FR

ICANN85 Mumbai | Forum de la communauté – Séance conjointe : ALAC et SSAC
Dimanche 8 mars 2026 – 13h15 à 14h30 IST

CLAIRE CRAIG — Bonjour tout le monde. Veuillez lancer l'enregistrement.

YESIM SAGLAM — Bonjour et bienvenue à cette séance conjointe ALAC et SSAC. Je m'appelle Yesim Saglam, et je suis responsable de cette séance.

Cette séance est enregistrée et elle est régie par les normes prescrites par l'ICANN et ses politiques anti-harcèlement.

Les questions et les commentaires ne seront lus à haute voix que s'ils sont soumis de la façon appropriée. L'interprétation est disponible en anglais, français et espagnol.

Si vous souhaitez prendre la parole pendant cette séance, les participants à distance auront l'autorisation d'allumer leurs micros virtuels et les participants sur place recevront un micro. Veuillez indiquer votre nom pour l'enregistrement, la langue dans laquelle vous prendrez la parole si elle est autre que l'anglais, et veuillez vous exprimer à un débit raisonnable.

Je donne maintenant la parole à Claire Craig, qui est la vice-présidente de l'ALAC, et à Ram Mohan, président du SSAC.

CLAIRE CRAIG

Bonjour tout le monde ou bonsoir en fonction de votre emplacement. Bienvenue à cette séance conjointe ALAC et SSAC. C'est toujours une très bonne séance.

Alors, il s'agit donc de [inaudible] qui est à distance. Commençons notre séance. Je vais passer en revue l'ordre du jour et, ensuite, chacun aura l'occasion de se présenter. Alors, nous allons d'abord souhaiter la bienvenue à tout le monde. Nous allons parler donc du DNSSEC pour les utilisateurs finaux. Il s'agira ensuite donc des priorités et des parties prenantes pour le SSAC et les priorités pour 2026. Et nous aurons donc une séance de *brainstorming* sur les prochaines étapes. Et ensuite, il y aura les remarques de clôture.

Et avant de donner la parole à l'intervenant suivant, je voudrais vous demander donc de gérer donc la logistique sur Zoom. Donc, je voulais dire cela avant de donner la parole à Ram Mohan. Et je vous donne la parole pour la suite.

RAM MOHAN

Bonjour, Claire. Bonjour tout le monde ! Je crois que c'est une heure tout à fait indue. Je vous félicite pour votre dévouement. C'est remarquable. J'apprécie énormément. Merci beaucoup.

Donc, en ce qui concerne la gestion de la logistique, si le personnel du SSAC peut m'aider, ça serait très apprécié. J'ai accès à mon écran, mais je ne vais peut-être pas pouvoir tout faire en même temps.

Nous sommes toujours très heureux d'être avec vous, de participer à ce que fait l'ALAC. Il y a beaucoup d'idées partagées que nous avons commencé à mettre en pratique, et je me réjouis de continuer la discussion avec Claire et avec votre comité afin de dégager nos objectifs communs.

Donc, sur ce, suite à cette introduction, il y a plusieurs membres du SSAC, Mathias, Peter Thomassen, qui sont à ma droite dans la salle. Nous leur avons demandé de vous parler un petit peu du DNSSEC, mais pas du point de vue des techniciens, mais vraiment de vous parler du DNSSEC du point de vue des utilisateurs finaux.

Alors, nous souhaitons avoir une conversation en quelque sorte avec vous. Nous allons peut-être vous montrer quelque chose en direct si les dieux des démos le veulent bien. Alors, sur ce, je vais donner la parole à Matthias.

MATTHIAS HUDOBNIK Est-ce que vous pouvez passer à la diapositive suivante ?

Bonjour, je m'appelle Matthias Hudobnik. Je suis donc un membre du SSAC. Est-ce que tout va bien maintenant ? Mon objectif, aujourd'hui, c'est de vous donner une introduction rapide sur les principes de fonctionnement, donc, du DNSSEC.

Alors, le DNS, c'est l'annuaire téléphonique de l'Internet. Et donc il a été conçu il y a déjà un certain temps. Et maintenant, il faut que les réponses que nous obtenons de cet annuaire soient des

réponses correctes, ou du moins que nous puissions détecter les erreurs.

Diapositive suivante, s'il vous plaît. Merci.

Donc, je prends l'analogie d'une carte postale. C'est une carte postale ouverte et elle est envoyée. Et quiconque en cours de route peut la lire, ou, même pire, effacer l'adresse et en écrire une autre. Par exemple, envoyer la carte postale à un site malveillant plutôt qu'à votre banque.

Et le DNSSEC ? Donc, ce sont des extensions de sécurité du système des noms de domaine. Donc cette carte postale, il n'y a pas d'encodage, mais on voit s'il y a eu donc une utilisation frauduleuse et on bloque les réponses falsifiées.

Donc, il y a deux choses que vous devez retirer, c'est l'authentification de l'origine — on sait que l'information est venue de la bonne source — et l'intégrité des données, donc on doit savoir qu'il n'y a pas eu de modification en cours de route.

Diapositive suivante, s'il vous plaît. Très bien.

Donc, au cœur, la cryptographie des clés publiques du DNSSEC fait que l'utilisateur a sa propre clé, ce qui crée donc une signature numérique d'enregistrement de ressources. Donc, c'est un timbre numérique. Il y a un processus de vérification. Ensuite, il y a une publication de DNS clé -- de clé DNS. Et donc, il y a une réception d'une réponse pour vérifier la signature. Si la signature est valide, les données sont authentifiées, sinon elles sont rejetées. Il faut une

signature correcte et le résolveur fait une validation DNSSEC, ce qui n'est pas universel sur l'Internet, comme nous le savons tous.

Diapositive suivante, s'il vous plaît. Merci.

Ensuite, il y a la chaîne de confiance. Ici, il y a une question essentielle : comment savons-nous que la clé publique est légitime ? Donc, un attaquant peut donc intervenir. Donc, il y a une hiérarchie naturelle et chaque parent, donc, garantit la légitimité de son enfant. La chaîne en elle-même fait qu'il y a une chaîne continue, par exemple sur .EU ou .COM. Et la racine est donc l'ancre. Et on a donc une situation de confiance pour la totalité du DNS mondial.

Diapositive suivante. Donc, il y a un exemple négatif ici. Donc, la difficulté, c'est la façon dont le DNSSEC traite les choses qui n'existent pas. Donc, normalement, dans le DNS normal, un attaquant peut falsifier une réponse et vous rediriger. Et donc, il y a une mesure pour empêcher une redirection vers quelque chose qui n'existe pas — donc quand il n'y a rien entre l'entrée A et l'entrée C.

Diapositive suivante, s'il vous plaît.

Donc, l'expérience de l'utilisateur final. Ce qui est très important, c'est qu'il y a une protection invisible. Vous n'avez pas besoin d'en installer quoi que ce soit. Une application sur votre résolveur récursif est fournie par votre fournisseur de services Internet ou par le DNS public. Donc, si la validation échoue, donc la réponse est

qu'il y a une erreur *serve fail*. Et c'est un peu comme un garde du corps silencieux qui empêche l'attaque. Et parfois, il a simplement un signe que quelqu'un a effectué une configuration incorrecte.

Je vous demande de passer à la diapositive suivante.

Donc, en résumé, le DNSSEC fournit une authentification de l'origine et de l'intégrité des données, ce qui renforce la confiance de la fondation du DNS. Et c'est très important.

Il faut savoir que le trafic n'est pas codé. Cela n'empêche pas les logiciels malveillants. Et en cas d'erreur, il peut tout de même y avoir des problèmes. C'est un outil puissant, mais ce n'est pas la panacée.

Et maintenant, je vais donner la parole à Peter. Merci.

PETER THOMASSEN Oui. Donc, l'airbag, par exemple, de votre voiture, vous ne devez pas le déclencher automatiquement. C'est un peu la même chose. Donc je m'appelle Peter Thomassen. Je vais vous parler de quelques considérations concernant le DNSSEC.

Alors, tout d'abord, le DNSSEC n'est pas une seule sécurité permettant la sécurité de votre Internet. Il est -- il fait partie de différentes mesures de sécurité. Le DNSSEC permet de sécuriser les informations concernant les noms de domaine, et notamment la traduction de ces noms de domaine en adresse IP ou quoi que ce soit que vous voulez visiter dans le DNS.

Alors, le système de routage dans l'Internet est vulnérable parfois. Par exemple, une section de site Internet fait la publicité par rapport au fait qu'il se charge d'une certaine partie des adresses IP. Tout cela doit être sécurisé, bien sûr, par le DNSSEC. Et cela permet d'empêcher certaines personnes de voler les adresses IP d'autres personnes. Donc ça, c'est ce qu'on appelle le RPKI, les infrastructures de clés publiques de ressources.

Alors, le DNSSEC ne protège pas le contenu d'être inspecté. Donc, il faut aussi assurer la confidentialité de son contenu. Et ça, c'est ce qu'on appelle le chiffrement. Pour ce faire, on utilise la méthode de la TLS, de la sécurité de la couche de transport, par exemple. Donc, idéalement, lorsqu'on se connecte à un service, à une messagerie, un chat, un site Web, eh bien, qu'est-ce qui va se passer ? Eh bien, l'IP adresse est vérifiée. Dans l'idéal, elle est sécurisée, ce qui signifie que le nom de domaine -- l'intégrité de ce nom de domaine est assurée.

YESIN SAGLAM Donc on a demandé à Peter de ralentir pour les interprètes.

PETER THOMASSEN Alors ensuite, la première chose à faire est de vérifier que l'adresse IP est sécurisée grâce au DNSSEC. Ensuite, il s'agit de préparer sa requête HTTP. Ce qui signifie que l'email, par exemple, qu'on veut envoyer doit être chiffré pour le transport. Ça, c'est permis grâce à

la TLS — la sécurité de la couche de transport — qui permet donc de garantir le caractère privé du contenu.

Et puis, ensuite, il faut envoyer l'adresse IP, qui est donc dirigée de manière sécurisée grâce à la RPKI. L'infrastructure de clé publique de ressources.

Diapo suivante, s'il vous plaît.

Alors, ici, vous avez des exemples d'attaques du DNS, ou plutôt des attaques contre lesquelles le DNS vous protège. Donc, par exemple, le détournement d'espace de noms en 2019.

Par exemple, il y a eu une attaque qui est assez connue qu'on a appelé l'attaque Sea Turtle. Je ne sais pas très bien pourquoi on l'appelle comme ça, mais bon, bref. Et donc, grâce à des attaques d'hameçonnage, des bureaux d'enregistrement ont été attaqués et le service de noms -- les noms de domaine ont été changés. Différentes agences ont été affectées : des ministères, des agences de renseignement, des agences de télécom, des FSI. Et donc, en fait, les utilisateurs étaient redirigés vers les serveurs de noms des attaquants qui ont pu, par exemple, rediriger les emails vers leurs services à eux et inspecter le contenu de ces emails, par exemple, utiliser aussi et vérifier, par exemple, quelles étaient les références, par exemple les mots de passe des utilisateurs. Et donc, on disait que le département du ministère des Affaires intérieures des États-Unis a donc dirigé cela -- a donc décrit cela comme un trafic utilisateur redirigé vers des infrastructures contrôlées par les attaquants, qui permettaient d'obtenir le chiffrement valide, les

certificats de chiffrement valides. Donc, cela signifie qu'on pourrait être affecté par un faux certificat de chiffrement qui serait accepté par votre navigateur.

Diapo suivante, s'il vous plaît. Merci.

Alors ensuite, il y a eu l'affaire Packet Clearinghouse concernant les ccTLD. Une diapo en arrière, s'il vous plaît.

Et donc, cette attaque Sea Turtle a également affecté ce point-là.

Deux diapos en arrière s'il vous plaît maintenant ? Il faut revenir en arrière de deux diapositives. Maintenant il faut aller en avant une diapo. Merci.

Et donc ils ont également été attaqués. Et cette attaque n'a pas été une réussite parce qu'ils se sont servis du DNSSEC. Il y a Bill Woodcock de PCH qui en parle sur YouTube. Donc vous avez un hyperlien qui vous permet d'y accéder. Si vous téléchargez les diapositives, vous pourrez cliquer et accéder à cette vidéo.

Alors, les services Serveurs de noms ont été installés auprès du bureau d'enregistrement. Mais ensuite, étant donné que les employés de PCH utilisaient le DNSSEC et des mesures grâce au DNSSEC, eh bien, ces noms de domaine n'ont pas été acceptés par leur système et il n'y a pas eu de détournement des données. Ensuite alors, les enregistrements de la délégation du signataire n'étaient pas changés non plus.

Ensuite, deuxième type d'attaques qui pourraient être atténuées grâce au DNSSEC, ce sont les attaques de routage. Par exemple, un

attaquant revendique le fait qu'il est responsable de la gamme d'adresses IP de quelqu'un d'autre.

Par exemple, en 2018, une attaque avait été revendiquée pour le serveur de noms Amazon Route 53 qui est utilisé par un portefeuille de cryptomonnaie. Et le résultat de cette attaque a été que la requête pour ce nom de domaine s'est retrouvée dans le serveur de noms de l'attaquant. Ils ont pu présenter un faux site et voler environ 150 000 USD de cryptomonnaie avant que le problème ne soit résolu. Alors cette attaque n'a pas été prévenue par le DNSSEC, car il n'était pas utilisé à ce moment-là. Mais si l'entreprise avait utilisé cela, alors ces adresses IP se seraient retrouvées tout de même sur le serveur des attaquants. Mais par contre, les faux noms de domaine n'auraient pas pu être des réponses acceptées par le système d'Amazon Route 53.

Donc, l'idée ici est de vous préciser que le DNSSEC protège contre la transmission de données via le Wifi. Par exemple, il vous protège d'attaques qui cherchent à exploiter le DNS via d'autres vecteurs.

Diapo suivante, s'il vous plaît.

Alors j'ai parlé des trois technologies qui se complémentent. RPKI, par exemple, l'infrastructure de clé publique de ressources qui protège le routage. Eh bien, il est déployé à 62 % et ce chiffre a augmenté fortement au cours des deux dernières années. Pourtant, il est apparu sur le marché il n'y a pas si longtemps. Mais cette ressource est si bien déployée parce qu'elle peut être déployée par les FSI ainsi que par les RIR — les Registres Internet

régionaux. Cela n'exige pas la coopération des titulaires de noms de domaine ou des utilisateurs finaux. Donc, il n'y a pas besoin d'éduquer, de former le public à l'utiliser.

S'agissant du HTTPS qui protège le contenu, eh bien, il est déployé environ 95 % à l'heure actuelle. Eh bien, c'est parce qu'après différents scandales, il y a eu une automatisation, en fait, de l'utilisation de HTTPS, qui est maintenant utilisé dans pratiquement tous les services Internet. Vraiment, c'est automatique de l'activer.

Ensuite, la protection grâce au DNSSEC. Donc, 7 % des noms de domaine enregistrés utilisent le DNSSEC. Alors, en note de bas de page de cet écran, vous pourriez trouver une ressource qui vous donne plus de chiffres. Mais voilà. Quoi qu'il en soit, le pourcentage de déploiement du DNSSEC est bien plus inférieur comparé aux deux autres technologies, parce qu'il y a deux étapes pour l'activer. Parce qu'il faut signer une zone créée, ensuite il faut entrer les informations de la clé là où on cherche à se connecter. Et très souvent, en fait, cette deuxième étape n'est pas bien configurée.

Alors, les bureaux d'enregistrement exploitent les noms de domaine. Et si votre fournisseur de DNS est différent de votre bureau d'enregistrement ? Très souvent, le bureau d'enregistrement doit s'impliquer dans ce processus. Et très souvent, les gens ne sont pas au courant de cela.

Je vais vous montrer à quel point c'est compliqué et c'est vraiment inutile que ce soit si compliqué. Mais bon, bref.

Diapo suivante, s'il vous plaît.

Donc, ici, je vais vous montrer certains exemples de formulaires. Et ils sont très différents. Vous ne devez pas tout lire, mais voilà.

Ici, vous avez un formulaire permettant à un bureau d'enregistrement d'introduire un DNSSEC -- des paramètres DNSSEC pour un nom de domaine. Voilà, ça c'est une façon de le faire.

Diapo suivante. Ça, c'est un autre formulaire pour faire la même chose. Ça semble un peu étrange, mais donc il faut sélectionner différentes choses, copier-coller différents éléments de l'enregistrement DS. Et voilà. C'est difficile de savoir quoi faire si on n'a pas les bonnes instructions.

Diapo suivante. Et voilà encore une fois un autre formulaire pour faire la même chose. Bon, je pense que vous avez compris.

Diapo suivante, s'il vous plaît.

Le DNSSEC connaît un problème d'accessibilité. Donc, ça ne veut pas dire que cette technologie est fragile. C'est plutôt qu'elle est difficile à configurer dans l'intérêt des utilisateurs finaux. Il serait judicieux de pouvoir faire des progrès à cet égard et de pouvoir permettre une activation plus accessible, plus automatique du DNS. Ce qui ne veut pas dire que tout le monde doit l'utiliser, mais

si vous voulez l'utiliser, par contre, eh bien, ça devrait être aussi simple que d'appuyer sur un interrupteur.

Diapo suivante, s'il vous plaît.

Alors, il y a des solutions à ce problème. Si on retire toute intervention manuelle, il y a moins de possibilités d'erreurs. Comment faire cela ? Eh bien, l'opérateur du DNS peut dire à un opérateur de registre qu'il voudrait activer le DNSSEC, et il peut prouver qu'il s'agit là d'une requête authentique.

Alors je vais vous montrer tout cela avec un exemple qui a fonctionné. Nous avons mené un webinaire il y a quelques semaines avec le RALO, et nous avons démontré cela en direct. Et cela nous a pris à peu près 1 h, parce qu'il faut que les fichiers de zone racine soient mis à jour. Mais bon, voilà. À ce moment-là, nous avons fait une démonstration en direct.

Diapo suivante, s'il vous plaît.

Imaginons qu'on enregistre le nom de domaine euralowebinar.cz. Eh bien, alors, ça veut dire qu'on peut s'adresser à l'opérateur de registre cz et leur dire « Voilà ma requête pour activer le DNSSEC, voici les informations nécessaires ». Donc, il y a un signal entre la clé enfant et la clé parente.

Diapo suivante s'il vous plaît.

L'opérateur de registre cz va vérifier cela -- va vérifier la validité de cette requête et va ensuite intégrer l'enregistrement DS.

Diapo suivante. Alors ici, vous voyez l'état d'avancement des analyses du DNSSEC pour ce domaine. Ça, c'était avant qu'on enregistre le nom de domaine euralo-webinar.cz. Vous voyez ici, en bas, il est dit que la réponse est nxdomain pour euralo-webinar.cz. Ce qui veut dire que le nom de domaine n'est pas enregistré. Une fois que le nom de domaine est enregistré, il y a des informations supplémentaires au bas de l'écran concernant les signatures. Mais voilà, il manque l'enregistrement DS, la croix rouge, comme vous le voyez à l'écran. Donc le nom de domaine est enregistré. Le DNSSEC n'est pas encore activé. Mais—

Diapo suivante. Sans interaction de l'utilisateur, lorsque la fonctionnalité automatisation est activée, à un moment, cette croix rouge va devenir un V vert. Il va y avoir une interaction entre l'opérateur du DNS et le nom de domaine parent, et ça va permettre d'activer le DNSSEC. Et donc il semblerait que ce soit une bonne façon de permettre aux titulaires de nom de domaine d'activer cette fonctionnalité sans devoir passer par plein de formalités.

Diapo suivante, s'il vous plaît.

Alors qu'en est-il ? Eh bien, ce n'est pas encore employé pour les ccTLD. J'ai parlé de .CZ. Il y a aussi .Suisse, .Ouzbékistan, le Costa Rica, l'Afrique du Sud, le Liechtenstein, etc. Mais ce qu'il est important de savoir, eh bien, c'est que, pour les gTLD, pour le moment, le DNSSEC n'est pas activable.

Et il y a des petites différences de mise en œuvre. Par exemple, lorsqu'il y a un verrou de mise à jour, ça veut dire qu'on ne sait pas si l'activation du DNSSEC est autorisée ou pas. Et donc ça veut dire qu'on doit se pencher là-dessus pour que tout fonctionne de la même façon. Une fois que l'activation du DNSSEC sera permise pour les gTLD—

Il y a un document [dans] l'IETF. Ce sont des recommandations sur la façon de procéder. Ça deviendra donc un RFC plus tard dans l'année. Et à ce stade, il serait bien que l'automatisation du DNSSEC soit autorisée dans tout l'espace TLD afin qu'il y ait moins d'erreurs, que le DNSSEC soit plus accessible. Et donc cela est issu du rapport de la recommandation du rapport SAC126.

J'espère que cela vous a été utile. J'espère que vous allez -- vous avez pu voir à quel point cela pourrait être facile. Les choses pourraient être faciles. Et j'espère que vous avez pu voir quels sont les écueils.

CLAIRE CRAIG J'ai la main levée dans le chat. Je saisis cette occasion de poser une question. Vous avez parlé de la difficulté de mettre en œuvre le DNSSEC dans les petits [marchés]. Je me demande est-ce que le DNSSEC peut être mis en œuvre à un point d'échange Internet?

PETER THOMASSEN Cela porte sur la livraison de paquets entre l'expéditeur et le destinataire. Cela va dans le réseau [net] -- réseau Google, par

exemple, et on voit que l'infrastructure de clé publique de ressources fonctionne correctement. Et donc, le DNSSEC n'a aucun rôle à jouer dans ce cas-là.

CLAIRE CRAIG Merci. Y a-t-il d'autres questions ?

RAM MOHAN Je vois que donc il y a des questions. M. Nath. Oui, vous avez la parole.

M. NATH Vous avez parlé de l'automatisation pour les ccTLD. Et quelle est la difficulté pour les ccTLD ? Et donc combien de temps vous a-t-il fallu pour faire adhérer les ccTLD correspondants ?

PETER THOMASSEN Je n'ai pas été impliqué dans ce processus. Je crois qu'ils ont pris leur décision. Donc, les questions de mise en œuvre se posent depuis plusieurs années. Je ne sais pas quand cela a commencé -- peut-être 2020 ou quelque chose comme ça. Et depuis ce moment-là, il y a des aspects opérationnels, tels que les verrous qui ont été clarifiés. Et donc, il y a eu des ajustements, notamment en Suisse.

Quelles ont été les difficultés ? C'est une bonne question. Je pense que, à l'atelier DNSSEC qui se déroulera mercredi, donc, il y aura

quelqu'un de CPH qui nous fournira son rapport. Et je vous suggère d'écouter ses contributions.

AMRITA CHOUDHURY

Nous avons beaucoup de formations DNSSEC, du moins au niveau de l'Asie. Est-ce qu'il y a un état d'esprit qui doit être présent pour les fournisseurs d'accès de services Internet ? Donc est-ce que ce sont les FSI qui doivent intervenir principalement ? Donc, très souvent, quand on parle de mise en œuvre, on envisage des coûts. Est-ce que ça doit être une approche verticale ?

PETER THOMASSEN

Oui, je crois que c'est vrai. Il y a donc la signature et la validation. Il y a souvent un coût qui est associé à tout cela. Et souvent, les entités ne sont pas désireuses de dépenser.

Donc, il y a eu un incident de détournement en 2019. Je crois qu'il y a eu des articles et il y a eu des organisations au Moyen-Orient, en particulier en Arabie Saoudite. Donc, au début, donc, il y avait un taux de 20 % d'impact. Et ensuite, c'est passé à 90 %.

Donc, en général, il faut savoir qu'au-delà des questions de coûts, il ne faut peut-être pas toujours attendre.

SETONDJI HOUNZANDJI

[Inaudible] français. Ok. J'attends Peter, il n'est pas prêt. Ok. Ok. Donc c'est Hervé Houzandji. Je suis le secrétaire d'AFRALO. La question que je vais poser, c'est une question personnelle.

Moi-même, je suis ingénieur en informatique. Et donc ça m'arrive déjà d'implémenter DNSSEC sur des domaines. Et je me suis toujours demandé, ce que vient de présenter Peter, pourquoi on ne l'a pas fait depuis longtemps? C'est-à-dire qu'aujourd'hui, lorsque vous voulez configurer un serveur Web Apache ou [inaudible] avec du certificat, vous pouvez utiliser latin scripts, et ça vous donne directement comment il faut faire. Vous lancez juste un script et le système vous dit comment il faut configurer. C'est très facile. Donc je me demandais toujours pourquoi on ne l'a pas fait pour le DNSSEC.

Ma question, surtout, c'est, le travail que vous faites là -- vous savez, il y a des ccTLD en Afrique. Ok? Comment vous allez faire pour que ce truc-là soit aussi utilisé par les Africains ? Moi, aujourd'hui, quand je veux faire -- je viens du Bénin. Notre ccTLD, c'est .BJ. Lorsque -- oui, voilà. Lorsque je veux faire du DNSSEC sur un sous-domaine du .BJ, ce n'est pas facile. Même quand je crée moi-même les clés. Après, il faut que j'envoie l'information au .BJ. Des fois, quand je lui envoie l'information, ça met une semaine pour qu'il me valide ça. Voilà. Or, avec votre script, je pense que ça va les obliger et ce sera mis à jour automatiquement. Est-ce qu'il y a une procédure qui est en place pour toucher plus de ccTLD, surtout en Afrique, pour les aider ? Je ne sais pas comment vous allez faire. Merci.

PETER THOMASSEN Merci pour cette question. Je ne suis pas au courant d'un processus particulier qui soit en place.

Le degré de difficulté dépend du logiciel que vous utilisez. Il y a des logiciels modernes qui ne sont pas DNS. Je crois qu'il y a aussi, au niveau de CZNIC, des éléments utiles. Pour les registres qui utilisent ces logiciels, il faut tout de même faire la configuration. Mais vous n'êtes pas obligé de faire la mise en œuvre vous-même. Je ne sais pas quels sont les logiciels qui sont utilisés par BJ, mais il n'y a pas de procédure particulière.

Je ne sais pas si cette réponse vous a été utile.

RAM MOHAN Merci Peter. Pari ? Maarten ?

MAARTEN AERTSEN Donc cela revient à la réponse qui a été donnée à Claire. Je ne crois pas qu'il y a quelque chose qui retienne le déploiement des technologies mentionnées par Peter. Je crois que, sa réponse, c'est de savoir s'il y a donc un point d'échange qui se rapporte aux DNS. Mais pour les petits marchés, certains des ccTLD qui ont déployé cela sont des petits marchés. Donc, je voulais juste ajouter cet élément.

PETER THOMASSEN Je voudrais ajouter quelque chose. Le DNSSEC existe depuis un certain temps. Et l'automatisation, c'est nouveau. Et il y a eu

beaucoup d'erreurs et de défaillances qui se sont produites. Et donc l'image du DNSSEC en a pâti comme étant instable et non fiable. Donc, il y a un problème d'image. Donc, il y a le fait que maintenant l'automatisation est disponible.

Il y a un article intéressant rédigé par Barbara qui est ici, et je le mettrai dans le chat. Pour ceux qui s'intéressent donc aux facteurs non techniques qui empêchent le déploiement du DNSSEC, je vous encourage à lire l'article.

RAM MOHAN Merci pour la gestion du chat. Donc il y aura Sébastien et puis ensuite nous aurons les intervenants qui souhaitent prendre la parole.

SEBASTIEN BACHOLLET [Inaudible] beaucoup en ayant commencé à parler en français. J'ai des noms de domaine ; comment est-ce que je peux m'assurer que j'ai DNSSEC ou pas de DNSSEC ? Et qu'est-ce que je peux faire pour l'avoir d'un point de vue d'un utilisateur du DNS. Merci.

PETER THOMASSEN Maarten veut répondre.

MAARTEN AERTSEN

Si j'ai bien compris, la question, c'est de savoir comment est-ce qu'on peut vérifier que les choses sont correctement, donc, configurées.

Donc, il y a des outils qui sont conviviaux pour vérifier que votre domaine est bien configuré. Donc dans mon pays, c'est internet.nl. Vous pouvez faire une vérification. Vous mettez votre nom, et ainsi on vous indique si le DNSSEC est configuré pour un domaine donné. Et vous pouvez aussi vérifier si votre FSI est validé. Vous pouvez vérifier votre connexion. Donc je ne sais pas si cela répond à votre question.

Il y a deux outils disponibles et, l'un de ces outils, c'est dans le domaine internet.nl.

PETER THOMASSEN

Donc, Sébastien, donc, si vous achetez un domaine, vous pouvez voir s'il y a un chiffrement. Vous pouvez faire la vérification des identifiants de l'utilisateur. Il suffit de cocher une case et c'est tout.

RAM MOHAN

Merci Matthias.

VASYL « BILLY » BRATCHENKO

Matthias a dit que, en tant qu'utilisateur, quand vous recevez un message d'erreur, cela veut dire qu'il y a une tentative d'interception ou que quelque chose est mal configuré. Est-ce qu'il y a une façon technique de clarifier ? Est-ce que c'est une tentative

frauduleuse ou est-ce que c'est une mauvaise configuration ? Est-ce qu'on peut faire la différence ?

PETER THOMASSEN C'est très difficile à détecter d'une manière générale. Comme Matthias l'a dit donc, le DNSSEC, c'est votre garde du corps silencieux. S'il fait une erreur, c'est qu'il a reçu les mauvaises instructions et l'accès sera bloqué. Et c'est en fait ce que le DNSSEC est censé empêcher. Il empêche -- il doit empêcher les mauvaises configurations. Donc, de nos jours, c'est beaucoup plus rare.

MATTHIAS HUDOBNIK Je voulais dire donc nous aurons un webinaire DNSSEC pour l'EURALO. Vous pouvez donc écouter ce webinaire. Il y aura des gens de .CH, .PT, l'EURALO et Cloudflare. Et Barbara aura une intervention. C'est un webinaire d'une heure et demie qui sera très utile. Vous pourrez apprendre beaucoup de choses et je vais donc afficher le lien dans le chat. Merci.

RAM MOHAN Il y avait une question de ce côté-là. Je vous en prie.

AVIRAL KAINTURA Aviral pour l'enregistrement. Donc merci Peter et Matthias d'avoir expliqué ce qu'est le DNSSEC du point de vue de l'utilisateur final.

Lorsque le DNSSEC échoue, ça veut dire qu'on va recevoir une erreur serve fail. Et ça veut dire qu'il y a peut-être aussi toute une

série de problèmes sous-jacents. Il n'y a qu'un moment -- que dans une situation bien spécifique qu'on reçoit ce message d'erreur serve fail. Mais ça peut être un problème de sécurité, une erreur de configuration.

Donc, du point de vue des utilisateurs finaux, y a-t-il plus de transparence par rapport à ce qui se passe là derrière dans ce cas-là ?

PETER THOMASSEN Oui, pardonnez-moi. J'étais distrait. Est-ce que vous pourriez reposer votre question ?

AVIRAL KAINTURA Oui. Donc, lorsque la validation DNSSEC échoue, on reçoit un message d'erreur serve fail. Mais cela sous-tend peut-être différentes choses. Ça peut vouloir dire qu'il y a une erreur de configuration, qu'il y a un problème de sécurité. Donc moi, je demandais, du point de vue des utilisateurs finaux, est-ce qu'on peut avoir plus de transparence pour savoir, en fait, ce qui se passe derrière ce message d'erreur?

PETER THOMASSEN Oui et non. Donc vous avez raison. Effectivement le code d'erreur serve fail est générique pour tous types d'erreurs, mais il y a différentes exceptions.

Au DNS, par exemple, des codes d'erreur étendus DNS ou d'autres codes similaires — je ne sais pas quelles sont les abréviations — donc le résolveur inclut des informations dans la réponse qu'il envoie et qui précise ce qui n'a pas fonctionné. Par exemple, il y a eu une erreur de nom de serveur, ou alors la signature de clé est expirée. Et si vous avez cela, cette information ne va pas ressortir au niveau du navigateur parce que le navigateur va demander au système d'exploitation l'adresse IP et il ne va recevoir que l'adresse IP ou pas de réponse. Mais il n'y a pas de structures de données qui permettent de transférer cette erreur -- cette précision quant à l'erreur au niveau du navigateur. Mais les navigateurs, à l'avenir, pourraient peut-être afficher plus d'informations permettant de savoir pourquoi on ne peut pas accéder à telle ou telle chose.

Ça, c'est un travail qui est en cours. Je pense qu'il y a de grandes entreprises de navigateurs qui souhaitent s'impliquer là-dedans, mais je ne sais pas quand ce système sera opérationnel.

Moi, je me dis que ce n'est pas vraiment à l'utilisateur final de déterminer ce qui ne s'est pas bien passé, c'est plutôt à l'opérateur de registre. Il y a différentes façons dont un résolveur peut informer l'opérateur des erreurs qui ont été réalisées.

RAM MOHAN Merci. Alors je vais maintenant mettre fin à cette partie questions-réponses. Mais bon, voilà, il semblerait que ce sujet intéresse beaucoup de personnes. Cela a suscité beaucoup de questions.

Je vois Mourad qui souhaite prendre la parole en ligne. Oui, on vous entend.

MOURAD MELLITI

Oui. Oui. Bonjour. En fait, je voulais rebondir sur la question de la sécurité. Bon, je vais reprendre, je vais répondre en quelque sorte sur est-ce que c'est suffisant donc d'avoir DNSSEC sur la zone, donc, ou bien c'est pas suffisant ? Donc là, dans toute la chaîne, il y a plusieurs intervenants sur la sécurité du domaine, Ce n'est pas uniquement l'utilisateur final et non plus l'opérateur du registre. Il y a aussi donc les prestataires de services. Il y a les prestataires de services cloud ou bien les bureaux d'enregistrement qui proposent en fait le DNSSEC pour l'utilisateur final. Il y a une petite nuance là sur cette chaîne. C'est-à-dire, le fait que le domaine soit signé ou bien soit sécurisé, c'est une condition nécessaire, mais pas suffisante pour que le domaine soit protégé ou bien pour que le site derrière lequel le domaine fonctionne donc soit protégé. D'accord ?

Donc je gère le .TN. Le .TN donc est sécurisé depuis 2014. Mais il y a des bureaux d'enregistrement, donc, qui ne proposent pas les domaines qui utilisent le .TN. C'est-à-dire activer l'automatisation en fait de l'utilisation de DNSSEC aussi bien sur le ccTLD ou bien pour le gTLD, ce n'est pas toujours donc la solution finale en fait pour avoir DNSSEC activé par défaut. C'est-à-dire qu'il y a toujours des intervenants au milieu qui doivent proposer ça à l'utilisateur

final. Je voulais juste en fait rebondir sur cette question, parce que c'est très important d'impliquer en fait toute la chaîne dont--

PETER THOMASSEN Oui, effectivement. C'est un problème multifacettes et multiacteurs. Vous avez raison. Cependant, donc il faut aussi avoir les paramètres DNSSEC. Donc, le bureau d'enregistrement est une partie intermédiaire. Et bon, c'est une partie qui doit transférer les informations. Mais si vous trouvez une façon de pouvoir obtenir les informations auprès d'un opérateur de registre, eh bien, ça fonctionne aussi.

Et pour les ccTLD, voilà, très souvent, ils ne passent pas par les bureaux d'enregistrement. CZ est directement passé par CloudFlare, par exemple. Ici CloudFlare est le principal opérateur de nom de domaine, puis il se tourne vers l'opérateur de registre. Et ici, le bureau d'enregistrement n'est qu'un observateur dans tout ce processus. Donc oui, c'est possible.

C'est aussi possible que le bureau d'enregistrement se charge de cette automatisation. C'est en fait une question un peu politique. Il semblerait qu'il serait plus facile que l'opérateur de registre, justement, retire cette charge des épaules du bureau d'enregistrement. Certains ont décidé de le faire.

Si vous êtes intéressé d'avoir plus de détails par rapport à tout ça, eh bien, ça fait partie des recommandations opérationnelles

incluses dans le document qui est ici à l'écran. Si vous avez les diapos, vous pourrez cliquer sur l'hyperlien et y avoir accès.

Donc, oui, le bureau d'enregistrement peut s'impliquer, mais il ne doit pas nécessairement être impliqué.

RAM MOHAN Merci Peter. Robert.

ROBERT GUERRA Oui, alors je voulais juste remonter d'un niveau, on va dire.

Là, les discussions portaient sur les questions, les problèmes qui surviennent. Mais il ne faut pas non plus oublier l'intégrité des données et l'authenticité du DNS. Le chiffrement, ça aide et c'est quelque chose que les utilisateurs et que tous les groupes de l'ALAC utilisent. Et il faut aussi former les personnes, éduquer les personnes à utiliser cela. Et il faut faire savoir aussi que, maintenant, c'est un choix que les bureaux d'enregistrement font ou ne font pas. Ils ont le choix d'activer ou non le DNSSEC. Et ceux qui le font vont permettre une meilleure authenticité des données. C'est un mécanisme qui existe, qui est peut-être invisible aux yeux des utilisateurs. Mais, par contre, c'est un choix que l'utilisateur peut faire. Et c'est très important.

Alors maintenant, malheureusement, il y a de plus en plus d'attaques sur différentes infrastructures, des problèmes… Et le fait de choisir le bon bureau d'enregistrement qui dispose des

mécanismes permettant de vous protéger, eh bien, voilà, ça, c'est un choix que l'utilisateur final peut faire.

Donc, ici, voilà, on se penche vraiment sur les détails, mais il faut aussi se rendre compte que des bureaux d'enregistrement déploient cette solution -- automatisent l'activation du DNSSEC. Et, vraiment, si vous avez un nom de domaine enregistré, eh bien, allez voir si le DNSSEC est activé. Et sinon, allez voir comment le faire et comment le recommander aux autres.

Vous avez une discussion à la pause-déjeuner concernant votre choix de bureau d'enregistrement. Ça peut aider. Souvent, maintenant, les personnes choisissent les bureaux d'enregistrement un peu moins chers, mais est-ce que ça, c'est une fonctionnalité qu'ils offrent ? Peut-être pas. Et donc, le DNSSEC, c'est une bonne chose de le déployer et ça deviendra de plus en plus facile au fil du temps.

RAM MOHAN Merci Robert. Donc cela nous amène à la fin de cette dernière section. Frederic à vous.

FREDERIC TAES Oui. Frederic au micro. Merci beaucoup pour cette session très intéressante.

Alors, nous avons organisé une table ronde sur le DNSSEC qui a été une véritable réussite et je dois dire que l'enquête que nous avons envoyée à nos participants nous a donné des retours très positifs.

Entre 80 à 100 % des participants ont été convaincus d'activer le DNSSEC après notre table ronde. Donc un résultat exceptionnel, vraiment.

Et je voulais vraiment dire que oui, c'était très complexe, très abstrait. On se demandait comment -- qu'est-ce que c'est le DNSSEC, comment faire pour l'activer. Et en fait, nous avons rendu -- nous avons pu rendre les choses très concrètes grâce à cette table ronde.

Alors j'en reviens aux utilisateurs finaux. L'EURALO a également déployé -- développé une extension du navigateur pour nous aider à utiliser le DNSSEC pour protéger les données -- les noms de domaine. Je l'ai postée dans le chat. Donc c'est www trust.org. Donc c'est une extension que vous pouvez installer sur votre navigateur et qui peut afficher si le DNSSEC est activé pour tel ou tel nom de domaine. Parce que voilà, ces informations ne sont pas si facilement accessibles. Et cela vous donne aussi d'autres informations concernant les noms de domaine que vous visitez. Voilà. Merci beaucoup.

RAM MOHAN Merci beaucoup. C'est absolument génial d'avoir ce retour de votre part. Et puis merci aussi d'avoir partagé avec nous le fait que cette session s'est très bien passée.

Je pense que c'est une véritable récompense pour toutes ces personnes qui font des efforts pour transformer notre jargon technique en un langage que les gens comprennent.

FREDERIC TAES Oui. Et d'ailleurs, il y a eu aussi des participants qui venaient d'entreprises. Donc ce ne sont pas des membres de la communauté ICANN. Donc on avait un peu des personnes lambda qui ont participé aussi à ce webinaire. Et ils ont appris beaucoup de choses sur la sécurité grâce à nous.

RAM MOHAN Merci beaucoup. Allez-y !

JONATHAN ZUCK Bon, je ne pense pas que c'est un problème, mais si ça n'a pas été enregistré ou si ça a été enregistré plus tôt -- enfin, bref, on n'a pas besoin de tout l'enregistrement Zoom, mais peut-être qu'on pourrait tirer les informations principales de cette réunion pour rendre ces informations accessibles à toutes et à tous. Je ne sais pas si vous l'avez déjà fait. Et malheureusement, nous n'avons pas entendu le commentaire de Frederic.

FREDERIC TAES Oui, merci beaucoup pour ce commentaire, Jonathan. Oui, c'est prévu. Donc on s'améliore aussi. On communique beaucoup mieux sur les réseaux sociaux, sur LinkedIn et voilà. C'est le genre de

chose justement qu'on promeut auprès d'une communauté plus large de personnes.

JONATHAN ZUCK

Oui, et puis alors vous avez la déesse des médias juste à côté de vous d'ailleurs.

NATALIA FILINA

Oui, merci beaucoup pour votre aide pour avoir organisé cette table ronde. Alors, Joly McFie de l'ISOC a beaucoup aidé aussi pour mieux structurer les informations grâce -- il a rédigé des résumés de nos enregistrements. Et donc je vais poster le lien vers toutes ces informations dans le chat si vous voulez plus d'informations.

RAM MOHAN

Merci beaucoup. Alors je pense que l'une des leçons à tirer, on va dire l'une des choses à retirer de cette réunion, un des points sur lesquels on voudrait pouvoir bénéficier de votre aide, eh bien, vous nous entendez dire que l'automatisation, ça aide ; l'automatisation, ça rend tout plus facile -- mais cela signifie aussi une réduction des erreurs, une simplification de ce sujet.

Bon, il y a encore du pain sur la planche et il y a beaucoup de choses en cours au sein de l'ICANN aussi. Le SSAC a publié un rapport sur l'automatisation, il y a quelque temps, mais nous encourageons aussi, bien sûr, les gTLD à faire en sorte que l'automatisation devienne un mécanisme normal.

Et donc, lorsqu'il y aura un débat à ce sujet, on pourrait avoir besoin de votre voix pour promouvoir ce que nous apportons, c'est-à-dire le côté technique.

Bien, alors nous n'avons encore qu'un peu de temps. Donc, ce que je voudrais faire, c'est que l'on passe directement à la discussion sur la campagne pour un cyberespace plus sûr. Et c'est maintenant donc Jonathan qui va nous en parler et qui va nous expliquer comment avancer avec cette idée.

Alors, si vous ne connaissez pas -- si vous n'avez pas entendu parler de cela, pour info, l'ALAC et le SSAC se sont engagés dans des discussions très productives au fil des dernières années pour faire de quelque chose d'abstrait une réalité. Nous avons pu créer du contenu. Nous avons créé du matériel de formation grâce à l'ALAC, avec des diapositives qui donnent des explications et qui vraiment expliquent de manière non technique ce qui se passe lorsqu'on est victime d'hameçonnage et qui traduisent tout cela en actions à mettre en œuvre pour les utilisateurs finaux. Et on veut encourager cela.

Et donc on voulait partager avec vous, vous informer de ce qu'on fait avec d'autres sections de notre communauté. Et puis, ensuite, on vous donnera la parole pour un *brainstorming* pour savoir ce qu'on peut faire ensemble.

JONATHAN ZUCK Je ne savais pas, alors.

RAM MOHAN Je croyais que nous avions quelque chose d'ouvert ici.

Diapositive suivante, s'il vous plaît. Alors, depuis le début de cette année, nous avons commencé une collaboration avec ISPCP. Et avec, donc, l'ISPCP, nous avons annoncé des séances à l'ICANN en plus des webinaires sur plusieurs sujets. Chacun de ces sujets est un sujet auquel le SSAC s'intéresse, mais aussi peut proposer des contenus, des éléments. Et donc nous fournissons les experts techniques.

Donc, Billy était présent en février. Est-ce que vous voulez nous parler de la façon dont ça s'est déroulé ? Combien de personnes il y avait ? Après, j'apporterai des éléments supplémentaires.

VASYL « BILLY » BRATCHENKO Il y avait 107 personnes, je pense. Billy au micro. Donc, il s'agissait de l'automatisation de l'atténuation de l'utilisation malveillante. Et il y a eu des activités. Et il y a eu donc un bon niveau de participation.

RAM MOHAN Je ne vais pas tout lire — tout ce qu'il y a à l'écran ici. Vous voyez donc quelque chose qui a beaucoup plus de pertinence pour une organisation de type FSI. Donc, tout cela est proposé ici à l'écran, à titre informatif, mais aussi pour faire démarrer la discussion.

JONATHAN ZUCK

Amrita a peut-être des choses à ajouter. Nous avons formé un sous-groupe au sein de ces ACES. Nous regardons aussi les autres moyens de diffuser les informations à travers nos réseaux.

Donc, il y a les ALS, qui ont leurs propres idées. Nous avons dégagé plusieurs idées. Par exemple, une campagne sur Twitter -- sur X, plutôt X. Il peut y avoir donc une liste de numéros de téléphone à joindre, à atteindre pour la diffusion.

Il y a eu donc une campagne Twitter liée à l'acceptation universelle. Nous avons donc réfléchi à une marque mondialement connue qui n'avait pas encore mis en place l'acceptation universelle. Et l'ICANN a œuvré assidument pour cerner quelle marque pourrait faire l'affaire.

Je ne sais pas quelle est la bonne réponse. Est-ce qu'il y a une façon d'identifier les personnes qui pourraient être les récipiendaires d'une telle campagne dans l'espace DNSSEC ?

Donc, comment est-ce que l'on peut corréler la question du DNSSEC avec l'utilisateur final ? Est-ce que nous pouvons être utiles ? Est-ce que nous pouvons faire en sorte que notre réseau communique avec les plus gros réseaux à titre expérimental, pour sensibiliser, pour inciter les gens à opérer un déploiement ? Est-ce que vous pouvez réfléchir à une façon d'identifier qui doit entendre ce message ? Alors, à ce moment-là, nous pourrions mobiliser notre réseau pour effectuer les choses.

RAM MOHAN

À titre personnel, je pense que, depuis des années, nous -- prenons le DNSSEC, par exemple. Au début, nous le traitions comme une question technique. Nous expliquions la technologie pour démystifier la technologie. Et plus nous essayons de démystifier cette technologie, plus elle devenait mystérieuse. Alors nous avons vu qu'il y avait des erreurs de configuration. Il y avait des rapports qui disaient que ce TLD a rencontré un problème à cause du DNSSEC.

Et au sein de SSAC, ce que nous faisons, c'est deux choses. Premièrement, comme Peter et Matthias le font, eh bien, ils expliquent la technologie de façon plus accessible. Ça, c'est un aspect. Et par ailleurs, il y a aussi une équipe qui doit terminer ses travaux à la fin de l'année sur toutes les considérations opérationnelles du DNSSEC.

Et une chose qui n'est pas dite, c'est que le DNSSEC est complexe du point de vue opérationnel. Et certaines organisations vont peut-être décider que ça ne les intéresse pas. Ce n'est pas pour elles. Donc, les 100 principales organisations ou sociétés sur Internet qui n'ont pas déployé le DNSSEC, pourquoi ? Pour de nombreuses raisons. Donc, si vous voulez déployer le DNSSEC, quelles sont les choses que vous devez mettre en place pour vous préparer non seulement pour le déployer, mais aussi pour le maintenir déployé, pour faire en sorte qu'il continue à être sûr et sain du point de vue opérationnel ?

JONATHAN ZUCK Voilà, c'est ça. C'est le message principal.

RAM MOHAN Il faut réfléchir au fait que si l'utilisateur final n'a pas accès aux outils et qu'il ne comprend pas la valeur, les avantages d'avoir le DNSSEC -- alors est-ce que nous devons déployer notre énergie vers les intermédiaires pour qu'eux expliquent la technologie aux consommateurs plutôt que nous nous adresser directement aux consommateurs, aux utilisateurs finaux ?

JONATHAN ZUCK Ils sont un peu plus sophistiqués. Par exemple, si vous faites partie d'une ALS, vous avez une structure un peu différente. Nous, nous essayons d'agir au bénéfice des utilisateurs finaux, mais à travers notre réseau.

Je pense que nous avons des gens qui ne vont pas considérer que ce que nous faisons est une bonne idée. Ils n'auront peut-être pas les connaissances nécessaires pour faire un déploiement ou expliquer ce qu'il faut faire, mais il faut peut-être commencer par déterminer qui est notre public. C'est à ça qu'il faut réfléchir.

RAM MOHAN Il y a une file d'attente pour les questions. Il y a Russ, ensuite Hervé, ensuite Amrita et ensuite Sébastien.

RUSS MUNDY Je voudrais répondre à la question de Jonathan.

À qui faut-il parler dans de nombreux cas ? Ceux qui sont donc sur le terrain ont une meilleure connaissance -- savent mieux à qui il faut parler. Ils le savent mieux que le SSAC.

En général, ce que l'on a entendu depuis de nombreuses années de la part de nombreux fournisseurs, et aussi de la part des bureaux d'enregistrement, c'est qu'il n'y a pas de demande pour le DNSSEC. Personne ne demande le DNSSEC. Alors, toutes les interactions que vous pouvez avoir ou que vos équipes peuvent avoir avec leur FSI ou leur bureau d'enregistrement ou leur opérateur de registre, eh bien, ils demandent donc un soutien. C'est important, car au sein de l'ALAC, des RALO, beaucoup de gens sont conscients de l'importance du DNSSEC. Et c'est eux qui peuvent transmettre le message aux fournisseurs.

Moi, j'ai changé de bureau d'enregistrement parce que certains des bureaux d'enregistrement que j'utilisais, donc, ne soutenaient pas le DNSSEC. Donc, moi, je suis passé à un autre bureau d'enregistrement. Et c'est vraiment un levier qu'un utilisateur peut avoir, pas dans tous les cas, mais dans de nombreux cas. Merci.

RAM MOHAN Merci Russ.

SETONDJI HOUNZANDJI Merci. En fait, moi, je voulais juste relever un message d'espoir.

Ce matin, on a discuté un peu sur l'intelligence artificielle et ses inconvénients par rapport à tout ce qui est abus du DNS. Moi, je peux vous garantir que, aujourd'hui, l'intelligence artificielle permet quand même le côté positif à beaucoup de personnes -- de maîtriser ou de commencer par comprendre comment implémenter le DNSSEC. Donc, il y a quand même cet avantage qu'il faut relever.

Et de plus en plus, je pense que tous ceux qui avaient peur de comment il faut créer une clé, comment il faut la clé de la clé, tout ça, ça va, s'améliorer. Donc, pour moi, j'ai l'espoir que ça va continuer et il y aura de plus en plus de domaines qui seront en DNSSEC. Voilà. Merci.

RAM MOHAN Merci. Donc voilà. On dit bien que l'espoir est le chemin qui mène vers le bonheur.

AMRITA CHOUDHURY Alors oui, deux choses.

Tout d'abord, j'ai une question. Est-ce que nous souhaitons promouvoir le DNSSEC ? Comme vous l'avez dit, beaucoup d'entreprises font le choix de ne pas le mettre en œuvre.

Et pour répondre à Jonathan, par exemple, quand on regarde les FSI, il y en a plusieurs types. Il y en a qui ont donc une ou deux personnes qui font tout dans les pays en développement. Et il y a des catégories. Il y a donc des différences de capacités

considérables. Donc, si on pense à une campagne pour permettre aux gens de savoir s'ils sont prêts à mettre en œuvre le DNSSEC, est-ce que nous pourrions, avec SSAC, par exemple, et l'ICANN, proposer donc une page avec les informations nécessaires. Parfois, c'est difficile d'obtenir les informations nécessaires et tout le monde souhaite avoir quelque chose qui soit presque clé en main. Est-ce que nous pourrions faire quelque chose dans ce sens ?

At-Large en tous cas, au moins au niveau des RALO, nous pouvons probablement envisager cela. Et donc, est-ce que nous pourrions envisager une chose qui permette aux gens de savoir s'ils sont prêts pour la mise en œuvre de DNSSEC ?

RAM MOHAN Sébastien.

SÉBASTIEN BACHOLLET Merci Ram. Alors, il y a beaucoup de sujets que vous avez projetés à l'écran et ça pourrait nous intéresser aussi, nous en tant qu'utilisateurs finaux. Peut-être devrait-on réfléchir à la façon de gérer l'IPCP avec At-Large. Mais il y a deux sujets notamment pertinents pour l'ICANN86 qui me semblent très importants. Le postquantum. Le postquantique, c'est maintenant. Ce n'est pas demain. Et ensuite vie privée vs sécurité. C'est aussi une question qu'on doit traiter, nous, en tant qu'utilisateurs finaux.

Donc ces deux sujets, je pense, doivent être vraiment l'objet de notre programme. Aussi, je serai heureux qu'on puisse le faire. Merci.

RAM MOHAN Merci. Bien sûr, nous serions heureux de travailler à vos côtés là-dessus. Nous voilà ici. L'idée, c'était de lancer la conversation.

Maarten, vous aurez le dernier mot.

MAARTEN AERTSEN Oui, je me demandais si l'ALAC voulait que Peter revienne une fois qu'ils auront terminé de normaliser l'automatisation du DNSSEC, parce que vous avez mentionné dans vos diapos qu'il y a encore un peu de pain sur la planche. Mais lorsque ce sera terminé, il sera peut-être judicieux de commencer à parler de lancement de campagne ou autre.

SÉBASTIEN BACHOLLET Oui, s'il vous plaît. Parlez de l'At-Large. Il n'y a que 15 membres à l'ALAC. Nous en aurons besoin certainement. Mais nous, les millions d'utilisateurs au sein de l'At-Large, nous en aurons besoin encore plus.

RAM MOHAN Merci. Bien. Ah ! Vous avez encore une question ? Oui, je vous en prie.

KARAN Bonjour à tout le monde. Le DNSSEC a ses limites, bien sûr. Donc, cette initiative est une bonne chose, certes, mais est-ce que nous, au sein de l'ICANN, nous pensons que le DNSSEC n'est pas la seule réponse à l'utilisation malveillante du DNS vu ses limites ?

Ensuite, bon, bien sûr, il y a différentes étapes à entreprendre — des campagnes, par exemple —, mais qu'est-ce qu'on pourrait faire d'autre ?

RAM MOHAN Bien, je pense que l'utilisation malveillante du DNS, et notamment dans le cadre de l'ICANN, peut être résolue par le DNSSEC. Mais le DNSSEC n'est qu'une petite solution.

Bien sûr, il y a bien d'autres questions qui sont suscitées. Il y a des PDP aussi par rapport à ces utilisations malveillantes du DNS, les vérifications de domaine associées, etc. Donc oui, le DNSSEC, ce n'est pas la panacée pour les problèmes liés au DNS.

Et nous, au sein de SSAC, nous venons de lancer un groupe de travail qui se penche sur l'impact de l'IA sur les utilisations malveillantes du DNS. Donc on se lance. On vient tout juste de se lancer dans ce travail, dans ce domaine. Donc voilà, je vous dirai gardez les yeux ouverts, car il y a encore beaucoup d'autres choses qui vont se produire.

JONATHAN ZUCK

Oui, il y a beaucoup de choses qui sont en cours aussi à l'heure actuelle. Par exemple, le nouvel EPDP sur les noms de domaine associés. Une autre PDP sur les enregistrements de masse, les programmes de notification de confiance, l'aide aux contrats, etc.

L'OCTO, dans le cadre de l'ICANN, a également commencé à déployer des outils qui permettent de comprendre aussi la source de ces utilisations malveillantes du DNS.

Donc voilà. Oui, c'est certainement un domaine multifacettes. Il y a différentes façons de résoudre ce problème. Et il n'y a pas que le DNSSEC. Il y a aussi beaucoup d'autres initiatives en cours.

RAM MOHAN

Merci. Eh bien, sur ce, je voudrais remercier Jonathan et Claire pour leur temps. Merci de nous avoir accueillis ici. On apprécie toujours nos réunions avec At-Large et on voit, là, la profondeur.

Le détail de nos discussions d'aujourd'hui témoigne vraiment de la richesse de la relation que nous sommes en train de construire, mais aussi de la qualité de l'intérêt que nous avons pour ce dont nous nous chargeons les uns les autres.

JONATHAN ZUCK

Oui, et on est toujours heureux de vous accueillir. Merci d'être venus nous voir. Comme je l'ai déjà dit, vous faites vraiment un travail incroyable. Vous produisez aussi beaucoup d'études, de

thèses, que personne ne lit jamais. Mais vraiment, je suis heureux qu'on puisse faire connaître votre travail. Merci.

[FIN DE LA TRANSCRIPTION]