ICANN73 | Semaine de préparation – Mise à jour des normes pour le partage de connaissances et l’instauration pour la sécurité du DNS et du nommage (KINDNS)
Mercredi 23 février 2022 – 11h00 à 12h00 AST

ADIEL AKPLOGAN : Bienvenue à cette séance sur KINDNS. L’enregistrement est lancé. Bienvenue à cette séance.

Nous allons vous donner une mise à jour sur cette initiative qui s’appelle KINDNS, ce partage des connaissances et des meilleures pratiques.

Nous avons la traduction et l’interprétation aujourd’hui. Vous pouvez tout à fait utiliser les services d’interprétation. Nous allons parler lentement et clairement pour assurer une interprétation précise et pour que les interprètent puissent faire leur travail.

Utilisez le Q&A pour poser vos questions et vous pouvez également lever la main si vous le désirez et nous vous permettrons ainsi de prendre la parole.

Nous allons donc passer à la diapositive suivante. Nous avons cette présentation en deux parties. Je vais tout d’abord présenter tout cela. Et je vous présenterai ensuite Philip Regnauld qui est un expert sur ce projet qui va vous parler de l’avancée de cette initiative.

Nous avons déjà eu cette séance durant l'ICANN72 où nous avons introduit ce concept de KINDNS. Nous allons donc définir un petit peu cela pour commencer.

C'est instaurer des normes pour le DNS et pour la sécurité du nommage. C'est surtout pour partager les meilleures pratiques avec la communauté, pour s'engager envers les meilleures pratiques, pour promouvoir les meilleures pratiques et s'assurer que nous travaillions ensemble en collaborant pour avoir des normes solides pour le DNS. Nous passons à la diapositive suivante.

Certains sont déjà familiers avec MANRS. Il s'agit des normes sur lesquelles nous sommes mutuellement tombés d'accord pour l'initiative de sécurité de routage. On a des bonnes manières et nous avons également KINDS pour s'assurer que l'internet soit sûr pour tout le monde. Ce que nous essayons d'effectuer ici, c'est d'avoir des meilleures pratiques pour que les opérateurs puissent suivre facilement ces meilleures pratiques pour s'assurer que le DNS est sûr. Ce sont des meilleures pratiques techniques sur les opérations du DNS.

Il y a d'autres services qui tournent autour du DNS comme les applications. Nous allons nous concentrer ici plus précisément sur les aspects techniques. Donc si vous êtes familier avec le DNS, vous savez que nous avons beaucoup d'identificateurs de meilleures pratiques par rapport au bon fonctionnement du système de noms de domaine qui est complexe. Nous essayons de voir ce qui est le plus important pour les opérateurs du DNS, quelles sont les pratiques qui doivent

vraiment être effectuées et sauvegardées pour le DNS. Diapositive suivante.

Nous allons maintenant vous parler de cette initiative, de ces éléments clés. Premièrement, c'est identifier et de documenter les normes de sécurité les plus essentielles pour les opérations du DNS. Cela a trait à l'aide de Phil Regnauld qui va nous parler un petit peu plus tard. Nous avons une liste de diffusion où nous partageons ce qu'il y a de nouveau dans le travail d'identification des normes. Nous avons un retour de la communauté qui est effectué de cette manière. Nous nous basons sur ces meilleures pratiques et nous allons lancer un portail dédié pour publier ces meilleures pratiques, pour fournir des lignes directrices de mise en œuvre et pour que les opérateurs aient un endroit où trouver les informations utiles pour évaluer le bon fonctionnement du DNS et soutenir cette initiative qui sera ainsi promue. Nous voulons publier sur ce site web dédié.

Une fois que nous avons effectué cela, nous allons commencer à travailler tous ensemble pour identifier des opérateurs qui nous permettront de mesurer et d'évaluer l'impact de l'initiative concernant la sécurité du DNS. Nous allons voir le temps s'écoulant ce qui fonctionne bien et si nous allons dans la bonne direction, si nous sommes sur la bonne voie. Ce sera la prochaine phase.

Lorsque nous présentons cela dans un contexte de l'ICANN, nous nous poserons la question suivante : est-ce que cela va avoir trait aux fonctions politiques du DNS pour les registres, pour les bureaux d'enregistrement, pour les titulaires de nom de domaine ? La réponse est non, cela n'a pas d'impact sur les politiques parce que nous

travaillons sur les fonctions essentielles du DNS. Il y aura peut-être une autre phase où nous serons en mesure d'avoir une cartographie de tous ces systèmes, de ces meilleures pratiques et là, ce sera plus important pour les registres et les bureaux d'enregistrement. Mais nous allons nous concentrer d'abord sur la première phase sur les opérations du DNS.

Quelles sont toutes ces catégories sur lesquelles nous allons nous concentrer ? Si vous gérez le DNS, vous êtes dans un environnement où il y a beaucoup d'éléments pour assurer la sécurité du DNS. On ne va pas tout couvrir, mais nous allons nous concentrer particulièrement sur des éléments du DNS, sur les serveurs qui font autorité dans différents environnements, pour les TLD, pour les opérateurs de zone critique, pour les noms de domaine de second niveau notamment. Nous avons les TLD, nous avons la zone critique et les SLD. Nous voyons ce qui est absolument essentiel pour le fonctionnement de ces TLD.

La deuxième catégorie, c'est toutes les personnes qui gèrent des registres de noms de domaine de second niveau. Nous avons également les résolveurs récursifs. Nous avons des résolveurs privés, des résolveurs partagés qui sont privés également et des résolveurs publics. Les meilleures pratiques que nous allons promouvoir vont se concentrer autour de ces cinq catégories, mais nous allons également fournir des informations sur comment renforcer l'environnement opérationnel au niveau des services, des systèmes, des réseaux. Nous allons également prendre en compte le respect de la vie privée et l'impact que cela a sur la sécurité en général.

Mais à cette étape et pour le moment, si vous voulez vous joindre à cette initiative KINDNS, vous allez faire une auto-évaluation au niveau des deux catégories que j'ai mentionnées, soit les serveurs faisant autorité et les résolveurs récursifs.

Nous allons publier bien entendu des lignes de conduite pour la mise en œuvre avec des listes de contrôle, des exemples de configuration, des processus. Sur quels logiciels allons-nous travailler ? Nous allons présenter ces concepts de telle manière qu'ils puissent être utilisés avec tous les différents logiciels qui existent. Diapositive suivante.

Je vais donner la parole maintenant à Philip Regnauld qui va nous parler des différents éléments que nous avons et des différentes catégories dont on a déjà un peu parlé. Philip, vous avez la parole.

PHILIP REGNAULD : Merci beaucoup de m'avoir présenté, merci Adiel.

C'est un projet tout à fait intéressant et j'espère que nous allons avoir un retour de la communauté à ce sujet, sur les différentes meilleures pratiques que nous allons identifier.

Nous avons partagé cela de cette manière. Nous avons fait des catégories avec les types d'opérateurs du DNS. Au départ, nous avons pensé aux TLD, aux SLD. C'était peut-être un petit peu simpliste ou peut-être complexe, donc on a décidé d'utiliser un autre système, les opérateurs faisant autorité pour le DNS et également pour les zones critiques avec l'utilisation de résolveur.

Pour commencer avec les serveurs qui font autorité, nous avons différents types de zones dans l'internet. Et nous avons une certaine hiérarchie. Vous avez la racine qui est absolument critique pour le fonctionnement du DNS et qui ne peut pas être compromise. S'il y a un problème de sécurité au niveau de la racine, c'est très sérieux. Les TLD ont donc un rôle important à jouer.

Mais nous avons également des domaines qui pourraient avoir un rôle à jouer. Si l'on voit les serveurs de différents pays, pour le Danemark, nous avons dk et parfois, il y a un sous-domaine et cela peut poser problème. Ces sous-domaines sont extrêmement importants.

Donc nous avons décidé d'avoir deux catégories : nous avons les zones critiques comme on les appelle et nous avons les zones auxiliaires de soutien qui sont utilisées pour certains ccTLD ou pour des serveurs de nom et d'autres dépendances. Et également, quelque chose de tout à fait à important. Une zone critique, ce n'est pas vraiment en lien avec le fonctionnement du DNS, mais pour les ccTLD, il y a des fichiers de zone qui sont associés à par exemple la gouvernance électronique, au service bancaire, au service de soins de santé et c'est extrêmement important et cela doit tout le temps fonctionner. Ce sont des systèmes par exemple d'identification. Si on ne peut plus s'identifier, par exemple pour le Danemark, cela pose de graves problèmes. Tout cela est en rapport avec une auto-évaluation. Ce sera le modèle qu'on va utiliser et on ne veut pas dicter les zones qui sont critiques ou pas. Il s'agit plus d'un cadre de référence que nous donnons pour identifier les zones critiques pour que les organisations identifient le fait qu'ils

présentent des services critiques ou pas, quelles sont les meilleures pratiques que nous devons observer pour protéger ces services.

Bien sûr, nous avons aussi introduit des aspects financiers et autres qui peuvent être considérés comme essentiels pour le fonctionnement des économies dans ce domaine. Ce sont des décisions que nous avons prises de structurer cela ainsi et d'introduire l'impact que cela peut avoir et ce qui peut arriver si le nom de domaine est affecté avec un problème au niveau du ccTLD. Prochaine diapositive.

Ensuite, nous avons d'autres noms de domaine, tous les autres noms de domaine qui sont en-dessous ou les domaines de premier niveau qui sont aussi critiques qui vont fournir différents services à des sites internet, des sites gouvernementaux, des e-commerces, etc. Donc il faut être aussi responsable dans ce sens. Et ce n'est pas seulement parce qu'on est des domaines de deuxième niveau qu'on a moins de contraintes. En tout cas, il y a des contraintes peut-être moins liées aux meilleures pratiques, mais on peut encourager les personnes à commencer à appliquer cette initiative KINDNS, d'avoir les meilleures pratiques et d'appliquer cela. Et si on a un domaine de deuxième niveau, on ne va peut-être pas avoir autant d'impact sur le reste de la communauté, sur les autres publications, mais on peut quand même être soumis à des attaques cybernétiques ou à des problèmes de système. Donc on peut se demander si on applique ces meilleures pratiques pour atténuer ou se remettre de ce type d'incident. Quelque soit le domaine, je dirais que tout le monde devrait appliquer ce système parce que si un domaine a été piraté, il ne va pas fonctionner, un point c'est tout. Prochaine diapositive.

Nous allons maintenant parler des opérateurs DNS récursifs. C'est l'autre partie de notre écosystème. Lorsqu'on regarde les opérateurs faisant autorité, on a les opérateurs récursifs. Et ici, on va voir un petit peu ce qu'on a.

Il y a deux possibilités : ils peuvent être publics ou privés. Et si on regarde un peu plus dans ces services de résolveurs, il va y avoir des résolveurs publics et privés. Ceux qui sont publics seront fermés, ils ne seront pas accessibles de l'extérieur. Il faudra un accès contrôlé. En général, ce sont des résolveurs qui ne sont pas publics, qui correspondent à des banques, à des services de santé et autres et d'autres réseaux résidentiels ou domestiques.

Un peu plus ouverts, nous avons les résolveurs privés partagés. Je ne voulais pas spécifier ici les fournisseurs de service internet ou autres parce qu'ils sont privés. Ils sont destinés à une série de clients, des institutions universitaires par exemple. Ils ne sont pas accessibles de l'extérieur mais ils peuvent être partagés entre différentes entités qui sont bien déterminées. Cela peut être dans un contexte de service d'organisation fédérée ayant une administration technique commune. Donc ce sera une autre catégorie.

Ensuite, on peut avoir les résolveurs publics. On sait que ce peut être Google ou autre, ce type de service. Mais entre les deux, on a les services DNS qui correspondent au filtrage du DNS commercial.

Je vais essayer de parler un peu plus lentement, excusez-moi.

Pour ces résolveurs publics, nous avons ce que l'on a, comme Google et autres.

Puis, nous avons des résolveurs semi ouverts avec des composantes commerciales, des accords, des contrats qui vont donner des services additionnels pour ces opérateurs de résolveurs pour les servies de DNS pour lesquels on a un trafic qui est analysé pour savoir s'il y a des zones qui sont compromises ou infectées. Ce type d'opérateurs sont publics et ont des mécanismes de contrôle d'accès qui sont contrôlés qui vont permettre de tirer profit des services qu'ils vont fournir. Voilà donc les différentes catégories.

Dans la section suivante, nous allons identifier comment cet accès est restreint pour ces résolveurs et comment l'accès peut se faire avec une adresse IP ou avec des certificats, peu importe ici ce qui fonctionne. Nous essayons de voir quelles sont les catégories, comment elles vont fonctionner pour que l'on sache si cela s'applique à notre cas et pour connaître les meilleures pratiques à appliquer ici.

Il y a des utilisateurs finaux, des organisations, un commerce par exemple, une organisation, une entreprise qui dit : « Je suis connecté à mon fournisseur de service internet. J'utilise ce résolveur, j'ai ce type de requête DNS. Qu'est-ce que je dois appliquer ici ? Est-ce que j'applique vraiment ce qui correspond ? Est-ce que je dois en parler avec mon ISP, avec mon département technique pour savoir si tout le monde applique les bonnes pratiques dans ce domaine de la façon dont nous l'avons décrit ici ? » Prochaine diapositive.

Quelles sont les recommandations pour les résolveurs privés ? Nous avons couvert les recommandations destinées aux résolveurs faisant autorité, mais ici, pour les résolveurs privés, c'est différent. Il y a des réseaux privés et parfois, ils appartiennent à des domaines actifs avec

différents environnements. Nous, lorsque nous travaillons ici, nous nous focalisons sur la sécurité du réseau, nous identifions le besoin de transparence, ce qui signifie que certaines recommandations peuvent s'appliquer dans le cas du DoH ou du DoT. Il y a encore certains réseaux qui ne peuvent pas encore appliquer ces systèmes, mais les bénéfices pour utiliser le DoH ou le DoT, c'est une série de sécurité qui va vous permettre de sécuriser votre réseau. C'est un scénario différent en fonction des opérateurs.

Ensuite, la disponibilité et la résilience des services. Comme cela a été dit, certaines de ces meilleures pratiques vont comprendre les meilleures pratiques d'administration de système. Nous n'allons pas en parler ici, mais tous ces détails, vous les trouverez sur le site internet, dans notre programme. Vous pouvez trouver ce type d'informations.

Et nous voyons la validation du DNSSEC, j'ai oublié de vous le dire, pour les serveurs faisant autorité. Il y a des meilleures pratiques qui sont promues et il s'agit de la signature du DNSSEC. Ici, pour le type de choses qui correspondent aux résolveurs, nous pensons qu'il y a des exigences qui sont la validation du DNSSEC pour ces résolveurs. C'est déjà le cas pour beaucoup de logiciels, mais nous soulignons cela, nous l'avons mis ici en caractères gras parce que c'est important. Cette validation du DNSSEC est très importante.

Ici, les résolveurs privés et partagés : il s'agit d'ISP ou autres avec des exigences similaires, mais il y a quelques différences au niveau de leur clientèle parce qu'ils vont avoir un mélange de portables, câbles, fibre, résidentiel. Il va y avoir parfois le contrôle de l'accès, donc il y a des

problèmes de protection de la vie privée. On doit s'assurer lorsqu'on offre ce type de service DNS qu'on le fait à travers des services privés. Donc on recommande de mettre en place le DoH ou le DoT de façon à ce que vos clients se sentent plus à l'aise et soient sûrs qu'ils peuvent vous envoyer des questions et des préoccupations et pour s'assurer qu'ils vont pouvoir trouver des solutions. Cela ne veut pas dire qu'ils ne peuvent pas aussi trouver des solutions ailleurs, mais ils peuvent vous consulter, ils peuvent utiliser votre système. Ils savent qu'ils ont une bonne solution avec vous comme fournisseur de service internet. Au niveau de la protection de la vie privée, c'est une bonne chose aussi.

Au niveau de la disponibilité et de la résilience des services DNS, il y a beaucoup de recommandations que nous faisons ici que vous trouverez sur le wiki et sur le site internet bientôt. De nouveau, de sont des bonnes pratiques pour le système, une hygiène du système qui est importante et l'on pense que tous ceux qui travaillent dans le domaine de la sécurité du DNS devraient l'appliquer.

Pour les opérateurs de résolveurs publics, ici, nous parlons des grands comme Google et autres, ils ont bien sûr leurs propres manières de travailler, mais je pense que beaucoup d'entre eux mettent déjà en œuvre ces pratiques. Nous avons la validation du DNSSEC par exemple qui est appliquée par les grands, les considérations liées à la vie privée et les systèmes DoT ou DoH ou les deux aussi. Nous avons par exemple le Quad9 ou Cloudflare.

Nous parlons aussi de la minimisation Qname pour éviter les pertes de noms de domaine entièrement qualifiés vers la racine pour s'assurer

que l'on révèle seulement une partie du nom de domaine. Parce que qu'on le veuille ou pas, ces noms de domaine vont être révélés et ils vont divulguer des informations sur nos utilisateurs, sur leurs habitudes, sur ce qu'ils font et ce n'est pas toujours positif. C'est la même chose pour les résolveurs publics fermés pour la question des services de paiement avec des contrôles d'accès : ils vont devoir offrir un système avec une minimisation du Qname, le DoT, le DoH. C'est presque, je dirais, une pratique standard actuellement.

Je ne sais pas si c'est à moi de couvrir cela ?

ADIEL AKPLOGAN : Je peux reprendre la parole.

Nous avons eu un aperçu des différentes meilleures pratiques et de la manière dont ce sera structuré. Notre objectif ici est de nous concentrer sur ce qu'il y a de plus important, donc d'avoir un certain nombre de meilleures pratiques qui se dégagent. Nous ciblons entre sept et 10 meilleures pratiques que l'on puisse identifier pour tout le monde pour que ce soit très clair et que pour que cela ne prête pas à confusion.

Voilà comment cela va être présenté et structuré. Une fois que nous allons lancer cette initiative, il y aura un site web KINDNS.org et l'ICANN va soutenir cette initiative. Si vous êtes intéressé à vous joindre à nous, les informations sont disponibles. Il y aura une séance qui va parler de diverses catégories, Phil a mentionné cela. Pour le soutien et la participation accrue, tout le monde sera bienvenu. Il y aura également des parrains, des ambassadeurs. Nous avons une

séance où nous développerons des outils, où les opérateurs peuvent s'auto-évaluer. Nous verrons quels sont ces outils d'auto-évaluation. Nous voulons que ce soit simple, parce que ce n'est pas du tout une obligation. Il s'agit de quelque chose de volontaire, cet engagement envers ces meilleures pratiques. C'est pourquoi ces outils d'auto-évaluation seront utilisés par les participants et cela leur permettra de répondre à certaines questions.

Nous allons avoir un tableau de contrôle également avec beaucoup d'informations et nous suivrons les identificateurs. Et nous aurons également ces lignes de conduite qui présenteront les meilleures pratiques, qui donneront plus de détails et d'informations sur ces meilleures pratiques. Par exemple, si vous regardez ce qu'a mentionné Philip, vous aviez une diapositive sur la sécurité des systèmes. Cela ne va pas être dans les meilleures pratiques essentielles, mais cela sera souligné néanmoins dans les lignes directrices. Nous pourrons avoir un blog par exemple consacré à cela.

Donc nous travaillons avec ces objectifs en vue d'identification des meilleures pratiques. Nous avons déjà commencé à développer certaines lignes de conduite. Nous avons récemment publié pour le DNSSEC un document des services OCTO, du directeur informatique de l'ICANN. Cela est en rapport avec cette initiative KINDNS. Nous allons passer maintenant à la diapositive suivante.

Nous avons un contrat pour le développement d'un nouveau site web. Voilà un exemple de site que nous sommes en train de développer. Nous ne sommes pas encore arrivés à la version finale au niveau de la présentation du site web. Cela va ressembler à cela, kindns.org.

Le calendrier maintenant. Nous avons dû l'ajuster un petit peu depuis que nous nous sommes parlés depuis la dernière présentation. Évidemment, la situation a beaucoup changé pour nous tous, mais nous espérons lancer à ce trimestre de 2022, à la fin du mois de mars, le site web, peut-être pas avec toutes les fonctions, mais nous allons lancer les fonctions essentielles. Cela va nous permettre d'avancer, cela va permettre aux opérateurs de travailler sur cette initiative.

Nous allons tenir la communauté au courant de l'avancée de notre travail. Et nous recommandons que vous vous joigniez à la liste de diffusion, tout le monde est le bienvenu. Vous pouvez dès à présent contribuer. Vous avez cela à l'écran. Nous avons également une page wiki temporaire où nous publions des documents préliminaires en attente du site web formel. Ensuite, on transitera de la page wiki au site web avec toutes ces informations.

C'était la dernière diapositive. J'aimerais vous remercier de votre attention. Nous espérons que vous allez nous poser des questions, effectuer des suggestions et que nous allons pouvoir continuer la discussion.

KINGA KOWALCZYK : Nous avons une question. Est-ce que vous voulez que je lise cette question.

ADIEL AKPLOGAN : Oui.

KINGA KOWALCZYK : Nous avons une question de Sivasubramanian Muthusamy : « Est-ce que KINDR développerait un engagement commun, pas envers un seul résolveur mais maintenir des résolveurs redondants et multiples que tout le monde peut utiliser ? C'est un scénario qui n'est pas très clair. Par exemple, les universités qui bloquent ses étudiants par rapport à l'utilisation de résolveurs externes ou le maire d'une ville qui insiste pour que tout le monde dans la ville n'utilise pas le résolveur de la ville. Il s'agit d'engagement et de meilleures pratiques. »

ADIEL AKPLOGAN : Oui, ce sont des scénarios intéressants. Et c'est tout à fait pertinent, ce genre de questions. C'est pour les utilisateurs, c'est important et c'est en rapport avec les politiques. Ce sont des décisions de politique. Lorsque quelqu'un demande à des clients, à une communauté d'utiliser un certain service, oui, c'est quelque chose qui est important. On ne contrôle pas beaucoup ces choses.

Pour les titulaires de noms de domaine, c'est un autre point de vue. Vous pouvez avoir plusieurs résolveurs dans votre installation. Donc je pense que pour la gestion des réseaux, c'est une bonne chose. Il s'agira là de meilleures pratiques. Mais nous ne sommes pas concentrés sur cet aspect précisément parce que c'est plus pour les utilisateurs de nom de domaine et au niveau des prestataires de services d'internet, les ISP.

KINGA KOWALCZYK : Nous n'avons pas d'autres questions pour le moment. Si vous voulez poser une question, n'hésitez pas à lever la main et on vous donnera la

parole pour que vous puissiez poser votre question. Ou vous pouvez indiquer votre question dans le Q&A.

ADIEL AKPLOGAN : J'aimerais avoir plus de retour sur ce que nous vous avons présenté dans les diapositives au niveau des résolveurs publics. On en a beaucoup parlé au niveau interne.

Le DoH et DoT au début étaient très controversés. Il y avait des inquiétudes au début en ce qui concerne le DNS sur TLS et DNS sur HTTPS. Mais cela semble tout à fait positif.

En ce qui concerne la sécurité, la question qui se pose, c'est : est-ce qu'on doit beaucoup parler dans l'initiative KINDNS des questions de vie privée et de respect de la vie privée ? Nous avons déjà des documents de travail là-dessus, mais est-ce que vous pensez que ce respect de la vie privée est assez souligné et mis en exergue dans nos documents ? Parce que l'on parle de plus en plus ces dernières années de la vie privée.

En ce qui concerne les résolveurs, il est très clair qu'on peut assurer une meilleure sécurité pour la plupart des logiciels. Mais en ce qui concerne le DoT et le DoH, nous avons des personnes qui se disent : « Est-ce qu'il faut vraiment présenter cela comme étant des meilleures pratiques ou pas ? » Il y a des personnes qui ne sont pas d'accord avec cela. J'aimerais en savoir plus de la part de la communauté, ce que vous pensez du respect de la vie privée par rapport au DoT et au DoH.

Je crois qu'une main s'est levée. Nous allons pouvoir donner la parole à Ulrich de s'exprimer. Ouvrez son micro.

ULRICH WISSER : Bonjour. Merci beaucoup Adiel de me donner la possibilité de m'exprimer.

Je voulais dire que je pense que le DoT résout certains problèmes de respect de la vie privée parce que cela limite les requêtes. Mais il faut vraiment avoir beaucoup de confiance en votre opérateur. Et cela peut être uniquement résolu par un DNS Oblivious, mais ce n'est pas encore le cas. C'est au niveau du DNS que l'on doit travailler pour assurer le respect de la vie privée parce que sinon, il faut totalement faire confiance à l'opérateur et tout n'est pas résolu pour le moment.

ADIEL AKPLOGAN : Oui, c'est un bon retour de votre part. C'est une bonne perspective. C'est important en effet qu'il y ait un rapport de confiance qui s'instaure entre les utilisateurs et les prestataires de service ISP. Il y a des contrats qui doivent être respectés et dans ces contrats, il y a le respect de la vie privée. Donc il faut voir quelles sont les politiques qui existent pour le respect de la vie privée. Mais lorsque vous utilisez un réseau d'entreprise, les questions de confidentialité sont un petit peu différentes, il y a moins de confidentialité.

Est-ce que nous devrions plus souligner ces questions de respect de la vie privée, de confidentialité lorsqu'on utilise différents types de résolveurs ? Je crois que les utilisateurs sont parfois un petit peu

inquiets des informations qu'ils envoient et de leur confidentialité lorsque c'est envoyé à certains résolveurs.

Est-ce que quelqu'un d'autre veut prendre la parole, poser des questions sur les résolveurs ou sur les serveurs faisant autorité au niveau des meilleures pratiques dont nous parlons aujourd'hui ?

S'il n'y a pas d'autres questions ou d'autres commentaires, cela veut dire que nous sommes sur la bonne voie. Donc je vous remercie tous pour avoir participé à cette réunion. N'hésitez pas à joindre notre liste de diffusion pour apporter votre contribution.

Je crois qu'il y a une question.

KINGA KOWALCZYK : Oui. « Est-ce que la mesure appartient à cette conception de KINDNS, une manière de mesurer dans laquelle la communauté a des moyens d'accéder aux données de résolveurs qui sont maintenues par différents résolveurs ? Est-ce que c'est une méthode de comparaison ? »

ADIEL AKPLOGAN : Comme je l'ai déjà dit, nous avons différents moyens qui nous permettent de voir l'impact que cela a au niveau des aspects de la sécurité des opérations du DNS en général. Quels seront ces indicateurs ? Cela n'a pas encore été défini, mais nous allons peut-être partager tout cela et nous allons partager ces initiatives de l'ICANN qui existent déjà.

En tout cas, ici, nous voulons évaluer les résolveurs avant et nous voulons savoir ici en fonction de chaque cas notre perspective, c'est que nous essayons de mesurer ce qui selon notre perspective est important. Nous ne voulons pas accéder aux données privées, bien sûr. Et nous allons mesurer toutes ces choses en fonction des meilleures pratiques. Nous allons peut-être pouvoir dire : « Le nombre de résolveurs qui ont des considérations concernant la confidentialité a évolué de telle ou telle manière au cours de telles années. » Donc c'est une manière de mesurer tout cela pour savoir quels sont les résolveurs qui ont des activités de minimisation, différentes activités. Tout cela peut être mesuré directement.

Je ne sais pas ce que vous voulez dire lorsque vous dites « accéder aux données des résolveurs ». Je ne sais pas très bien. Mais en tout cas, nous allons mesurer ce que nous voyons de manière publique mais ce qui lié aux meilleures pratiques que nous aurons indiqué préalablement. Nous allons essayer de joindre le plus grand nombre possible de résolveurs pour qu'ils participent à cette initiative.

Et nous avons trouvé un moyen de coopérer tous ensemble et de voir un petit peu ce qui peut être ajouté à cette initiative. Mais je dirais à nouveau que nous essayons de faire les choses de la manière la plus simple possible de façon à ce qu'il n'y ait pas de controverse au niveau des utilisateurs mais aussi au niveau de ceux qui vont utiliser les résultats de cette initiative.

La liste de diffusion est ouverte, n'hésitez pas à y contribuer. Nous allons poursuivre cette discussion sur la liste de diffusion. Si vous avez des observations, vous pouvez les faire sur la liste ou nous joindre

directement à octo@icann.org. Vous pouvez donc nous écrire si vous avez une question à nous poser directement. Merci.

Ah, je vois qu'il y a une question de Désirée. Merci Désirée. Oui, comme je l'ai dit, il y a une composante de communication et de sensibilisation qui est importante pour travailler avec la communauté en général. Nous avons un programme d'ambassadeurs. Nous travaillons avec la communauté pour promouvoir tout cela et l'ICANN aussi va diffuser des ressources pour promouvoir ces initiatives. Donc le succès va dépendre vraiment de cet aspect de la promotion de cette initiative pour que ce soit plus facile d'évaluer tous les résultats et que la communauté puisse nous donner son opinion sur tout cela et utiliser ces informations.

Merci à tous de vous être joints à cette présentation. Nous avons terminé avec neuf minutes d'avance. Je ne vois pas d'autres questions, donc nous pouvons en rester là. Et n'hésitez pas à envoyer vos commentaires à la liste de diffusion ou à nous écrire.

KINGA KOWALCZYK : Nous avons répondu à toutes les questions. Cette présentation va être publiée sur le site internet de la réunion de l'ICANN73, la *Prep Week*. Merci.

ADIEL AKPLOGAN : Merci Kinga. Merci à tous. Merci Philip. Merci Steven.

Cette réunion est maintenant terminée.

PHILIP REGNAULD : Merci.

[FIN DE LA TRANSCRIPTION]