce qui est intéressant parce que je pense que les gens pensent utiliser le 8, mais beaucoup des bureaux d'enregistrement, de plus en plus, utilisent cet algorithme. Et je pense que c'est bien.

Alors, en jaune, quelques domaines signés avec le 5, me semble-t-il.

En ce qui concerne la validation, donc 14 %. Le Danemark se débrouille très, très bien, avec 64 %. Donc 4 sur 5 FSI. Ca c'est basé sur les chiffres d'APNIC.

Dernière diapositive, nos objectifs pour l'avenir. Nous avons un système unique où tous les serveurs de noms doivent être enregistrés dans le registre, donc tous les opérateurs de noms doivent être inscrits dans notre registre, ce qui leur permet de mettre à jour directement par l'opérateur de serveurs de noms.

Nous avons un fournisseur depuis 2010. Nous avons signé pour la première fois juste après la racine.

En bas, vous avez une commande avec des informations clefs pour automatiser les signatures de clef. Ou alors vous pouvez utiliser une interface ERP.

Nous avons CDS/CDNSKEY. En ce qui concerne la zone, le nombre d'enregistrements CDS avec publication, CDS/CDNSKEY donc nous n'avons que 1218 pour le CDNSKEY et 1256 pour le CDS.

Donc à l'avenir, la signature devrait être plus facile pour les opérateurs.

Voilà mes chiffres pour le .DK.

RUSS MONDY: Merci beaucoup. Nous apprécions énormément ces informations. Ensuite, nous allons passer la parole à Michael Hausding, du .CH, de SWITCH.

MICHAEL HAUSDING: Alors je vais vous parler un petit peu des chiffres, de ce que nous faisons pour promouvoir le DNSSEC.

Diapositive suivante.

Alors, le nombre de domaines signés. Aujourd'hui nous avons 57 000 noms de domaines CH signés, donc 3 % pratiquement. Donc là vous avez un diagramme. Nous avons également publié ces informations sur notre site web il y a un an.

En 2017, vous voyez qu'il y a une augmentation de domaines signés avec le DNSSEC. La raison c'est qu'un des bureaux d'enregistrement signe par défaut. Si le domaine est enregistré, vous voyez donc une petite partie plate, ou un plateau en haut, c'est parce qu'en fait il a oublié de changer, il a effectué certains changements et il n'y avait pas de bouton pour mettre en marche et à l'arrêt donc il a effectué des changements et il a oublié de signer ces domaines. Et donc il s'en est rendu compte et il a remis le système en marche.

Nous pensons que les chiffres sont importants et voilà pourquoi nous publions ce qu'on appelle le .CH, donc tableau de bord de résilience du .CH. Nous avons fait ceci avec Hardenize. Il y a un nouveau projet qui s'appelle Hardenize où ils mesurent les normes de sécurité standardisées.

Donc nous avons pris les 1000 premiers domaines .CH à Hardenize, et nous avons fait un tableau de bord pour indiquer quel est le niveau de sécurité de ces domaines. Donc 91 % des HTPS, STARTTLS, c'est pas mal non plus. Si vous voyez la diapositive suivante, par contre, vous voyez que le DNSSEC n'a que 3 % dans les 1000 premiers .CH.

Mais c'est important de mettre ceci de manière visible pour que les gens voient un petit peu où ils en sont ;

Ensuite, nous essayons de promouvoir le DNSSEC. Cette année nous avons une formation DNSSEC. Au début nous avions prévu 3 formations DNSSEC, donc trois d'une journée où on apprenait les bases. En 24 heures ces formations étaient pleines. Donc il a fallu en

organiser d'autres. Donc ça a très bien marché, les bureaux d'enregistrement étaient très intéressés.

Ensuite, formation DNSSEC, très bien.

Nous avons également donné un prix DNSSEC aux bureaux d'enregistrement qui avaient effectué la signature par défaut. Donc Infomaniak qui est dans la partie française de la Suisse, c'est lui qui a gagné le prix. Ils ont 38 000 domaines signés sur plus de 60 000, donc ça fait plus de 60 %.

Nous avons commencé le CDS au début du mois d'octobre. C'est en option jusqu'à la fin de 2018. Et ensuite ce sera pour tout le monde. Nous avons le premier bureau d'enregistrement qui a choisi de le faire. Et actuellement nous avons signé 27 domaines, demain je crois avec CDS.

Et je vous donnerais davantage d'informations là-dessus plus tard.

Ensuite, nous avons un roulement d'algorithme, un roulement de clef annuel de 8 à 13.

Nous sommes très heureux que le gouvernement fédéral a signé le domaine qu'il utilise, donc le ADMIN.CH. C'était prévu depuis des années. Et heureusement, en janvier, il y a eu une question au parlement, et on s'est dit si le gouvernement utilise le DNSSEC – en fait le ministre ne savait pas ce que c'était – donc ils ne l'ont pas fait, mais petit à petit ils se sont informés et ils ont fini par signer.

RUSS MONDY: Merci beaucoup. J'apprécie. Et notre prochain intervenant est Peter Koch du .DE.

PETER KOCH: Merci beaucoup. Bonjour à tous. C'est moi, ici, Peter Koch. Je vais partager certains chiffres et certains schémas avec vous pour ce qui est des produits DNSSEC.

En ce qui concerne la croissance du DNSSEC, je vais commencer par vous présenter brièvement la taille, le nombre de domaines DNSSEC ne parait pas si impressionnant, 16.2 millions ; nous avons 300 membres, des bureaux d'enregistrement, des revendeurs. Et pour les bureaux, pour envoyer les demandes de DNSSEC, il n'y a pas d'exigence particulière, il n'y a pas non plus de test qui soit exigé.

Les trois premiers bureaux d'enregistrement détiennent 50 % de tous les domaines signés. Il y a une certaine concentration, comme partout. Et, pour ces cas-là, le bureau d'enregistrement est aussi l'opérateur DNS de presque tous ces domaines. Donc ils font tout eux-mêmes.

C'est un modèle qui fonctionne pour les petits bureaux d'enregistrement, comme Michael l'a dit en Suisse.

Comme je l'ai dit, nous travaillons sur les enregistrements de ressources DNSKEY. Nous calculons donc les enregistrements DS aussi.

Nous avons des tests de pré-délégation pour les enregistrements et les bureaux d'enregistrement présentent le matériel clef. Nous présentons également les tests qui couvrent plusieurs validations. Ils ne peuvent pas présenter des clefs qui sont dans la zone, et nous acceptons ceci – pardon excusez-moi c'est un peu tôt ce matin – nous accepterons des clefs qui ne sont pas présentes dans la zone seulement s'il y en a au moins une qui valide complètement l'enregistrement de ressources DS.

Nous avons 100 000, parfois 200 000 domaines qui sont autoritaires dans la zone DS et ils sont signés par leur propre ZSK.

Alors, il est encore un peu tôt le matin, mais il faut parler d'un sujet qui sera présent dans toutes les discussions à cette réunion. Alors, le 25 mai a eu une grande influence. Qu'est-ce qui s'est passé le 25 mai ? Quelqu'un peut me dire ? Quelqu'un a parlé du RGPD ?

Diapo suivante s'il vous plait ? Pouvons-nous changer vers la droite ? Non excusez-moi un petit peu sur la gauche. La diapo précédente s'il vous plait. Encore une. Voilà. Merci.

Bon, bien sûr, rien à voir avec le RGPD. Il y a un changement par rapport au nombre de domaines signés, qui a coïncidé avec le 25 mai. Ils ne se sont pas rendu compte, ils ont effacé la clef pour beaucoup de domaines. Avec l'aide d'un autre bureau d'enregistrement qui s'est rendu compte de cette erreur, nous avons représenté toutes les clefs pour ces domaines - pouvons-nous passer à la diapo suivante – et c'est ce que vous voyez, ce petit changement en mai. Et croyez-moi que c'est le mois de mai, même si on ne le voit pas.

Je montre cela non seulement par curiosité, mais pour vous dire que certains bureaux d'enregistrement ont des processus qui doivent encore être mieux surveillés.

Donc j'ai encore deux diapos à vous montrer.

Si vous regardez le matériel qui a été présenté, nous avons commencé avec 20 000 domaines signés au mois de mars, et maintenant nous avons 100 000 domaines signés. Nous avons donc 25 %¨d'augmentation

Nous allons passer à la diapo suivante.

On parlera d'algorithme... Non pas vraiment. Diapo suivante. Il devrait y en avoir une autre. Oui très bien.

Pour ce qui est des algorithmes prédominants, donc on a le RSASHA256. Vous savez qu'on a 27 % en rouge, mais on a encore ECDSA, encore un petit peu et on a également 1 DSA, parce que les gens le testent encore.

RUSS MONDY: Merci beaucoup Peter. Le prochain orateur c'est Brett Car de Nominet. Brett s'il vous plait.

BRETT CARR: Bonjour à tous.

J'ai la souris... Peut-être que... Voilà très bien.

Quand j'ai parlé avec Jack pour faire une présentation dans ce groupe, on avait dit qu'à Nominet il y a eu beaucoup de présentation de ce type, donc j'ai décidé de faire une chose un petit peu différente. J'espère que vous serez d'accord avec moi.

Alors pas de statistique. Je voulais vous dire comment nous avons un petit peu simplifié le DNS. Une histoire très résumée de ce que nous avons fait dans le passé.

En 2009, nous avons signé le domaine .UK. Vous vous souviendrez que nous avons eu un petit problème en 2011, parce qu'on a commencé à utiliser une clef sans l'avoir pré-publiée auparavant. Et on nous rappelle cet événement toutes les années, parce que cette photo que vous voyez sur l'écran c'était ma photo FaceBook, c'est ma femme qui l'a publiée, au moment où j'essayais de résoudre ce problème qu'on a eu en 2011. Donc voilà, vous me voyez, j'étais plutôt stressé au moment d'essayer de résoudre ce problème.

Nous l'avons résolu en fait, et en 2014 nous avons commencé à signer les gTLD.

Au fil des années, nous avons en 2009 commencé à utiliser SCA6000 pour OPEN DNSSEC, c'était assez fiable. Il y a eu quelques problèmes en 2011, mais nous avons pu l'utiliser sans problème de manière générale. Le problème, ça a été que les prix d'Oracle sont beaucoup montés à l'époque, et cela a représenté une difficulté pour nous au niveau du Open DNSSEC.

Nous croyons que les 6 solutions sont assez complexes. Le matériel était vraiment fiable, mais c'était compliqué à comprendre, c'était assez complexe. C'était compliqué à résoudre quand les choses ne se passaient pas bien. Et donc il a fallu essayer d'avoir toujours un service de soutien pour ces cas.

En 2016, nous avons donc adopté une solution plus simple. Maintenant, nous n'avons plus HSM, toute la signature se fait sur une version VM répliquée géographiquement avec BIND. Nous avons eu quelques problèmes, mais aucun problème majeur. En général, le service de soutien était très fiable là où on a eu des problèmes.

Les clefs sont protégées par une partition chiffrée et un mot de passe long. La moitié de ce mot de passe est donnée à des ingénieurs et l'autre partie à un groupe de sécurité. C'est-à-dire c'est un mot de passe qui est partagé. Et pour pouvoir agir, il faut que ces groupes soient ensemble pour utiliser ce mot de passe. L'officier de sécurité va surveiller ce qui est fait, et l'ingénieur va mettre son mot de passe. L'accès à la machine se fait par XFR et une console, sans aucune intervention externe. Tout est fait avec la console, avec ce mot de passe dont je vous ai parlé, qui est partagé.

Et tous les changements, comme j'ai dit, sont faits par un ingénieur et surveillés par un agent de sécurité.

En 2018, vous voyez ma photo, pas de stress, ma fille a grandi bien entendu, mais j'ai l'air moins stressé.

Merci.

RUSS MONDY: Merci beaucoup Brett, merci de ces informations du Royaume-Uni. Le prochain c'est Patrick Falstrom.

PATRICK FALSTROM: Ce n'est pas .SE, mais ce serait intéressant d'avoir des informations sur la Suède, même si ce n'est pas ce que je vais faire. Je vais les laisser faire. Comme vous le savez, ce n'est pas une présentation de la Suède, mais c'est une présentation à moi. Je n'ai pas de présentation.

Et je pense que ça aurait été bien d'avoir eu des diapos, mais bon, je n'en ai pas.

La première chose que je veux vous dire, c'est que nous étions le premier TLD qui a été signé. Et nous avons fait cela bien avant beaucoup d'autres TLD.

Ce que nous avons pu voir très tôt, qu'une fois qu'on commençait à signer la zone, nous avons poussé la validation, nous poussions beaucoup la validation, et c'est quelque chose que je vous recommande.

En général, pour le déploiement DNSSEC, d'après notre expérience d'il y a 10 ans, cela ne fonctionnait pas, il fallait commencer par la validation.

Aujourd'hui, en fonction des mesures qui ont été prises, nous avons 74.4 % de validation en Suède. Ce n'est pas le meilleur pourcentage du monde, mais c'est déjà mieux que la Norvège et c'est déjà bien pour

nous. C'est zéro point et quelque pour cent de plus que la Norvège et c'est déjà très bien nous. Nous avons ce petit jeu entre les pays scandinaves. Si vous, vous essayez d'attaquer un pays de Scandinavie, je ne vais pas être content, mais entre nous, on a ces petites batailles ;

Quelque chiffre. Pour le moment, il y a 1.77 million de domaines, dont 800 000 sont signés. Si vous avez un peu de mémoire, cela correspond à 1 million qui ne sont pas signés. Cela veut dire que nous avons réussi la validation, mais c'est plus facile de vendre le concept de zone signé quand la validation est déjà en cours.

Nous parlons avec beaucoup de prudence du roulement de la KSK parce qu'on a beaucoup de validations en cours. Mais en même temps, il fallait changer la clef. Mais il n'y a eu aucun problème.

Un autre chiffre qui pourrait être intéressant, nous avons 86 000 domaines IDN.

Ce qui est intéressant et qui se passe en Suède en ce moment, c'est quelque chose qui devait se passer hier, mais qui a été reporté à aujourd'hui, c'est un changement au niveau de la clef de l'algorithme de RSAHA1-NSEC3-SHAI ECDSA Curve. J'ai eu un mail ce matin, je l'ai lu ce matin, que le changement d'algorithme a été reporté à aujourd'hui. Je n'ai pas d'information technique par rapport à la raison pour laquelle cela a été changé.

Il y a deux URL que je vais essayer de partager avec vous, que vous pouvez consulter si vous allez donc... Je vais vous passer ces adresses,

ces URL, pour que vous puissiez en savoir un peu plus sur ce changement d'algorithmes.

Ensuite, en Suède, nous avons cce mec un peu fou qui a décidé de faire faire ce type de t-shirt, comme vous voyez hein. Il a aussi un site web qui dit dnssecipv6.se. et il a une carte où il y a plusieurs pays, des pays scandinaves, et il mesure si les municipalités et les organisations et les entités ont signé leur zone, utilisent IPv6, ont bien établi leur enregistrement de ressource ; C'est un site très, très utile. Et c'est bien quand les hommes politiques n'ont aucune idée, mais que les gens de la technique sont très fiers de participer à ce type d'initiative. On voit, dans ces cartes, qui l'a fait, qui ne l'a pas fait. Et c'est vraiment très utile.

Merci.

RUSS MONDY: Merci beaucoup Patrick. Ensuite nous avons Arianna pour l'Italie, le .IT.

ARIANNA DEL SOLDATO: Bonjour. Alors, il faut que je puisse afficher les diapositives.

Bonjour, Arianna, du registre .IT. Donc nous sommes un registre récemment DNSSEC.

Alors, on ne voit pas bien la diapositive...

Alors, le DNSSEC, pour nous, c'est un processus assez long qui a commencé en 2014 en collaboration avec le registre, le Netnod, pour consolider les connaissances technologiques qui existaient déjà dans le .IT. En 2016, il y a eu un groupe de travail technique conjoint entre les registres et les bureaux d'enregistrement. Ils ont décidé d'adopter ceci à l'interne. Et quelques mois plus tard, en 2016, une plateforme de test a été rendue accessible à tous les bureaux d'enregistrement IT.

Voilà notre plateforme de test. C'est une plateforme qui réplique en fait la plateforme d'enregistrement. Nous avons un test DB spécial avec un serveur test EPP. C'est une autre zone que celle qui est en production. Nous avons également répliqué un test de résolveur avec un serveur esclave que nous utilisons donc pour tester le serveur EPP et pour mettre à jour la base de données.

Alors, nos choix entre les deux possibilités. Nous avons choisi l'interface de données DS. Nous n'avons pas d'interface web pour gérer le serveur DS, mais nous devons gérer le serveur DS par la commande EPP.

Nous avons mis au point un validateur de DNS qui a une interface web, et donc le registre l'utilise avant de signer le nom de domaine, avant d'enregistrer le nom de domaine.

Le DNSSEC, pour nous, n'est pas obligatoire. Mais les bureaux d'enregistrement doivent réussir un test d'accréditation pour pouvoir enregistrer les noms de domaine. Les bureaux d'enregistrement accrédités sont identifiés par un logo spécifique sur notre site web. Ce

logo peut être utilisé par les bureaux d'enregistrement sur leur site, pour montrer qu'ils sont accrédités.

Le test d'accréditation donc, leur permet de s'inscrire pour leur test. Ils reçoivent également certaines spécifications techniques qu'ils utilisent pour réussir le test. Donc le nom du nom de domaine, la machine à utiliser, l'algorithme à utiliser, pour pouvoir signer la zone. Ils doivent enregistrer les noms de domaine et créer une KSK et une ZSK. Et ensuite transmettre l'enregistrement de DS.

Il n'y a pas de délai pour réussir le test, mais chaque test dure 90 minutes. Et en cas d'échec, il faut attendre une semaine avant de faire un deuxième test.

Alors, voilà le statut actuel en 2016. Donc la plateforme de test DNSSEC a été mise à disposition en 2016, ensuite en 2017, nous avons signé la zone IT, donc enregistrement DS dans la racine. Ensuite 2018, publication des nouvelles directives techniques qui comprenaient les spécifications DNSSEC. Et un mois plus tard, en septembre 2018, nous avons ouvert notre test d'accréditation pour les enregistrements. Enfin, en septembre, nous avons eu la première accréditation de bureau d'enregistrement et le premier domaine signé.

Les chiffres actuels. Nous avons actuellement une surprise, puisque nous devons changer ce visage, parce qu'hier, nous sommes passés à 6 bureaux d'enregistrement accrédités, 1384 domaines signés. Donc en un jour, le bureau d'enregistrement nous a envoyé ceci ; donc plus de 1300 domaines signés.

Nous avons organisé un cours de formation dans le contexte de ce que nous avions fait pour les bureaux d'enregistrement et dans le contexte également du cours de cybersécurité organisé par le département ingénierie de l'université de Pise.

Merci.

RUSS MONDY: Merci beaucoup Arianna. Donc grosse augmentation du chiffre, n'est-ce pas, juste au moment du programme. Donc excellente nouvelle.

Ensuite, nous avons Jose Lopez, du .ES qui va nous expliquer ce qu'il se passe chez lui.

JOSE LOPEZ : Bonjour à tous. Jose Lopez du .ES.

Je vais parler du DNSSEC en ce qui nous concerne.Alors nous allons commencer par un petit historique.

En 2006 nous avons créé un essai, un test, pour mieux comprendre le DNSSEC, comment ça fonctionne, comment le mettre en œuvre, etc. Ensuite, en 2013, nous avons inclus le DNSSEC dans notre logiciel de système de registre. Ensuite activation en juillet 2014.

Alors quelques informations sur notre plateforme. Nous utilisons le BIND, le DNSSEC ouvert et quelques serveurs HSM. En ce qui concerne la politique de signature, nous avons le roulement de la KSK tous les deux ans, et de la ZSK tous les trois mois.

La plateforme a été assez stable. Nous avons eu uniquement un problème en janvier de cette année avec des erreurs de signatures, et donc nous avons dû identifier où était l'erreur. Et finalement, ce qu'il s'est passé, c'est qu'il y avait un problème pour un de nos serveurs HSM. Pour trouver la racine du problème, nous devons remercier notre ami registre qui nous a permis de trouver l'origine du problème.

Alors des chiffres. Le nombre de domaines signés commence à grandir petit à petit. Nous en sommes à 17 000 domaines signés sur le 1,9 millions que nous avons au total. Je ne sais pas si vous connaissez les taux, mais les taux sont très importants. Donc les 5 premiers bureaux d'enregistrement qui signent les domaines représentent 95 domaines signés. Alors cette année on devrait avoir une augmentation de 70 à 80 %.

Alors, quelles sont nos difficultés ? Donc du côté des initiatives, moins de 1 % de domaines signés dans le domaine des initiatives. Nous souhaitons que davantage de bureaux d'enregistrement locaux soient impliqués et activent les DNSSEC, et identifier davantage de moteurs de croissances.

Donc pour les initiatives, nous migrons du côté opérationnel nos serveurs HSM pour arriver au niveau 4 FIPS. Nous avons également collaboré avec INCIBE, donc l'agence de sécurité nationale, pour aider les gens à mettre en place le DNSSEC.

Par ailleurs, il y a d'autres activités de sensibilisations avec ESNOG, qui est un groupe d'opérateurs national espagnol.

Voilà, c'est tout. Merci.

RUSS MONDY: Merci. Bravo, vous avez respecté les délais. Et excellente présentation. Maintenant, Jaromir de CZNIC, qui va donc nous parler de la République Tchèque.

JAROMIR TALIR: Merci Russ. Je vais vous faire une petite mise à jour sur la situation dans .CZ.

Alors, petit à petit nous arrivons à 700 000 domaines signés. C'est environ 53 %. Récemment, nous sommes passés au-dessus du seuil des 50 % de domaines signés, ce qui est très important pour nous, parce que depuis ce moment-là, on peut dire qu'avoir le DNSSEC, c'est quelque chose de normal. Donc c'est un bon point marketing pour le DNSSEC.

Cependant, au cours des quelques années passées, il y a une stagnation. Donc l'augmentation n'est pas aussi importante qu'elle l'était auparavant ;

Nous avons également publié des statistiques sur le soutien des algorithmes dans la racine CZ, et donc on voit qu'il y a une grosse augmentation de l'algorithme ECDSA, grâce à notre plus gros bureau d'enregistrement. Il y a 3 gros bureaux d'enregistrement qui sont responsables de la situation. Parce que le ECDSA 13 est le plus utilisé des algorithmes dans la racine CZ. Nous avons également deux

bureaux d'enregistrement plus petits qui sont passés à l'algorithme 14, ce qui est un peu inhabituel.

Donc avec ce soutien ou cet appui de l'ECDSA, on pourrait s'attendre à ce que certains domaines apparaissent dans la zone racine. Il y a actuellement deux TLD, le CZ et le BR qui ont roulé la clef avec le CDSA en juin. Et là nous sommes au mois d'aout. Donc j'ai représenté ceci, ou j'ai pris les analyses en aout.

Par rapport au logiciel que nous développons. Donc notre registre OpenSource FRED est utilisé par davantage de TLD. Récemment nous avons mis au point une vérification d'algorithme de DNSSEC. Avant on n'avait pas de vérification d'algorithmes. Donc un algorithme pour être mis dans le registre, maintenant on peut toujours mettre un algorithme dans le registre, mais au moins, il est possible maintenant de configurer. Par exemple, si on souhaite ne pas permettre à d'anciens algorithmes d'être inclus.

L'année dernière, nous avons mis en place le scanner CDS-CDNSKEY. Donc André en parlera tout à l'heure. Il vous montrera des statistiques.

Notre logiciel DNSSEC dans le résolveur de nœuds, donc nous avons une nouvelle version, récente, qui soutien, qui est compatible avec le Caching NSEC3 agressif. Et il y a également une mise en œuvre de la sentinelle KSK.

Alors pour ce qui est d'autres DNS, nous avons la mise en œuvre de la KSK hors ligne, c'est quelque chose de nouveau qui devrait nous aider à l'utiliser dans nos propres scénarios. Nous avons la gestion divisée,

séparée de ZSK et de KSK avec pré-génération des ZSK à l'avance, nous les signons hors ligne. Donc nous espérons que ce scénario sera compatible ou sera supporté selon ces scénarios.

Alors si vous utilisez ces scénarios, et bien j'espère que cela vous intéresse.

Voilà, c'est tout.

RUSS MONDY: Merci beaucoup. Maintenant, nous allons écouter Paul Ebersman, de Neustar.

PAUL EBERSMAN: Neustar c'est une société commerciale. Nous avons un service de résolveurs récursifs ouverts et nous avons des opérations DNS pour des tiers. Donc il y a des parties de notre système qui ont DNSSEC.

Bonne nouvelle, nos résolveurs ont été validés depuis un certain nombre d'années. Nous faisons une validation DNSSEC pour chaque requête. Nous faisons 10 milliards de requêtes par jour, et nous n'avons pas eu de signalement d'incident au cours de la dernière année.

Donc le DNSSEC peut être fragile, mais...

Une compagnie commerciale soutient les entreprises notamment, donc l'histoire de signature de zone n'est pas trop longue. Le nombre

de zones signé a augmenté, mais nous nous sommes engagés à la faire augmenter de 30%.

Je crois qu'il y a 29 qui n'ont pas signé la zone, mais nous devons encore collecter les données.

Une partie de la difficulté, et j'entends dire cela à chaque fois que je parle avec les clients, c'est que nous faisons beaucoup de banlancing, [DAP], et eux ils sont plus intéressés aux tricks des DNSSEC qu'au fonctionnement du DNSSEC. Il y a certaines configurations du DNS qui les intéressent plus que le fait que le DNSSEC soit appliqué correctement.

Nous sommes en train de mettre en place une reconception de nos codes. Et ce que nous voulons faire, c'est faire la signature « on the fly » cela nous permettrait de mieux travailler même si on continue de signer DNSSEC.

Nous sommes au milieu d'une courbe assez conservative. L'algorithme, nous avons vu certains collègues qui font des dessins mais nous devons encore revoir les réponses au niveau de nos serveurs d'autorité.

Nous voyons un petit peu ce qui se fait par rapport à CDS, pour voir comment nous pouvons créer un plan pour l'année 2019.

Si vous avez des questions...

RUSS MONDY: Merci Paul. Nous avons 5 minutes pour des questions pour les membres du panel ; mais avant d'écouter les questions, nous allons applaudir les intervenants.

[Applaudissement]

Maintenant nous avons l'opportunité de poser des questions au panel.

Oui, ici.

RAED ALFAYEZ: Je viens de [inaudible]. Pour ce qui est des opérateurs de registre, croyez-vous que nous devons vérifier les clefs ou nous devons laisser les bureaux d'enregistrement télécharger ce qu'ils veulent sans validation ?

JAROMIR TALIR: Pour .CZ nous avons mis en œuvre les CDS. Nous avons donc vérifié la validation de la zone avec la clef CDS. Vous ne pouvez pas casser quoi que ce soit en publiant votre CDS, votre enregistrement CDS.

RAED ALFAYEZ: Mais le problème c'est que pourquoi vous avez téléchargé la nouvelle CDS ? Les DS.

JAROMIR TALIR: Nous avons quelque chose qui s'appelle le statut, le portail de statuts qui nous montre qui et comment ont mis en œuvre cela dans la zone

parent. Et nous essayons de montrer ces informations à travers ce portail.

RUSS MONDY: Est-ce qu'on a des réponses de quelqu'un d'autre ? Oui.

NON IDENTIFIE: C'est une approche différente. Pour nous, nous laissons que le bureau d'enregistrement télécharge ce qu'il veut dans la zone. Ce que nous faisons, c'est que nous faisons des vérifications techniques après, et nous informons le bureau d'enregistrement s'il y a des erreurs. Mais c'est à eux de résoudre s'il y a un problème. C'est une approche plutôt libérale de notre part.

RUSS MONDY: Peter.

PETER KOCH: Oui, bien entendu nous avons mis en place des tests de pré-délégation, depuis toujours. Et nous avons décidé de les appliquer au DNSSEC. Mais c'était non pas spécialement pour protéger les bureaux d'enregistrement de leurs propres erreurs, mais surtout pour qu'il n'y ait pas une perception négative des DNSSEC dans leur ensemble. C'était plutôt ça plutôt que de prévenir les erreurs des bureaux d'enregistrement.

PATRIK FALSTROM: Si vous mettez en place une politique, il faut être très prudent lorsqu'on télécharge plusieurs DS. Parce qu'il y a les anciens et les nouveaux, donc il faut faire super attention à ce qu'on permet de charger. Parce que cela peut avoir un impact sur les responsabilités de la zone vis-à-vis du client. Que ce soit un bureau d'enregistrement ou autre. Voir qui a la responsabilité, et cela diffère beaucoup en fonction des ccTLD. Nous avons écouté l'approche du Danemark, d'autres pays ont d'autres approches. Donc il n'y a pas d'approche unique qui puisse convenir à tous.

NON IDENTIFE: Si c'est un DS pour une DNSKey existante et que vous mettez l'information erronée, il faut leur dire que cette information est incorrecte.

RUSS MONDY: Très bien. Je pense que nous n'avons plus de temps.

Nous devons passer au prochain panel ; mais je veux remercier les intervenants. Si vous avez d'autres questions il faut que vous contactiez directement les panelistes, cette communauté a toujours été très efficace pour répondre aux questions des gens.

Merci beaucoup.

Notre prochain intervenant c'est Frederico Neves de .BR qui a très récemment été engagé dans le roulement d'algorithmes.

FREDERICO NEVES: Bonjour à tous. Je travaille pour .BR.

Pendant les 10 derniers mois, nous avons travaillé au changement d'algorithmes pour BR et donc je vais vous donner un bref aperçu de ce que nous avons fait.

Alors, il y a eu 10 mois de préparation, beaucoup de tests, beaucoup d'écriture de logiciels. Nous sommes passés de RSA-SHA1 à ECDSAP256. Cela a été fait du 20 au 23 aout 2018. Et tout s'est bien passé, pas de problème à signaler.

Un petit peu d'introduction. .BR a été signé en 2007, nous avons plus de 128 zones filles. Cela représente tous les domaines qui sont en dessous de .BR, avec des délégations de troisième niveau. Tout cela a été signé en RSA-SHA1.

Nous avons eu deux roulements KSK, réguliers, en 2010 juste avant la signature de la racine, et puis en 2015. Et pendant ces deux roulements KSK nous avons augmenté la taille de la clef KSK. Tout d'abord de 1280 à 1536 pour la KSK et de 1024 à 1280 pour la ZSK pour la zone à BR. donc de 1024 à 1280. Donc voilà la taille des clefs que nous avions avant le roulement de l'algorithme.

1280 pour ZSK et 1536 pour la KSK.

Alors, pourquoi ? Pour améliorer la sécurité et surtout pour être préparés au roulement de l'algorithme, parce que nous utilisions notre propre signature et donc nous n'avions pas de soutien au niveau du logiciel pour ce changement. Nous avons décidé d'être préparés avec des roulements réguliers, pour ne pas avoir à le faire à la va-vite.

Réduire la taille des réponses DNS c'était une autre motivation. Nous avions donc au niveau des RRSIG et DNS Key 60 % de réduction. Je vais présenter des chiffres un peu plus tard.

Une autre motivation, le système d'avitaillement DNS avait été créé en 2004, il commençait à dater, nous commencions à avoir des problèmes de maintenance au niveau des codes, des défaillances au niveau de la gestion de la mémoire qui posaient des difficultés pour nous. Et donc nous voulions passer à une étape supérieure.

Nous avions un dilemme : comment mettre en place ce roulement d'algorithme ? Je ne vais pas rentrer dans le détail, mais nous avons décidé de tester les deux méthodes, conservatrice et libérale, et finalement nous avons choisi la méthode libérale selon laquelle c'est beaucoup plus simple.

Le problème qui a été signalé par RIPE, par le passé, affectait seulement les anciennes versions Unbound. Mais nous avons fait les tests. Nous avons donc fait des essais avec 10 000 et nous n'avons pas vu des différences significatives entre les deux méthodes.

Dans d'autres diapos, nous avons tous les chiffres concernant ces vérifications.

Alors, roulement de l'algorithme, nous sommes passés de RSA-SHA1 avec les tailles de clef que vous voyez sur l'écran, à une seule CSK. Et pour le deuxième niveau RSASHA1 RSASHA1NSEC3. Et maintenant nous avons une seule clef pour le deuxième niveau CSK et une clef divisée.

Pour ce qui est de l'exécution, nous avons donc fait des mises à jour des logiciels du HSM, de tous les HSM pour être synchronisés, et nous les avons exportés aux différents endroits où il nous fallait les avoir. Et c'était fait dans une cérémonie séparée, trois semaines avant le roulement.

Nous avons réduit le temps à vivre TTL de certains enregistrements à 1 heure pour pouvoir accélérer le processus et nous avons pu réussir à avoir un roulement de 7 heures pour la CSK, notamment pour .BR, qui est un domaine assez large.

Le roulement CSK pour .BR a commencé à midi ou 12 h le 20 aout. C'était une double signature. Nous avons attendu 105 TTL pour que la nouvelle clef soit propagée. Tout le monde avait déjà le nouveau jeu de clef.

À 17 h, nous avons changé le DS dans les zones parentes, et à 19 heures l'ancienne CSK était retirée de toutes les zones enfant.

Le roulement KSK a commencé à la même heure. À 17 h, nous avons demandé à l'IANA de changer le DS, nous avons fait les confirmations, et l'IANA l'a fait très, très vite. Et nous avons fini la transition de la zone le même jour, et au bout de trois jours, nous avons pu retirer l'ancienne clef de la zone BR.

La chaine de confiance pour le roulement CSK s'est passé en douceur. Vous voyez la ligne bleue, c'est la résolution sécurisée mesurée par les sondes de RIPE. Il n'y a pas beaucoup de différences entre les

algorithmes, et vous voyez que le pourcentage reste plus ou moins le même, environ un peu moins de 40 %.

Voilà donc la mesure de la taille des clefs avant le roulement. 638 octets et 289 Octets. Pour ce qui est de la taille des réponses, nous avons donc les chiffres d'un mois avant, c'était en juillet. Et comme vous le voyez, la partie d'en bas, correspond à l'après roulement. Vous voyez qu'il y a des pics de réponses négatives autour de 1200 octets. Avant le roulement c'était de 800. Donc vous voyez que c'est une grosse réduction.

On voit ici la taille de la réponse CDAF avant et après le roulement. La ligne verte c'est après le roulement. Comme vous le voyez, le ECDSA pour les réponses 512 octets, nous avions moins de 850 octets et 99 % des réponses sont de moins de 850 octets, alors qu'avant c'était 1200. Vous voyez que le changement a été positif.

Voilà le pourcentage de requêtes TCP. Encore une fois la ligne bleue correspond au mois de juillet. Et ensuite c'est sur une période de 24 heures. Nous avons eu des pics de 3,5 % de transport TCP. Et maintenant, nous avons 0,7 %. C'était vraiment une très bonne réduction.

Voici les références pour la mesure de données, si cela vous intéresse. Il y a beaucoup de données.

Voilà, c'était ma présentation, merci beaucoup. Nous avons encore 4 minutes si vous avez des questions.

RUSS MONDY: Merci beaucoup Frederico. Y a-t-il des questions ? Geoff ?

GEOFF HUSTON: Est-ce que j'ai bien compris, donc vous aviez des problèmes de DNS, vous aviez moins de 1200, ça me semble très petit comme chiffre.

FREDERICO NEVES: Oui, il y a eu des réponses au-dessus de 1280. Mais oui, c'est vrai, les requêtes TCP étaient supérieures avant, effectivement.

Si vous regardez le diagramme avant le roulement de CSK pour le .BR, il a chuté juste après qu'on ait descendu les old keys. Et donc lorsqu'on a fait les roulements, je n'ai pas montré le diagramme, j'en avais un autre qui montre la période de 7 heures et les trois jours pour le roulement BR, et donc il y a eu augmentation du volume de requête TCP de 4,5 %.

Mais à ce moment-là, on avait des [key set] d'environ 1600 octets. Mais le diagramme en fait était un mois avant celui que j'ai montré qui était en bleu. C'était donc la situation normale du BR.

Autre commentaire, nous effectuons régulièrement des roulements de CSK, tous les mois. Donc avant, il y a eu une semaine où nous avons publié un ensemble de clefs un petit peu plus important.

RUSS MONDY: Allez-y.

DUANE WESSELS: Merci. Très bonne présentation avec beaucoup de données.

Ce n'est pas directement avec ce que vous avez dit, mais est-ce que vous pourriez nous expliquer pourquoi vous utilisez une clef combinée pour votre deuxième niveau ?

FREDERICO NEVES: La ZSK pour le BR et la CSK pour le deuxième niveau, alors on utilise notre signataire en ligne. Et lorsque nous avons terminé le stack, tout est intégré. Donc il est beaucoup plus simple d'avoir une clef unique au deuxième niveau. Nous avons un ensemble de clefs plus petit. Il s'agit du même logiciel que pour le roulement normal, donc il était plus facile d'utiliser la clef combinée.

RUSS MONDY: Une question Frederico, j'ai vu que vous avez abandonné les TTL, est-ce que vous surveillez également la charge sur les serveurs, et est-ce que vous aviez vu des charges supérieures ou est-ce que c'est resté au même niveau ?

FREDERICO NEVES: En fait nous avons abandonné nos TTL sur les délégations DS deux mois auparavant. On avait la délégation DS sur 24 heures, et les délégations DS sur 6 heures, on avait les deux, et on est arrivé à 1 heure, ce qui a augmenté notre charge, notre groupe de changement de 30 %. Donc on a eu un nombre inférieur de requêtes, ce qui a augmenté de 30 %.

Mais là c'est limité à une heure, ce qui était très bien pour les clients.

Nous avons fait des appels d'assistance, surtout pour les changements NS.

RUSS MONDY: Très bien. Merci beaucoup. Alors rapidement s'il vous plait.

NON IDENTIFIE: Question de suivi ; est-ce que vous avez pensé à utiliser la CSK pour le TLD ? Je sais qu'il y a des problèmes de changement de la clef fréquemment avec IANA parce que ce n'est pas automatisé, mais peut-être qu'il pourrait y avoir des cas où ça fonctionnerait.

FREDERICO NEVES: Pour la KSK nous utilisons un HSM, [VIOHSM]. Et il y a le problème de la gestion de la relation avec la parente. Donc ce n'est pas possible d'utiliser la ZSK pour le BR.

RUSS MONDY: Merci Frederico, très intéressant. Nous en sommes maintenant au moment de la pause.

Il devrait y avoir du café, etc. pas très loin. Nous allons reprendre rapidement, donc à 10 h 30 précise. Et je demanderais donc aux membres du panel de 10 h 30 de venir s'installer à l'avant ici, sur le panel.

Voilà, merci beaucoup et profitez bien de votre café.

[FIN DE LA TRANSCRIPTION]