ICANN76 | Forum de la communauté – Programme de bourses de l'ICANN : introduction à l'OCTO et KINDNS
Dimanche 12 mars 2023 – 10h30 à 12h00 CUN

SIRANUSH VARDANYAN : Si vous voulez bien venir vous placer à l'avant de la salle, c'est une grande salle, nous aimerions vous voir. Changez de siège et venez plus près du podium ici. Je vous remercie. Mes amis NextGen et les boursiers qui sont assis là-bas au bout, venez vous asseoir près du podium, je veux voir vos visages et vous sourire surtout. Venez vous installer près de nous.

La séance va commencer. Veuillez lancer l'enregistrement s'il vous plaît. Merci beaucoup.

Bonjour à tous et bienvenue à cette deuxième journée de l'ICANN76. J'espère que vous avez apprécié la journée d'hier. Je m'appelle Siranush Vardanyan et je vous souhaite à tous la bienvenue à cette réunion avec notre équipe technologique et l'équipe de l'IANA qui vont vous expliquer un peu plus de choses sur toutes ces abréviations.

Une petite annonce logistique avant cela. Je serai votre directrice de la discussion à distance pour cette séance. Cette séance sera enregistrée et elle est régie par les normes de comportement attendues de l'ICANN.

Au cours de cette session, les commentaires et les questions soumis dans le chat seront lus à haute voix seulement s'ils sont présentés sous la forme appropriée, comme cela est indiqué dans le chat.

Si vous voulez prendre la parole pendant cette séance, levez la main dans la salle Zoom et l'on ouvrira votre micro. Les personnes dans la salle vont avoir un micro volant – il y en a deux dans cette salle.

Pour tous les participants, donnez votre nom pour l'enregistrement et parlez à un rythme approprié car nous avons une interprétation dans les six langues de l'ONU. J'encourage toutes les personnes à venir prendre un casque à l'entrée pour utiliser les services d'interprétation. Nous avons une équipe d'interprétation fantastique avec nous.

Sur ce, je voudrais présenter les présentateurs de la journée. Nous allons parler avec le directeur du bureau de la technologie, John Crain qui est là avec son équipe et avec Kim Davies qui il va nous parler des services de l'IANA. Nous allons commencer avec John.

JOHN CRAIN : Merci Siranush et merci à tous. Je suis heureux que vous soyez tous ici. Siranush le sait, les boursiers et les NextGen, ce sont mes deux groupes préférés à l'ICANN. Vous êtes des visages tout nouveaux, vous avez de nouvelles idées.

Je suis John Crain, vice-président sénior et directeur du bureau de la technologie de l'ICANN. Je suis à l'ICANN depuis au moins deux décennies, cela fait donc un bon moment. Je fais partie des meubles, disons. Je gère un groupe qui s'appelle IROS. Vous n'en entendez pas parler beaucoup, c'est une distinction un peu spéciale que nous avons. Nous sommes à l'extérieur. Nous adorons les acronymes. Le « I » d'IROS, c'est identificateurs, pensez à l'Internet. Nous parlons de la recherche des identificateurs. Le « O », c'est pour opérations et le « S »

est pour sécurité. Le « I », c'est la lettre qui est importante. Nous connaissons l'importance des identificateurs.

Vous pouvez ventiler ceci en deux thèmes. Nous avons un groupe qui s'appelle l'IANA : c'est l'autorité chargée de la gestion de l'adressage sur l'Internet qui est géré par Monsieur Kim Davies qui est à ma gauche et ensuite, nous avons un groupe qui est focalisé sur l'engagement relié à tout ce qui est technique, géré par Adiel qui est un ami à moi. Mais David est là aujourd'hui. Il y a beaucoup de recherches qui sont faites aussi. Deux de mes managers sont là. Je sais qu'il y en a un qui est timide et qui se cache là-bas dans la communauté. Dites bonjour, Samaneh, s'il vous plaît. Venez nous rejoindre si vous voulez. Je ne vois pas Matt. Le voilà. Matt, tu peux venir nous rejoindre. Ou alors il peut être timide et rester dans la salle, ce n'est pas grave.

Voilà les choses que nous faisons. Nous faisons des recherches sur tout ce qui traite des identificateurs. Nous travaillons sur les opérations et nous parlons de tout cela. Nous discutons de tout cela. Je ne vais pas passer tout mon temps à vous faire des présentations. Je vais demander aux personnes qui travaillent avec moi de vous donner une idée de ce sur quoi nous travaillons et je vais commencer avec la chose la plus importante que l'ICANN fait. Vous avez entendu parler de l'élaboration des politiques. Les politiques sont importantes si on peut vraiment les mettre en place et si on peut gérer ces fameux identificateurs. Alors, parlez-nous du rôle de l'IANA, Kim.

KIM DAVIES : Je vais aller vite parce que j'ai une présentation et je voulais la proposer bientôt.

En fait, l'IANA est un peu comme un grand magasin, un annuaire de tous les identificateurs sur l'Internet. Beaucoup de personnes connaissent les noms de domaine, il y a les identificateurs, mais il y a aussi les adresses IP que vous connaissez. Il y a des milliers d'identificateurs qu'on utilise tous les jours dans les communications que l'on a sur l'Internet. Il faut qu'il y ait un endroit centralisé où il y a des identificateurs qui sont signés pour que les choses fonctionnent au niveau du monde. Ce sont donc les fonctions de l'IANA et on va en parler un peu plus tout à l'heure.

JOHN CRAIN : Le « R », c'est pour la recherche. Vous pouvez parler de ce que fait votre groupe ?

SAMANEH TAJALI : Je suis à la tête du groupe de recherche sur la sécurité, la stabilité et la résilience, le SSR. Nous sommes au sein du bureau du directeur de la technologie. Nous travaillons sur des études qui sont liées directement ou indirectement à la sécurité du DNS. Il s'agit de thématiques dont vous entendez parler dans les réunions de l'ICANN, comme l'utilisation malveillante du DNS, la sécurité, toutes les choses qui ont un impact sur les noms de domaine, le phishing, les logiciels malveillants, les problèmes de sécurité, de protocole, etc.

Je vais passer la parole à Matt.

MATT LARSON : Je suis à la tête d'une équipe de recherche aussi. Nous travaillons parfois sur la sécurité, mais nous ne sommes pas autant focalisés là-dessus. Nous avons accès au trafic du serveur de l'ICANN. Nous faisons des recherches en utilisant cela. Nous faisons des recherches liées au contenu du DNS. Nous avons accès aux dossiers racine. Ce sont des ensembles de données qui nous apportent beaucoup. Nous sommes aussi très actifs lorsqu'il s'agit de l'IETF. Nous faisons des vérifications au niveau des protocoles, nous faisons des améliorations au niveau des documents opérationnels.

JOHN CRAIN : David, pouvez-vous nous parler un peu de votre travail sur l'engagement ?

DAVID HUBERMAN : Bonjour à tous. Nous travaillons dans ce département qui s'appelle l'engagement technique. Nous avons un personnel qui est composé d'ingénieurs mondiaux qui travaillent dans des communautés techniques et non techniques pour établir de bonnes compétences sur tout ce qui est le DNSSEC, le routing sécurisé et l'aspect RPKI des RIR. On travaille sur l'engagement surtout avec la communauté non technique sur des thématiques liées à l'ICANN pour être sûr que tout le monde comprenne bien le côté ingénierie et le côté qui est sous-jacent à la structure de l'Internet. Nous collaborons beaucoup avec nos amis, nos collègues de l'ICANN, avec les gouvernements et avec les communautés non techniques aussi pour nous assurer que tout le

monde puisse communiquer dans la même langue sur le fonctionnement de l'Internet.

JOHN CRAIN : C'était une bonne présentation.

Je vais passer aux questions très vite parce que vous avez entendu parler de nous. Mais avant, le personnel d'IROS dans la salle, veuillez vous lever afin que tout le monde puisse vous connaître.

Il y a plusieurs d'entre nous ici, mais nous avons beaucoup plus de personnel. Nous avons amené un petit contingent de personnes de notre groupe à la réunion pour pouvoir justement interagir avec la communauté. C'est important de recevoir vos informations de retour. Je vais passer la parole à mes collègues.

SIRANUSH VARDANYAN : Cette séance est planifiée pour les boursiers et les NextGen ; je vous encourage donc à communiquer et à poser des questions car vraiment, c'est une opportunité unique pour vous tous. Beaucoup d'entre vous ne sont pas des techniciens, mais il est très important de comprendre le point de vue technique sur lequel travaille l'ICANN. Ne soyez pas timide, je vous l'ai dit durant la première séance, il n'y a pas de questions stupides, jamais de questions stupides. Posez des questions et peut-être qu'on peut commencer comme cela. Pensez à ce qui vous intéresse et posez des questions.

Nous avons des micros volants. Je vais demander à ce que les micros soient en place. Quelqu'un a une question ? Les micros arrivent. Les

voilà, ils arrivent, donnez-nous deux secondes. Nous allons commencer par cette personne. Nicolas, on reviendra vers vous tout à l'heure. Merci.

HARISH CHOWDHARY : Bonjour, je suis Harish Chowdhary, je suis boursier. Je suis universitaire en Inde et je fais de la recherche sur la sécurité du DNS.

Pour l'équipe de recherche, comment contribuer ? Parce que je travaille sur la sécurité du ccTLD .in. Comment contribuer au travail ? Comment apprendre sur la nouvelle technologie de cette équipe ? Merci.

JOHN CRAIN : Samaneh, vous pouvez répondre ?

SAMANEH TAJALI : Merci de votre question. Merci d'être là avec nous.

En fait, je ne sais pas si vous connaissez le projet DAAR que l'ICANN a instauré ; c'est un outil pour faire des rapports sur les problèmes. Nous travaillons en collaboration avec ce groupe et je voudrais que vous m'expliquiez un petit peu les projets sur lesquels vous travaillez. Ainsi, nous pourrons peut-être travailler ensemble et discuter et peut-être vous envoyer dans la bonne direction. On fait beaucoup de travail sur la sécurité des TLD, donc on pourrait peut-être faire des choses avec vous. Encore une fois, on a un groupe de signalement des cas d'utilisation malveillante des noms de domaine s'appelle le DAAR.

JOHN CRAIN : Nous avons aussi publié des documents sous le nom de série OCTO. Vous pouvez les consulter et si pensez à quelque chose qui est intéressant ou vous pensez que ces documents peuvent être intéressants ou pas du tout, écrivez-nous, envoyez des commentaires, participez aux séminaires, posez des questions aux personnes de l'équipe. Nous sommes toujours là pour discuter. On pourrait trouver de meilleures manières d'effectuer nos recherches, peut-être que nous pouvons améliorer notre manière de faire. On a besoin de feedback.

NICOLAS FIUMARELLI : Bonjour. J'ai entendu parler que la sécurité ne faisait pas forcément partie de la mission de l'ICANN. Si cela fait partie des recherches de l'ICANN, je suis curieux de parler de la résilience des infrastructures des grandes entreprises. Par exemple il y a quelques années, il y avait eu un incident de Meta sur Facebook qui impliquait le DNS. Est-ce que vous pouvez nous donner un peu une idée de ce qui se passe avec la compagnie Meta et nous parler de la résilience de ces grandes entreprises ?

JOHN CRAIN : Votre question comprend beaucoup d'éléments. Vous parlez de la sécurité du routing. Le routing n'est pas sous le mandat de l'ICANN. L'ICANN est à propos des identificateurs. Nous avons, bien sûr, un intérêt dans ce sens car nous travaillons autour du DNS. L'ICANN fait partie d'une communauté, les bureaux d'enregistrement, les opérateurs de registre, les fournisseurs de résolveurs ; les adresses IP font partie de cette discussion et on parle des RIR. Nous discutons des

ISP. Ce n'est pas le même domaine que le DNS, mais nous ne faisons pas que le DNS. Je vais quand même passer la parole à David pour qu'il en parle.

DAVID HUBERMAN : C'est une très bonne question. C'est une question dont nous parlons en interne car on ne veut pas vraiment aller au-delà de notre mandat. Les RPKI et cette idée de sécurité du routing où les fournisseurs d'Internet et tous les participants dans le routing de l'Internet expliquent qui ils sont : « Voilà notre réseau, etc. », ceci n'a pas été sécurité pour 30, 40 ans.

Nous essayons d'apporter la sécurité. Nous mettons en place une infrastructure de sécurité qui pourrait peut-être prévenir les utilisations malveillantes ou les accidents dont vous entendez parler. Bien sûr, en tant qu'industrie, les industries ne veulent pas que vous en entendiez parler et nous voulons que cette infrastructure sous-jacente fonctionne. Lorsque vous prenez votre appareil, vous pouvez aller sur n'importe quel site et cela fonctionne. Vous n'avez pas à y penser.

Nous développons cette couche de sécurité au-dessus de tout cela. Nous devons être sûrs qu'elle soit bien faite. Il faut aussi savoir et avoir conscience du fait que l'infrastructure entière des noms qui est sous notre mandat est derrière cette infrastructure de sécurité, cette couche de sécurité. Si cela n'est pas bien fait et que l'on n'a pas accès au résolveur, si on n'a pas accès à tous ces éléments, c'est un problème. Nous veillons beaucoup à cela.

Vous avez parlé de Meta, vous avez parlé du mois d'octobre 2022 quand Facebook n'était pas disponible pour toute une journée. La cause en était le DNS. On dit toujours que quand l'Internet ne fonctionne pas, c'est la faute du DNS. Meta avait une configuration intéressante. Dans ce sens, pour l'accès physique au développement et pour accéder à un centre de données, allez au serveur Facebook, ils utilisent des données. Tout est quand même lié au système du DNS. Pour authentifier qui vous êtes, vous utilisez le DNS pour trouver les registres où les informations sont déposées.

Mais il y a un conflit entre les deux, il y a eu un effet cascade et le DNS n'était pas disponible. Quand vous essayiez par exemple d'ouvrir une porte, il fallait vous identifier. Mais vous n'avez pas accès au DNS. C'était le problème. C'est une façon un peu créative de ventiler les choses. Mais je pense que ce qu'il faut comprendre en général, c'est que lorsque l'on développe une infrastructure, que ce soit du business ou un logiciel gigantesque que tout le monde utilise, il faut toujours parler de l'interaction entre le routing, les autorisations, les authentifications et le DNS, et ne pas seulement construire des silos ou des îles desquelles on ne peut pas s'évader. Je pense que tout le monde a beaucoup appris de cette situation.

JOHN CRAIN : Dans cette réunion, vous pourrez peut-être trouver des gens qui font partie de Meta, peut-être leur parler et savoir ce qu'ils en pensent.

SIRANUSH VARDANYAN : Pour l'interprétation, parlez à un rythme raisonnable.

Nous avons une question de Shannelle McPherson, NextGen de l'ICANN76. Elle n'a pas pu venir au dernier moment. C'est une question pour John Crain qu'elle nous envoie : « Comment le DNSSEC est déployé ? Et comment l'ISP d'un pays peut être inclus dans la mise en œuvre du DNSSEC ? »

JOHN CRAIN : Tout d'abord, Shannelle, je suis désolé que vous n'ayez pas pu venir. On verra peut-être dans l'avenir. Continuez à essayer de venir aux réunions de l'ICANN et nous vous verrons la prochaine fois. En attendant, je vais passer la parole à Kim pour qu'il puisse parler de l'établissement des choses à la racine. Ensuite, je vais demander à David de nous parler de travail qu'ils font pour l'engagement du DNSSEC.

KIM DAVIES : Merci John.

L'une des fonctions de l'IANA, c'est la gestion de la zone racine du DNS. C'est la partie critique du DNS. C'est la première chose qu'on fait pour trouver une adresse. C'est quelque chose qui a autorité pour savoir quels sont les domaines de premier niveau qui existent. Notre responsabilité, en partie, comprend la gestion des clés cryptographiques qui sécurisent la zone racine pour le DNSSEC. C'est quelque chose d'assez complexe ; beaucoup de nos opérations et beaucoup de ressources sont consacrées à cette fonction. La raison à cela est simple : le DNSSEC fonctionne avec une clé essentielle, c'est ce qui lance le processus DNSSEC. Il est donc essentiel que cette clé reste dans un état sécurisé et que tout risque d'accès non autorisé soit évité.

Comment procédons-nous ? Nous maintenons la sécurité de cette clé, c'est notre responsabilité. Nous avons quelques installations très sécurisées. À plusieurs reprises au fil des mois, nous faisons des cérémonies, notamment des cérémonies intitulées « cérémonie de clé ». Le public peut surveiller ce que nous faisons et on peut recevoir la confirmation que l'ICANN suit les procédures sécurisées afin que ce ne soit pas utilisé de façon non autorisée.

C'est un aspect essentiel de nos processus opérationnels. Je pourrais vous en parler plus longuement car c'est très intéressant, mais voilà notre responsabilité fondamentale. C'est vrai pour l'IANA et aussi pour l'ICANN concernant la sécurité du DNSSEC.

Mais je note que la question était à propos d'un ISP dans le contexte du DNSSEC.

DAVID HUBERMAN : L'équipe de Kim a fait un très bon travail et maintenant, nous devons savoir comment utiliser ce processus. Nous devons voir ce qui peut être fait pour les domaines de premier niveau, notamment pour .com, .org, .museum. Au Mexique par exemple, tout domaine est sous le TLD .mx. Il y a un registre où l'on peut obtenir la validation DNSSEC pour tous les domaines qui se trouvent dessous.

Je regarde l'auditoire, je vois mon collègue Nicolas. Il vit en Uruguay en Amérique du Sud et voici ce qu'il fait : il va dans différents ISP, chez différents opérateurs de registre TLD et il leur apprend comment les choses fonctionnent, il leur donne des informations sur les outils

nécessaires pour maintenir leur processus et il fournit des informations sur la validation des signatures.

L'ICANN travaille au niveau racine pour faire en sorte que tout soit validé avec des clés. L'ICANN travaille aussi avec les ISP et avec les opérateurs de registre pour faire en sorte qu'ils aient toutes les informations, tous les outils et tout le soutien nécessaire pour fournir le DNSSEC au niveau suivant.

SIRANUSH VARDANYAN : Merci.

Merci Betty.

Olivier et ensuite Firuz.

HERVÉ HOUNZANDJI : Je voudrais m'exprimer en français, s'il vous plaît. Merci.

Je suis Hervé Hounzandji, je suis administrateur système. Je gère le serveur Linux. Je suis président d'ISOC Bénin même si je vis en France. Ma question va concerner les ccTLD. En fait, je m'intéresse beaucoup à tout ce qui est DNS. Je donne même des formations en Afrique sur la manière installer et sécuriser des serveurs DNS.

Je disais que ma question concerne les ccTLD parce que, comme vous le savez, dans beaucoup de pays, le registre ccTLD est choisi et c'est souvent une décision gouvernementale et on a remarqué qu'il y a beaucoup de registres qui gèrent des ccTLD. On va dire quoi ?

[inaudible] que les ccTLD sont mal configurés ou mal gérés, mal administrés. Enfin, il y a plusieurs choses à dire.

Mon problème, c'est qu'est-ce que – et est-ce que c'est possible déjà… Pourquoi l'ICANN ne peut pas faire un audit de tous les ccTLD ? C'est possible ? Et mettre la contrainte pour dire : « Voici ce que vous devez faire » pour que tout le monde soit en règle. Vous savez, il y a encore aujourd'hui beaucoup ccTLD qui n'ont pas implémenté le DNSSEC sur leur ccTLD. Qu'est-ce que l'ICANN peut faire ? Je voudrais que l'ICANN force les gens.

Je prends un exemple. Vous lancez un audit sur certains ccTLD, vous leur dites : « Vous n'êtes pas à jour, vous n'êtes pas OK, on ne peut pas continuer avec vous. Si vous n'avez pas les moyens, on va vous envoyer quelqu'un pour faire un audit. On va vous imposer des choses. Vous allez vous mettre à jour. » Parce que si les ccTLD européens ou américains sont sécurisés et que les ccTLD africains ne sont pas sécurisés, vous voyez, on a dit que la devise de l'ICANN c'est « un monde, un Internet », il ne faut pas qu'on ait un monde et plusieurs Internet. Voilà ma question.

Merci.

JOHN CRAIN : J'ai subdivisé ceci en deux parties. Tout d'abord, il y a une question concernant l'environnement ccTLD et vous avez fait des commentaires intéressants, mais j'aimerais bien discuter de cela avec vous séparément. J'aimerais voir quelles sont les données que vous avez à votre disposition car en tant que scientifiques, nous aimons beaucoup

les données. Vous avez parlé en gros de la qualité des infrastructures et si vous avez des données pour étayer ce que vous dites, ce serait très intéressant.

Vous avez dit par exemple que beaucoup de ccTLD ne sont pas conformes. Je crois que c'est un jugement peut-être par ce n'est peut-être pas forcément toujours le cas. Il y a peut-être une question de politique moins technique sur la gestion des ccTLD. Les ccTLD n'ont pas de politiques régies par l'ICANN. Ce sont des extensions géographiques qui ont des mécanismes dans les pays. Il n'y a pas de mécanisme de l'ICANN pour imposer une politique.

Ce que nous faisons, c'est d'établir une collaboration avec beaucoup de ccTLD. Les forums comme l'ICANN sont des forums où vous pouvez parler des politiques de ccTLD et c'est dans ce cadre que les ccTLD se rassemblent et se réunissent pour en parler. Il y a une journée Tech dans la plupart des réunions de l'ICANN. Il y a beaucoup de collaboration entre les ccTLD et l'ICANN et en particulier avec mon personnel pour améliorer les choses. Mais je crois qu'un audit exigerait qu'il y ait un processus qui soit approprié. Ce n'est pas le cas à ce stade, l'ICANN ne s'approprie pas ce processus. Il n'est pas possible pour l'ICANN d'imposer un audit. Conformément à la façon dont les politiques sont établies, ce n'est peut-être pas possible.

KIM DAVIES : Oui, je crois que c'est un bon résumé. Je crois qu'il faut à nouveau souligner la différence entre un domaine générique de premier niveau et un ccTLD. Pour le gTLD, la politique consiste à fixer des règles et des

exigences pour le fonctionnement d'un gTLD. Le travail de l'ICANN, une fois que les règles ont été décidées par la communauté, c'est de mettre en œuvre ces règles et d'assurer un suivi. L'ICANN a un département et chaque opérateur de gTLD doit remplir certaines conditions. Si cela n'est pas le cas, au bout d'un certain temps il y a des remèdes.

Il me semble que vous recherchez un arrangement de cette sorte pour les ccTLD, mais la relation avec les ccTLD est différente. Au tout début du DNS dans les 1980, une décision a été prise et elle est toujours en vigueur. Les ccTLD sont toujours régis par leur pays. Il faut trouver quelqu'un de confiance, un fiduciaire au sein de ce pays qui pourra opérer pour le bien du pays. Dans le pays, il pourrait y avoir tous les mécanismes de suivi et de contrôle pour faire en sorte que les ccTLD assument leurs responsabilités. Les différents pays ont différents mécanismes à cet effet.

Nous pouvons promouvoir les meilleures pratiques pour renforcer les capacités et informer les responsables de ccTLD sur leurs responsabilités et ce qu'ils peuvent faire pour remplir leurs obligations. Mais les ccTLD sont gérés dans les pays, les opérateurs n'ont pas le contrôle complet, mais ils ont la responsabilité au niveau local de la gestion de ccTLD. Donc, nous avons des limitations en ce qui concerne les ccTLD.

Merci.

SIRANUSH VARDANYAN : Merci.

Nous prendrons encore une question dans la salle et ensuite sur Zoom et nous donnerons à Kim l'occasion de faire sa présentation. Puis, nous passerons à la séance de questions et réponses.

OLIVER RISTESKI : Bonjour, je m'appelle Oliver. Je travaille pour le centre de la recherche sur la sécurité.

Nous avons reçu des e-mails dans les écoles, les aéroports, les centres commerciaux et les transports concernant des alertes à la bombe. Ceci exige un déploiement de ressources considérable pour notre ministère et nous avons une efficacité très faible en termes d'enquêtes sur ce type de crime. Ce scénario se reproduit dans les Balkans. Est-ce qu'il y a des possibilités de mener des recherches dans ce domaine ?

JOHN CRAIN : On dirait que vous parlez des logiciels malveillants. Nous pouvons mener des recherches dans ce domaine, surtout quand cela se rapporte au DNS.

SAMANEH TAJALI : Merci pour votre question.

Comme John l'a dit, c'est un problème assez typique qu'ont la plupart des utilisateurs d'Internet. Dans notre groupe SSR, nous menons des recherches qui seront bientôt publiées pour l'identification de méthodes pour classer ces e-mails malveillants, etc. Continuez à consulter nos publications. Nous allons publier une méthode une fois

qu'elle aura été examinée par nos pairs, notamment dans d'autres domaines.

JOHN CRAIN : Il y a d'autres choses auxquelles vous pouvez penser. Au niveau national, si vous avez des CERT, nous avons un forum. Essayez de vous impliquer dans cette communauté de personnes qui répondent aux incidents. Nous parlons de tout ce qui a trait à l'hameçonnage et aux pourriels.

En ce qui concerne les recherches, les ripostes en cas d'incident, il y a beaucoup de choses que vous pouvez faire. Si vous vous intéressez principalement à la sécurité publique de l'utilisation de l'Internet et si vous souhaitez vous impliquer dans la politique dans ce domaine, nous avons un comité consultatif gouvernemental et nous avons aussi un groupe de travail de sécurité publique. Si votre gouvernement participe au GAC, le Comité consultatif gouvernemental, si votre gouvernement s'intéresse à cette participation, à l'ICANN nous avons donc un travail qui est fait sur les menaces techniques, sur les utilisations malveillantes.

Beaucoup des menaces sur Internet ne sont pas liées au travail que nous faisons. Mais ce sujet est toujours un sujet très chaud à l'ICANN. Et actuellement, il y a beaucoup de choses qui se passent au sein de la communauté, il y a des négociations de contrats qui se déroulent sur ce que veut dire être un opérateur de registre, un bureau d'enregistrement. Actuellement, les contrats stipulent que vous devez recevoir des rapports, vous devez mener des enquêtes. Ce n'est pas la

formulation exacte des contrats, je ne suis pas avocat, mais ce qui manque dans notre formulation contractuelle, c'est qu'il faut atténuer l'utilisation malveillante. Les registres et les bureaux d'enregistrement nous ont dit que nous voulons ajouter ce libellé dans les contrats. Cette discussion est en cours, nous faisons beaucoup de formations, nos groupes font beaucoup de recherches et émettent des publications dans ce domaine.

Si vous avez des forces de l'ordre qui s'intéressent à ces sujets, nous avons des membres de notre personnel qui interagissent beaucoup avec les forces de l'ordre de plusieurs pays. Nous expliquons comment notre écosystème fonctionne et parfois, il s'agit simplement de développer la confiance entre les différentes parties. C'est très important.

N'hésitez pas à venir nous trouver. Nous pouvons échanger avec vous pour savoir comment votre ministère et votre gouvernement pourront s'impliquer.

SIRANUSH VARDANYAN : Merci.

Je voudrais demander à l'équipe technique s'ils peuvent mettre la présentation de l'IANA à l'écran.

En attendant, il y a des gens à distance qui veulent poser des questions. Ce nouveau participant veut savoir : « Comment ce projet d'atténuation et ce programme d'atténuation contre l'utilisation malveillante peuvent interagir les uns avec les autres ? »

JOHN CRAIN : Combien de temps avons-nous pour cela ?

Si vous regardez le mandat initial de l'ICANN, si vous étudiez les statuts et les objectifs de l'ICANN, il est dit que nous devons veiller à la sécurité et à la résilience du système d'identificateurs. Ce ne sont pas les sites Web des gens.

INTERPRÈTE : L'interprète s'excuse, mais il y a une personne qui parle sur Zoom et il est difficile d'entendre l'intervenant.

JOHN CRAIN : En fait, cela correspond un peu à tout ce que nous faisons. Tous les éléments interagissent avec la sécurité. La sécurité est toujours concernée. Nous, en tant que communauté, en tant que personnel de l'ICANN, lorsque nous travaillons sur quelque chose, nous pensons toujours à cela, à savoir quel est l'impact sur la sécurité, sur la stabilité, sur la résilience.

Dans notre groupe – et je vous ai d'ailleurs présenté plusieurs personnes d'IROS–, l'IANA fait son travail de la bonne manière, ce qui est toujours le cas d'ailleurs. Il est très critique de parler de la sécurité. Il faut avoir un bon enregistrement des identificateurs. Nous faisons de la recherche, de la sensibilisation, de l'éducation ; c'est ce que nous faisons. Mais comme l'a dit Kim, nous avons des éléments de conformité par rapport à nos contrats, nous avons des négociations. Nous devons participer à toutes ces discussions sur l'élaboration de

politiques. Tout cela a un effet sur la sécurité, la stabilité et la résilience du système et c'est notre travail, c'est ce que l'on fait.

SIRANUSH VARDANYAN : Kim, puis-je vous passer la parole pour que vous puissiez nous parler du travail de l'IANA ?

KIM DAVIES : En fait, c'est une bonne opportunité de faire une petite présentation sur les fonctions de l'IANA.

Vous avez dû en entendre parler beaucoup durant la réunion de l'ICANN, on en parle souvent, c'est un bref examen des fonctions de l'IANA. J'espère que cela pourra vous aider. Si vous avez des questions par la suite, faites-le-nous savoir et nous pourrons élaborer. Merci.

Nous avons parlé de cela déjà : l'IANA est l'autorité chargée de la gestion de l'adressage sur Internet. Même avec ce nom, nous ne travaillons pas seulement sur les numéros mais aussi sur les noms. Nous travaillons sur plusieurs systèmes d'identification. En fait, c'est l'institution la plus ancienne de l'Internet. Lorsque c'était au départ un projet de recherche, lorsque les premiers nœuds ont été connectés dans les débuts des 1960 et 1970, quelqu'un devait conserver les données de ce que pouvaient faire les ordinateurs. Ceci a été fait par Jon Postel, vous le voyez sur la droite. Jon Postel était vraiment l'IANA personnifié.

L'IANA est devenu un nom qui a été partagé durant les années 1980. Ensuite, c'est devenu non seulement une personne, mais une équipe.

En fait, au début, c'était son objectif et en fait, c'est encore son objectif aujourd'hui : pourquoi utilise-t-on les identificateurs ? Pourquoi y a-t-il un rapport de ce que font ces identificateurs ? C'était dans les années 1990 que les fonctions de l'IANA en particulier et la gestion de la zone racine avaient besoin d'être un peu plus structurées. Il fallait un peu plus que ce qu'un universitaire comme Jon Pastel pouvait faire tout simplement par lui-même et son équipe.

Dans la fin des années 1990, il a fallu formaliser ce projet, reconnaître la commercialisation de l'Internet, sa croissance et la demande énorme qu'il y avait sur les fonctions de l'IANA. L'ICANN a été créé en tant que gestionnaire et opérateur des fonctions de l'IANA. C'était le mandat au tout début et ceci s'appelait le nouvel IANA.

L'ICANN aujourd'hui existe encore avec cet objectif. L'ICANN a des mandats au-delà de l'IANA, mais l'IANA est au centre de la mission de l'ICANN. Le département de l'IANA de l'ICANN gère les registres des identificateurs uniques de l'Internet – je ne dis pas les registres de noms de domaine, mais les registres en général. Chacun d'entre eux a des politiques séparées. Le travail de notre équipe, c'est d'appliquer ces politiques. Cela dépend bien sûr des situations. Lorsque vous entendez le mot IANA, on parle de cette fonction d'allocation et c'est géré par le département de l'IANA à l'ICANN.

Pourquoi a-t-on besoin de quelqu'un qui coordonne les données ? L'Internet n'est pas gratuit ? En fait, les ordinateurs parlent entre eux avec des protocoles techniques. Il est important que tous ces protocoles soient uniformes pour que les ordinateurs se comprennent entre eux. Le contenu est transmis à travers ces protocoles, par

exemple TCP/IP. Ce sont les protocoles qui doivent fonctionner de la même manière sur chaque appareil.

Beaucoup de travail que nous faisons au sein de l'IANA n'est pas seulement à propos des protocoles que vous voyez, comme les noms de domaine, mais aussi des domaines sous-jacents de votre ordinateur pour assurer la transmission entre les différents appareils, pour que cela fonctionne très bien et que ce soit correct pour que les informations soient reçues d'un côté ou de l'autre dans le format correct. Quand vous vous connectez à un serveur par exemple, vous n'allez pas avoir un appel vocal au lieu d'un site Web. Nous essayons de soutenir cette communication et cela est utilisé par les vendeurs de logiciels. Ces gens-là s'assurent que les logiciels peuvent communiquer entre eux sur l'Internet.

Les fonctions sont maintenant exécutées par l'équipe IANA dans le cadre d'une multitude de contrats. Il y a de multiples contrats qui gèrent cette fonction aujourd'hui. En fait, vous connaissez peut-être ce terme, c'est la PTI, identificateurs techniques publics : c'est géré par l'ICANN, c'est une filiale de l'ICANN et ils gèrent les fonctions de l'IANA. Ce n'est pas forcément une distinction qu'on a besoin de connaître. En 2016, lorsque l'ICANN a vu la transition pour la supervision de l'IANA, l'IANA a été mis sous un différent chapeau, sous différents registres de l'ICANN. L'ICANN gère l'IANA. Ne vous tracassez pas trop de ce mot PTI, c'était le nom qu'on utilisait auparavant.

De façon journalière, nous fonctionnons comme les autres départements de l'ICANN. Nous avons environ 16 personnes qui fournissent des services. Quelles sont les fonctions en un peu plus de

détails ? En fait, nous avons trois sections : les paramètres du protocole, les ressources de nombre et les noms de domaine. C'est une distinction peu arbitraire, il y a un peu de chevauchement entre ces segments, mais pour une discussion à haut niveau, cela fonctionne à peu près bien de faire cette division en trois thématiques.

En premier, je vais me concentrer sur les paramètres de protocole. C'est vraiment l'aspect fondamental de nos fonctions. Les paramètres de protocole, il y en a des milliers. Il y en a même des centaines de milliers ou plus, des assignations de protocole d'Internet. Il y en a dont vous n'avez jamais entendu parler. Il y en a que je ne connais même pas. Il y en a énormément et il y en a qui sont utilisés pour des applications très spécifiques.

Si vous créez un logiciel pour une chose spécifique, vous n'avez même pas besoin d'utiliser certains d'entre eux. Pour les cinq, 10, 15 personnes qui travaillent dans cette industrie spécifique et qui développent des logiciels, sachez que le travail de l'IANA est absolument nécessaire. Il y a un index si vous le voulez, iana.org/protocols, et il y a des tas d'informations sur cela.

Pour les paramètres des protocoles, l'IANA joue un rôle direct par rapport aux développeurs de protocole, aux utilisateurs finaux. Vous pouvez venir à l'IANA et communiquer avec notre équipe pour obtenir les informations et les ressources nécessaires. Ce qui nous distingue des autres organisations, c'est qu'en fait les gens ne vont pas forcément vers nous pour obtenir un nom de domaine ou des ressources numériques. Au lieu, ils ont un système d'attribution où il y a des personnes, des intermédiaires, des personnes avec différentes

responsabilités. En fait, nous ne sommes qu'une petite partie du système d'attribution. La raison pour cela, c'est qu'il y a beaucoup de politiques à appliquer pour les autres organes.

D'où viennent ces protocoles ? En fait, ils sont développés au sein de l'IETF. C'est l'organe qui régit les projets Internet. La plupart des décisions sont prises à ce niveau-là. Il y a des standards qui sont développés au sein de l'IETF, vous avez peut-être entendu parler des RFC. C'est une série de documents où l'on publie les standards de l'Internet. Beaucoup de ces RFC se préoccupent des registres de l'IANA et créent les instructions pour les fonctions de l'IANA et les politiques qui doivent être appliquées.

On va parler un peu des ressources de numéro. Pour ceux qui ne connaissent pas bien, ceci fait référence à trois choses clés : les protocoles, les adresses et les numéros. Pour ceux qui ne connaissent pas les adresses IP, il y en a deux soit les IPv4 et les IPv6 ; ce sont les numéros qui sont attribués à tous les appareils liés à l'Internet – téléphone, télévision, ordinateurs, etc. Beaucoup d'objets maintenant dans le monde ont des IP. C'est un identificateur qui est utilisé pour transmettre des données entre les appareils. Quand la transmission est faite sur l'Internet, chaque transmission doit avoir une adresse « de » et « à ».

Lorsqu'il y a des milliards d'adresses, on a besoin de les agréger dans un ensemble général pour que ce soit plus facile à gérer, pour que les ingénieurs ne tapent pas toujours les adresses IP individuellement. Ceci est fait avec des numéros AS et c'est un peu comme des codes postaux pour l'Internet. Il y a des ensembles qui sont regroupés sous un simple

numéro, un numéro AS, et lorsqu'ils discutent de l'envoi de trafic sur l'Internet, ils utilisent ces numéros pour se faciliter la tâche.

J'ai parlé de l'IPv4. Nous n'en avons plus. Nous avons déployé la dernière adresse IPv4 il y a des années. Les RIR n'en ont certainement plus. Il y avait très peu d'IPv4. Il y avait une initiative pour aller de IPv4 à l'IPv6 et l'IPv6 est en pleine expansion.

J'ai mentionné les registres Internet régionaux. Vous ne venez pas directement à l'IANA pour une adresse IP. En tant qu'utilisateur final, on vous donne une adresse IP par un registre Internet régional. On vous attribue une adresse par appareil. Chaque fournisseur, que ce soit votre ISP ou le réseau de votre hôtel, a un ensemble d'adresses IP qu'ils partagent avec les personnes qui sont là.

Où obtiennent-ils leurs blocs ? Ils vont vers les registres Internet régionaux. Il y en a cinq. LACNIC est le registre pour Mexique ici, pour l'Amérique latine. Pour chacun d'entre eux, leur travail est d'attribuer les adresses IP dans leur région. Les RIR, à leur tour, reçoivent leurs attributions de l'IANA.

Dernièrement, les noms de domaine. Parlons des noms de domaine. Attendez, je vais y passer. Voilà la hiérarchie. Dans la hiérarchie, la pièce critique est la zone racine. C'est la base de ce que nous faisons à l'IANA. Vous voyez, il y a la racine qui est en haut sur ce diagramme à l'écran. Ensuite, vous avez le premier niveau, le deuxième niveau, etc.

Après, notre responsabilité principale, c'est l'administration de la zone racine du DNS. Ce sont les données des noms de premier niveau. Nous avons aussi des informations d'administration, des informations de

contact, des contacts de ces compagnies qui gèrent les TLD, etc. Nous avons un registre de ces informations. Nous recevons des demandes d'ajout de ces opérateurs et de modifications des TLD. Nous faisons la maintenance, nous nous assurons que ces requêtes soient bien faites. Nous nous assurons que toutes ces demandes soien t appropriées. Nous envoyons ces informations pour implémentation dans la zone racine.

Je l'ai mentionné tout à l'heure après que l'on m'a posé une question sur le sujet, nous gérons la clé de signature. Nous faisons cela à travers une cérémonie. Nous le faisons de façon publique pour promouvoir la confiance. Nous pourrions faire tout ce travail pour le DNSSEC et la sécurité d'Internet en privé et dire : « Nous sommes l'ICANN, faites-nous confiance », mais la meilleure chose à faire, c'est de vous amener dans le processus, qu'il y ait encore de la visibilité, un accès de la communauté pour mieux promouvoir la confiance. Tout le monde peut voir ce que nous faisons exactement. Il y a des experts de la sécurité du monde entier qui peuvent ainsi voir ce que nous pouvons observer et ce que nous faisons. Ainsi, nous pouvons démontrer que les choses soient faites d'une bonne façon et nous attirons ainsi la confiance.

D'autres fonctions que nous avons. Nous sommes opérateur de .int et c'est juste pour les organisations intergouvernementales. Ce n'est pas disponible pour le public. Nous sommes aussi gérant de .arpa. Ce n'est pas quelque chose que vous verrez directement, mais c'est un peu pour notre plomberie technique. Ensuite, nous avons des ensembles de règles de génération d'étiquettes ; c'est là où les registres partagent leurs pratiques en matière de langage IDN.

Voilà, c'est un peu le résumé, l'ampleur du travail de l'IANA. C'est une description un peu à haut niveau, mais je voulais terminer en parlant de la sécurité. Attendez, on va passer à autre chose. Passez cette diapositive à l'écran, passez à la prochaine.

Sous-jacent à tout ce que nous faisons, nous avons l'impartialité et la neutralité. Nous sommes là pour mettre en œuvre les politiques telles qu'elles ont été écrites. Nous pouvons ainsi fournir un avis qui est neutre. Nous nous focalisons aussi beaucoup sur la performance, nous utilisons des paramètres pour mesurer ce que nous faisons, c'est essentiel. Nous voulons continuer à nous améliorer, bien sûr. C'est une partie de notre travail. Aussi, nous avons des audits internes et en général, nous essayons d'avoir une certaine responsabilité vis-à-vis de la communauté. Vous allez en savoir un peu plus sur ce sujet quand vous serez un peu plus confiants avec l'espace l'ICANN.

Encore une fois, l'IANA gère les registres des systèmes de numéros uniques qui assurent l'interopérabilité de l'Internet. La plupart des registres de l'IANA sont simples et ne sont généralement pas visibles pour l'utilisateur final. Certains sont très complexes. On a parlé de la clé qui la protège la zone racine. Pour cela, sachez que l'IANA est un peu la racine mondiale pour tous ces systèmes. Voilà un petit peu ce en quoi retourne l'IANA.

SIRANUSH VARDANYAN : Merci Kim pour votre présentation. Pour les participants, si vous voulez voir cette présentation, elle se trouve sur le site de l'ICANN sous le titre de cette séance sur l'agenda. Si vous la voulez, vous pouvez aller la voir.

Nous avons le temps de prendre quelques questions. Il nous reste encore 30 minutes pour cela. Si vous voulez bien, allez-y.

FIRUZ AZIMOV : Merci. Bonjour, je m'appelle Firuz. Je suis boursier de l'ICANN. J'ai deux questions.

La première porte sur les problèmes de Meta. Il y a eu des problèmes relatifs à Meta. Meta subnet a été annoncé par un autre ISP. Dans notre pays, nous avons eu un problème : notre subnet alloué au DNS a été annoncé par un autre ISP pour tous les utilisateurs. Est-ce qu'il y a des solutions pour prévenir ce type de problème ? Il faut que le RPKI check soit activé. Est-ce que nous pouvons créer de la stabilité dans les couches inférieures, par exemple dans la couche 3 ?

JOHN CRAIN : C'est une discussion séparée sur la sécurisation du routing. Je vais donner la parole à David.

DAVID HUBERMAN : Le RPKI aide avec ceci. Le problème que vous décrivez se produit plusieurs fois par jour. Et nos amis à la société de l'Internet ont établi un observatoire pour observer ces évènements. Ils mesurent de 500 à 1 000 situations de cette sorte. Parfois, c'est malicieux, parfois c'est quelqu'un qui souhaite simplement semer la pagaille et parfois, ce sont des accidents. Depuis de nombreuses années, les ingénieurs de l'Internet saisissent à la main des configurations dans les routeurs, ils sont humains donc des erreurs se produisent. Quand vous faites une

erreur dans un routeur, cela peut être très mauvais. Le RPKI est une infrastructure qui permet d'être utile lorsqu'il y a une erreur humaine.

Ce que j'aime du RPKI, c'est qu'il ne faut pas forcément valider les annonces ; ce sont les gros réseaux de transit qui doivent faire cette validation. Par exemple, nous sommes à Cancún et nous sommes en communication avec Facebook en Californie ou avec autre chose au Venezuela. Tous ces paquets auront une centaine de chiffres par exemple. Par exemple, si ces 800 fournisseurs valident et signent les routes et rendent non valide ce qui n'est pas valable, cela peut remédier au problème.

Nous avons requis une adoption à 100 % sur les 800 ISP du monde. Si vous régissez une série de réseaux, il est important que ces réseaux émettent des certificats, ces autorisations d'origine de route, pour que tout puisse être validé.

Pour complètement sécuriser nos communications, il nous faut non seulement un RPKI, mais il faut aussi valider le chemin. C'est un paquet qui, lorsqu'il va vers sa destination et revient, passe par une série de réseaux intermédiaires. Il faut que ce chemin soit validé en tout temps afin que quiconque ne puisse pas subtiliser ce paquet pour en faire un usage malveillant.

La communauté des ingénieurs informatiques continue de travailler à ces solutions. Ce sera donc notre étape suivante de sécurité.

SIRANUSH VARDANYAN : Merci.

Nous passons ensuite à Nicolas.

[ORATEUR NON-IDENTIFIÉ] : Bonjour à tous. Je suis Daniel de NIC Costa Rica. NIC Costa Rica est responsable des TLD principalement au Costa Rica.

Je voudrais savoir si l'ICANN déploie des efforts pour forcer la mise en œuvre de politiques pour l'utilisation du DNS ou TLS plutôt que du DNS sur HTTPS ? Que vont faire l'IANA et l'ICANN concernant les questions de sécurité de routage ?

JOHN CRAIN : La première question est simple. La réponse est non car cela ne fait pas partie de notre cahier des charges. Nous étudions ces choses et nous nous y intéressons. Nous avons beaucoup de discussions dans d'autres domaines concernant l'efficacité. Si vous effectuez des recherches, si vous regardez les paquets DNS, vous pourriez délibérer si c'est bon ou si c'est mauvais. Je ne connais pas la réponse. Il y a toujours une tension entre la sécurité et la confidentialité des données. Nous n'avons pas, je pense, une position officielle sur DoH. Je ne sais pas si nous pouvons avoir une réponse.

MATT LARSON : Paul Hoffman dans l'équipe de recherche a contribué à des recherches sur les questions de normes. Nous avons contribué à élaborer des normes.

Compte tenu de l'augmentation de l'intérêt pour les questions de confidentialité, ces protocoles vont continuer à être élaborés, mais il y a davantage d'intensité en ce qui concerne tous les calculs qui doivent être faits.

En ce qui concerne les connexions TCP, il y a davantage de connexions. Mais quand on souhaite ajouter de la cryptographie, les interactions commencent à être plus complexes. Les fournisseurs répondent à beaucoup de questions et ils se demandent ce que cela va avoir comme conséquences sur leur infrastructure. S'il faut établir des connexions et agir au niveau de la cryptographie, les questions deviendront plus complexes. Mais au sein de notre industrie, nous pensons que nous nous dirigeons vers cela, vers une augmentation de ces protocoles.

SIRANUSH VARDANYAN : Merci.

Nous prenons une question de Nicolas et ensuite, David va nous présenter KINDNS.

NICOLAS FIUMARELLI J'ai participé virtuellement précédemment. Est-ce qu'il y a des efforts pour intégrer la cryptographie au DNS ? Est-ce que nous pouvons inclure des algorithmes dans d'autres protocoles ? L'équipe de la PTI, qu'est-ce qu'elle pense faire pour prévoir cela ? Et comment pensez-vous résoudre ces problèmes pour la sécurité et la stabilité de l'Internet ?

KIM DAVIES : Merci pour cette question.

À ce stade, nous n'avons pas de cryptographie post-quantum activement sur dans notre plan, mais nous pensons changer l'algorithme cryptographique dans la zone racine. Nous n'avons jamais changé cet algorithme et nous ne savons pas si cela sera facile ou difficile. Nous avons sollicité notre équipe de conception qui va se réunir dans 15 jours pour en délibérer. Le but de cette équipe de conception, c'est de savoir comment on peut changer l'algorithme dans la zone racine, qu'il s'agisse de la cryptographie post-quantum ou elliptique.

Nous en sommes à ce stade. Il est prématuré de parler de la cryptographie post-quantum. Nous y pensons. Mais en ce qui concerne les activités qui se déroulent, je vais donner la parole à Matt pour parler des activités de recherche. Je pense que c'est plutôt une activité qui est en cours de recherche.

MATT LARSON : Merci Kim.

C'est l'occasion pour moi de parler de la série de documents de l'OCTO. Nous avons rédigé un document, je ne peux pas vous le montrer, mais c'est OCTO-031. La cryptographie post-quantum suscite beaucoup d'intérêt. L'OCTO a donc demandé une recherche et nous avons demandé la rédaction d'un document. Il y a un document général, OCTO-031, qui nous donne un état des lieux de l'industrie de la cryptographie post-quantum. Nous avons encore un long chemin à

parcourir car nous sommes encore très loin d'un ordinateur quantum qui puisse menacer les algorithmes que nous utilisons actuellement.

Il y a beaucoup de choses qui se disent dans l'industrie. Si vous lisez les publications, vous vous dites peut-être que le danger est imminent, que le monde va s'effondrer. Nous avons encore des années, sinon des décennies devant nous. Il est encore prématuré de mener des recherches dans ce domaine. Nous avons encore beaucoup de temps car nous sommes encore très loin de cet ordinateur quantum qui puisse être une menace.

SIRANUSH VARDANYAN : Merci Matt. Le lien est affiché dans le chat de Zoom. Vous pouvez le consulter.

Maintenant, je voudrais donner la parole à David pour nous parler du projet KINDNS.

DAVID HUBERMAN : Merci Siranush.

Il nous reste encore quelques minutes et je voudrais vous parler de ce que nous faisons à l'ICANN pour améliorer la position technique de l'Internet.

Je suis allé dîner dans un restaurant avec un ami hier soir, nous avons passé une très bonne soirée et pendant que notre dîner était servi, le serveur a fait quelque chose qui représente probablement un scénario cauchemar pour un serveur : il a renversé ma boisson sur moi et j'étais

trempé. Quand quelque chose comme cela se produit, on peut réagir de plusieurs façons. On peut se mettre en colère : « Qu'est-ce que vous faites ? ». On peut donc faire une scène et là, les choses deviennent difficiles pour tout le monde. Ou alors, on peut ne pas réagir ou on peut adopter une meilleure approche, celle de rire et de sourire et on peut dire : « Pas de problème, l'erreur est humaine » et on peut transformer une mauvaise situation en bonne situation.

Voilà, c'est ce que nous avons fait hier soir, nous avons choisi d'en rire. Pourquoi est-ce que je vous raconte cela ? Parce qu'on peut faire la même chose dans le DNS. Nous pouvons être courtois, être gentils et rendre la vie meilleure pour chacun en menant de bonnes actions. L'ICANN a créé un programme intitulé KINDNS. Ceci est sur notre site Web, kindns.org. Le but de cette initiative, c'est que pour tous les opérateurs KINDNS, que vous soyez un grand ou un petit opérateur, sachent qu'il y a des mesures à prendre pour être plus gentil. Si tout le monde est plus gentil, le DNS on aura une position renforcée et améliorée.

Dans ce projet, vous êtes classé selon votre statut – si vous êtes un petit opérateur, si vous avez un serveur récursif, si vous êtes un résolveur public (public, c'est-à-dire que tout le monde peut l'utiliser), privé – et vous pouvez faire une auto-évaluation en tant qu'opérateur pour voir comment vous êtes évalué par rapport à un ensemble de normes que la communauté technique a établies, des normes que tout le monde doit respecter afin que le DNS soit plus sécurisé et plus sûr.

Il y a ces normes. Vous pouvez voir comment vous vous y conformez et vous avez la possibilité de combler vos lacunes. C'est ce qui a été fait

dans la sécurité du routage chez nos amis de la société de l'Internet. Toute la communauté Internet peut travailler afin de rendre les choses meilleures pour tout le monde par le biais de plusieurs mesures qui sont peu onéreuses et qui ne prennent pas beaucoup de temps. Cela vous permet de savoir où en est votre Internet pour améliorer votre réseau et votre infrastructure DNS. C'est la gentillesse, KINDS. Et vous verrez en termes très simples les normes acceptées par la communauté.

C'est ce que je voulais vous dire. Merci.

SIRANUSH VARDANYAN : Merci David.

Maintenant Mohamed Elnour Abdelhafez du Soudan a une question : « La validation du chemin est essentielle pour le routage. Le BGPsec a cela en vue, donc c'est très difficile en raison des ressources consommées par le BGPsec. Quel est le rôle de l'ICANN dans ce domaine ?

JOHN CRAIN : Nous pouvons jouer deux rôles : l'implication et la participation à la recherche. Je vais donner la parole à David.

DAVID HUBERMAN : Très bonne question, merci.

Je le disais plus tôt, les deux chemins pour une structure sécurisée, c'est le RPKI et la validation. Nous avons déjà une solution qui a été élaborée,

c'est la sécurité BGPsec, mais il faut savoir que les calculs sont tellement énormes que nous ralentirions l'Internet.

Pour l'ICANN et notre participation à l'élaboration de solutions, l'équipe de Matt est impliquée pour établir des processus. Le groupe de travail de génie Internet s'y attelle. Nous pouvons mesurer de façon empirique, de façon scientifique, par le biais de nos interactions avec la communauté. Nous pouvons aussi être un animateur de discussions. Dans la communauté de l'ICANN, nous pouvons voir quels sont les impacts, quels sont les moteurs et quelles sont les motivations pour voir comment les technologies améliorent la situation sur le terrain.

JOHN CRAIN : Je me demande combien de personnes dans cette salle ont participé à la *task force* de l'ingénierie de l'Internet. C'est bien. Si vous êtes des techniciens et que vous êtes intéressés aux protocoles, c'est un endroit intéressant. Si vous n'êtes pas geek, ceci va être compliqué pour vous. Mais si vous êtes un geek, vous allez adorer.

Vous allez être choqués d'entendre cela : l'ICANN ne gère pas l'Internet. Nous ne développons pas l'Internet, nous ne développons pas tous ces protocoles. C'est important de comprendre qu'il y a une communauté d'ingénieurs, des gens qui utilisent l'Internet, qui font cela, surtout au FGI et à d'autres forums, pas seulement ici.

Je pense qu'avec cela, on a fini. Y a-t-il d'autres questions ?

SIRANUSH VARDANYAN : On peut recevoir une autre question. Afifa, je pense que vous avez levé la main, allez-y.

AFIFA ABBAS : Je suis Afifa. Je suis mentor pour les boursiers depuis deux ans. J'ai une question que l'on me pose souvent qui vient des boursiers.

Quand on s'implique à l'ICANN, ces techniciens qui font partie de sécurité de la cybersécurité, souvent, j'ai cette question : si vous vous pouviez nous donner les noms de plusieurs plateformes sur lesquelles ils peuvent s'impliquer, parce qu'il y a des tas de personnes qui sont intéressées par la cybersécurité. Vous l'avez dit, les boursiers de l'ICANN viennent pour cela et nous ne voulons pas les perdre, nous voulons qu'ils soient intéressés. Je suis sûr que l'ICANN ne veut pas les perdre non plus. Comment peut-on utiliser leurs talents dans ce sens ? On parle de la cybersécurité.

JOHN CRAIN : C'est toujours bon de voir les boursiers qui nous reviennent, surtout quand ils deviennent des mentors.

Sachez que l'ICANN n'est pas un forum de cybersécurité, ce ne sont pas nos fonctions. Mais nous faisons un suivi au niveau de la sécurité et nous avons cela sur l'agenda de l'ICANN.

Si vous recherchez des conseils pour savoir où vous pouvez vous impliquer davantage sur ces questions de cybersécurité au sein de l'ICANN, nous avons une communauté qui s'appelle le SSAC, un comité pour la sécurité et la stabilité. Vous pouvez vous impliquer et devenir

membre. Ils cherchent vraiment des professionnels qui sont experts tout de même. Si vous arrivez en tant que boursier et que vous êtes un expert dans la sécurité, il y a des gens qui sont dans l'industrie depuis longtemps et qui sont boursiers, c'est un espace où vous pouvez vous adresser.

Nous avons des journées tech, il y en a plusieurs et il y a beaucoup de discussions liées à la sécurité durant ces journées. Et bien sûr, vous pouvez venir nous parler afin que l'on puisse vous donner des conseils.

Ce qui est important, ce n'est pas seulement ce qui se produit au sein des discussions sur l'élaboration des politiques, c'est ce que nous faisons. Nous élaborons des politiques pour les identificateurs. Il ne s'agit pas là seulement de la sécurité dans le sens de la cybersécurité, mais la chose importante que nous faisons ici dans les réunions, c'est d'interagir avec d'autres personnes dans les couloirs lors des événements.

S'il y a quelqu'un que vous voulez rencontrer par exemple dans votre domaine de la cybersécurité sécurité ou autres, parlez à vos mentors, venez voir quelqu'un du personnel de l'ICANN, d'ailleurs toutes les personnes de la communauté, et posez-leur la question : « Je suis intéressé par un tel sujet. Est-ce que vous pouvez me diriger vers quelqu'un qui est expert en la matière et me présenter à cette personne ? » Il s'agit de travailler ensemble de façon ascendante et pour cela, nous avons tous les membres de la communauté. C'est le meilleur conseil que je peux vous donner.

Nous avons un suivi technique. Quand il s'agit de l'aspect technique, il y a un groupe de travail sur les ccTLD, il y a le groupe RSSAC. Est-ce qu'il y a des gens ici dans la salle des ccTLD ? Est-ce que vous parlez de sécurité ? Vous êtes sur la liste ccTLD ? Vous avez le groupe de la ccNSO qui aussi a des thématiques sur la sécurité. Communiquez avec nous et envoyez-nous les personnes qui posent la question et nous trouverons la personne qui peut les aider. La cybersécurité veut dire tellement de choses pour différentes personnes, mais nous sommes heureux de vous aider.

Sam, d'ailleurs, veut prendre la parole.

SAMANEH TAJALI : Pour ajouter quelque chose à ce qu'a dit John, c'est une question intéressante car souvent nous en parlons mais pas de façon systématique. Nous avions des stagiaires et dans ce sens, nous avions des projets, des petits et des grands projets, et nous n'avons pas parlé de cela en interne. Nous sommes une équipe de recherche, donc nous avons des projets. Nous acceptons toutes ces nouvelles idées et nous avons des groupes opérationnels qui travaillent en interne et en externe. Si vous êtes intéressés par ces projets de recherche ou si vous avez des informations et que vous connaissez des personnes intéressées, envoyez-les vers nous et nous verrons comment les diriger vers la bonne personne.

SIRANUSH VARDANYAN : Je voudrais remercier John, Lars, David, Sam et Kim qui sont venus aujourd'hui. Ils ont un emploi du temps très occupé. Nous les

remercions d'avoir pris le temps de venir nous rejoindre pour que tous nos boursiers et nos NextGen qui sont intéressés à en apprendre plus puissent participer. Vous connaissez ces gens-là maintenant ; si vous les voyez dans les couloirs, posez-leur des questions.

Nous allons fermer la séance. En même temps, soyez gentils les uns avec les autres. Merci. La séance est fermée, nous pouvons fermer l'enregistrement. Merci beaucoup.

JOHN CRAIN : Nous sommes là pendant quelques minutes. Si vous voulez venir nous voir, nous sommes là, venez nous voir.

SIRANUSH VARDANYAN : Pour les NextGen et les boursiers, ne partez pas, restez dans cette salle, nous avons besoin de discuter.

[FIN DE LA TRANSCRIPTION]