ICANN79 | Forum de la communauté – Comment ça marche - Séance 3 : comment protéger vos pratiques opérationnelles DNS (tout sur KINDNS)
Dimanche 3 mars 2024 – 3h00 à 4h00 SJU

NICOLAS ANTONIELLO: Bienvenue à toutes et à tous. Nous allons commencer dans deux minutes.

Bienvenue à toutes et à tous. Nous allons commencer cette séance et lancer l'enregistrement. Bonjour et bienvenue à toutes et à tous à cette séance « Comment nous fonctionnons », consacrée au système KINDNS. Je m'appelle Nicolas Antoniello et je serai donc le responsable de la participation à distance pour cette séance.

Veuillez noter que cette séance est enregistrée et qu'elle suit les normes de comportement attendues de l'ICANN. Durant cette séance, les questions et commentaires ne seront lus à voix haute que s'ils sont soumis dans la fenêtre « Questions-réponses ». Si vous souhaitez parler durant la séance, veuillez lever la main sur Zoom et nous pourrons vous donner la permission de désactiver votre micro sur Zoom. Nous avons également un micro dans la salle.

L'interprétation inclura l'anglais, le français, l'arabe et l'espagnol. Veuillez indiquer votre nom pour les enregistrements et parler à un rythme raisonnable si vous parlez une langue autre que l'anglais.

Ceci dit, je donne maintenant la parole aux intervenants.

Remarque : Le présent document est le résultat de la transcription d'un fichier audio à un fichier de texte. Dans son ensemble, la transcription est fidèle au fichier audio. Toutefois, dans certains cas il est possible qu'elle soit incomplète ou qu'il y ait des inexactitudes dues à la qualité du fichier audio, parfois inaudible ; il faut noter également que des corrections grammaticales y ont été incorporées pour améliorer la qualité du texte ainsi que pour faciliter sa compréhension. Cette transcription doit être considérée comme un supplément du fichier mais pas comme registre faisant autorité.

ADIEL AKPLOGAN : Merci beaucoup, Nicolas. Bienvenue à toutes et à tous. Bienvenue à cette séance sur KINDNS.

Donc KINDNS, c'est une initiative, une initiative qui a commencé il y a un an et demi auparavant. Il s'agit donc d'une initiative qui est un outil supplémentaire par rapport à ce que nous faisons depuis de nombreuses années. Il s'agit là de la promotion des opérations, des meilleures pratiques pour le DNS, pour différents éléments du DNS. Et donc notre objectif est de simplifier toutes ces pratiques pour les opérateurs, pour qu'ils puissent tout simplement et facilement mettre cela en place dans leur cadre opérationnel.

Donc KINDNS – la gentillesse en anglais, c'est le partage de connaissances et l'instauration de normes pour la sécurité du DNS et du nommage. Donc nous avons un partage de connaissances, et nous essayons d'avoir un seul point d'accès. Il y a un site Web où vous pouvez trouver beaucoup plus d'informations sur le programme KINDNS de partage de connaissances et d'instauration de normes pour la sécurité du DNS et du nommage. Vous pouvez participer à tout cela et vous pouvez faire une autoévaluation également. Vous avez un outil d'autoévaluation. Vous pouvez vous rendre sur le site Web.

Nous allons passer à la diapo suivante.

Comme je l'ai mentionné, si vous êtes très familier du DNS, vous connaissez le projet qui essaye d'identifier donc tout ce qui touche au DNS. Et cela représente beaucoup. Donc si vous êtes un opérateur du

DNS, un opérateur de résolveur [autoritatif], vous voulez suivre toutes ces informations, vous devez vraiment travailler à plein temps pour cela. Ce sont des ressources importantes qui vont prendre beaucoup de temps, que vous soyez une petite ou une grosse entité. Donc vous pouvez avoir une équipe tout entière pour cela. Et parfois, ce n'est pas toujours très clair.

Donc l'idée, c'était de travailler avec la communauté, d'obtenir un retour d'informations des opérateurs sur le terrain et de construire un cadre de référence que l'on puisse suivre, que tout le monde puisse avoir comme objectif également. Donc KINDNS, ce n'est pas seulement le faire maintenant, mais envisager également l'avenir, avoir un objectif à atteindre et obtenir un niveau de maturité beaucoup plus élevé avec l'utilisation de ces meilleures pratiques. Et nous travaillons depuis plus d'un an avec la communauté à ce sujet. Et nous avons donc des retours d'opérateurs sur le terrain. Et c'est vraiment les meilleures pratiques opérationnelles qui nous concernent et que nous voulons renforcer. Donc on [vous] donne la possibilité aux opérateurs de s'autoévaluer. Il y a également un programme d'ambassadeurs qui existe.

Nous allons passer à la diapo suivante, nous allons voir quels sont les opérateurs ciblés.

Donc c'est un processus de discussion. Et nous avons vu cinq différents types de catégories de meilleures pratiques. Alors deux catégories par rapport aux serveurs qui font autorité et opérateurs de serveurs, et deux pour les zones critiques et TLD, parce que nous pensons que les personnes qui sont dans les zones les plus critiques avec des serveurs

faisant autorité ont un travail très difficile au niveau de leurs pratiques. Et nous avons également les opérateurs SLD. Ça, c'est toutes les personnes qui ont un nom de domaine, qui ont une responsabilité par rapport à un SLD. Et il y a donc des meilleures pratiques à ce niveau qui sont requises de ces opérateurs de serveurs de résolution. Et ces opérateurs de résolveurs jouent un rôle très important dans l'écosystème, et doivent adhérer à des meilleures pratiques.

Donc, nous avons trois différentes catégories. Nous avons ces résolveurs fermés et privés avec ces opérateurs. Ce sont des résolveurs où il y a des environnements très contrôlés. Il y a les résolveurs partagés et privés. C'est, en général, les prestataires d'accès à l'Internet qui gèrent cela. Ce n'est pas véritablement public. Il y a un certain niveau de partage [inaudible] au niveau de ces résolveurs. Nous avons également les résolveurs publics ouverts à toutes et à tous, à tous les utilisateurs de l'Internet. Nous en avons des très populaires. Nous avons 8.8.8.8 et ainsi de suite. Et nous avons donc un ensemble de meilleures pratiques là aussi pour ces résolveurs publics, que nous encourageons, que nous recommandons.

Et nous avons également quelque chose qui chapeaute tout. C'est un système. Nous essayons de renforcer le cœur du système. Et si votre système lui-même ne fonctionne pas en suivant des pratiques de sécurité de base, eh bien, votre système va être faible. Donc c'est pour ça qu'il faut renforcer le cœur du système, et que cela est si important. Donc nous avons des recommandations pour renforcer le cœur du système.

Donc si vous appliquez cette autoévaluation à vos pratiques KINDNS, c'est bien. On va vous demander de vous autoévaluer, comment est-ce que vous gérez votre système. Et nous voyons et nous verrons à ce moment-là si on peut améliorer les pratiques.

Donc le programme a deux aspects. Premièrement, l'autoévaluation, dont je parlais, pour utiliser les outils que nous vous avons remis, pour revérifier où vous vous en trouvez en ce qui concerne les opérations du DNS. Et vous pouvez décider ensuite de vous joindre au cadre de référence formel. Et là, vous indiquez publiquement que oui, j'apprécie ces pratiques, je vais les mettre en œuvre dans mes opérations et mon exploitation. Et également, nous serons très heureux de promouvoir auprès de nos clients le déploiement de ces systèmes et de ces pratiques. Et il y a des [poursuites] et des formations qui s'ouvrent à ce niveau. Nous sommes tout à fait disponibles, avec beaucoup de documents d'information également. L'objectif de KINDNS, c'est de rester simple et de pouvoir mettre en œuvre ces différents points.

Je parlais de l'autoévaluation tout à l'heure. Eh bien, vous pouvez la faire en ligne. Vous pouvez accéder au site Web. Vous pouvez choisir de vous autoévaluer, et vous n'aurez qu'à répondre à une série de questions par rapport à la manière dont vous exploitez votre DNS. Il s'agit d'un cadre volontaire. Vous fournissez les informations que cela. Si vous êtes, le résultat va refléter la vérité et ça va vous orienter par rapport à ce que vous devrez faire.

Vous recevrez un rapport à partir de cette autoévaluation qui reste bien évidemment anonyme. Nous ne collectons pas d'informations par

rapport à ce qui fait quelle autoévaluation. C'est vous qui allez capturer les informations par rapport à la manière dont vous exploitez ou gérez vos opérations DNS et votre réseau. Et à la fin, vous aurez un rapport qui sera généré.

Ce qui est intéressant dans le rapport, c'est que ça vous dit quel est votre état de situation, comment vous êtes classé, mais ça va également vous fournir une ligne de chronologie par rapport à la manière dont vous pourrez améliorer les résultats pour lesquels vous avez eu une note faible. Le rapport qui sera généré à la fin de l'autoévaluation va vous dire « regardez, vous avez une faiblesse ici, vous avez eu un 0/10 parce que vous avez dit que vous n'êtes pas en train de mettre ceci en œuvre. Voici les [directrices]. Voici pourquoi il est important de mettre cela en œuvre et voici les [directrices] pour savoir comment le mettre en œuvre. Vous pourrez télécharger ce rapport pour utiliser ces [directrices] et mettre votre système à l'épreuve avec cette autoévaluation à la main. Vous pourriez également l'utiliser pour convaincre les décideurs d'investir davantage de fonds dans ces systèmes et de vous consacrer plus de ressources pour faire évoluer ce système.

La participation à KINDNS est donc volontaire. Tout à l'heure. Ce n'est pas une obligation que l'ICANN impose aux opérateurs. Il s'agit tout simplement d'un cadre qui existe. Et les informations qui sont fournies sont également fournies de manière volontaire. J'insiste.

Nous faisons de notre mieux pour générer une relation de confiance entre le cadre KINDNS et les opérateurs qui l'utilisent. Lorsque vous

participez, vous rejoignez KINDNS comme participant. C'est-à-dire que vous devenez un défendeur de ces meilleures pratiques.

Diapo suivante.

Alors, la plate-forme d'autoévaluation et le site Web ont déjà été lancés. Cela fait un an et demi qu'ils sont en ligne et nous avons beaucoup vu beaucoup d'intérêt auprès des personnes qui utilisent cette autoévaluation. Nous avons 1500 personnes qui ont utilisé cet outil d'autoévaluation à ce jour, et ce que nous vous montrons à l'écran sont quelques constats d'intérêt que nous avons conclu à partir des données anonymes que nous collectons à partir de cette autoévaluation. Donc, par exemple, pourquoi KINDNS intéresserait les participants ? Ça vous surprendra de voir que la plupart des personnes qui font ces autoévaluations manifestent qu'il s'agit d'un exercice qui leur permet de comprendre quel est leur état de situation par rapport au DNS, et que ça leur permet de voir s'ils sont en train de mettre en œuvre les meilleures pratiques ou pas. Sur ces participants, 32 % ont finalement décidé de se joindre à KINDNS et ça les a aidés à améliorer leur système de sorte qu'ils peuvent s'inscrire formellement au programme. Au moment de vous inscrire formellement, vous allez devoir répondre à des questions plus détaillées sur [la pratique] parce que l'autoévaluation est un exercice entre vous et l'outil d'autoévaluation. Et les données et les résultats sont personnels. Nous ne les voyons pas. Mais au moment de vous inscrire en tant que participant à KINDNS, vous allez devoir répondre aux mêmes questions, mais avec un peu plus de détails par rapport à la manière dont vous mettez en œuvre certaines pratiques. Et là, nous vous poserons d'autres questions

supplémentaires pour nous permettre de mieux comprendre. Dès que vous dites je suis en train de [le pratiquer], c'est une déclaration publique. Et notre but est de nous assurer que vous le faites correctement. Alors, les participants font cette autoévaluation pour se préparer à s'inscrire et à devenir des participants.

Nous avons également remarqué avec intérêt que 40 % de ceux qui ont répondu à l'autoévaluation l'on fait pour utiliser les résultats afin de convaincre leurs responsables, leurs cadres de pouvoir améliorer leur système. Donc ceux qui prennent l'autoévaluation ont parfois du mal à avoir de l'aide pour pouvoir mettre en œuvre les meilleures pratiques. Donc, à partir de l'autoévaluation, ils obtiennent un rapport qui leur permet de montrer leur situation et donc de convaincre leurs responsables de pouvoir aller au-delà et aller de l'avant avec ces activités et ces mesures nécessaires. Et c'était intéressant pour nous de constater cela. Voici [inaudible] que nous avons tenu. La plupart de ceux qui ont répondu à l'autoévaluation exploitent à la fois des résolveurs et des serveurs faisant autorité. Ce qui est souvent le cas dans l'environnement des opérateurs. Vous allez exploiter un serveur faisant autorité pour vous-même, mais si vous êtes un fournisseur de services Internet, vous le ferez pour votre nom de domaine et en tant que service que vous fournissez à vos clients. Et donc la plupart de ceux qui ont fait l'autoévaluation ont répondu qu'ils faisaient les deux. 29 % des personnes qui ont répondu ont également dit qu'ils ne gèrent qu'un serveur faisant autorité. Et entre ceux qui exploitent un serveur faisant autorité, 29 % gèrent des TLD parmi le total des répondeurs à l'évaluation. Seuls 27 % ont les deux ; 29 % des noms de domaine de

premier niveau et 44 % des noms de domaine de second niveau. Et, c'est un bon reflet de la situation. La plupart de ceux qui utilisent le système des noms de domaine sont des opérateurs de nom de domaine de second niveau, parce qu'ils sont des titulaires de nom de domaine et qu'ils vont utiliser le nom de domaine eux-mêmes. Et c'est très logique. La plupart ou en tout cas une bonne partie de ceux qui ont répondu sont des gestionnaires de TLD et ça nous intéresse de pouvoir atteindre ces acteurs, parce que c'est eux qui vont gérer un aspect très important du système de noms de domaine.

Voici d'autres statistiques à propos de certaines des pratiques. On voit ici ce que les personnes ont répondu à partir de ce que les opérateurs des serveurs publics font et des pratiques donc qu'ils appliquent pour leur résolveur public. [Inaudible] pratiques pour les opérateurs de résolveurs récursifs publics. Et la pratique la moins commune est celle du DNS sur TLS ou DNS sur HTTPS, qui est en fait une question de mise en œuvre d'un système de cryptage qui permet de communiquer entre l'utilisateur et les opérateurs de résolveur.

Seuls 46 % des répondeurs à cette évaluation ont manifesté avoir mis en œuvre cette pratique spécifiquement, même sachant que la quantité de personnes ayant mis en place cette pratique n'est pas mineure.

Et du côté du DNS, nous avons beaucoup travaillé à la sensibilisation. Et ce depuis longtemps. Et nous voyons une augmentation considérable des serveurs faisant autorité qui ont déjà la validation du DNSSEC. C'est également repris ici parce que 70 % disent avoir la validation DNSSEC. Et donc, pour nous au sein de l'équipe de

participation des parties prenantes techniques, ça nous permet de voir où on a besoin de s'investir au moment de faire renforcement des capacités ou de sensibilisation. On voit ce qui manque et ce que les personnes pourraient avoir de leurs opérateurs.

Diapo suivante. Alors, nous vous invitons à vous abonner à la liste de diffusion, liste des discussions KINDNS discussed. Il s'agit de l'endroit où l'on tient tous ces débats. Mais nous espérons pouvoir utiliser cette liste de manière plus active pour que la communauté reste active, pour débattre des pratiques et débattre de l'évolution du cadre des meilleures pratiques également.

Nous avons déjà reçu des retours à propos de la pratique. Et nous sommes en train de mettre en œuvre tout cela dans le cadre de sorte que notre portée puisse être un peu plus large auprès des opérateurs. Donc la liste de diffusion est un outil d'importance pour pouvoir atteindre nos résultats.

On veut plus de retours de la communauté. Et on veut d'ailleurs générer une communauté autour de cela, et que ce soit cette communauté même qui gère ce projet par la suite, qui le dirige. Nos activités de sensibilisation sont également utilisées pour promouvoir cette initiative dans les différentes régions. Au niveau de l'équipe GSE et de l'équipe de participation des parties prenantes techniques, on organise des formations à propos des meilleures pratiques de KINDNS pour les opérateurs qui n'ont pas appliqué ce cadre de meilleures pratiques, pour qu'ils le fassent et pour qu'ils mettent en œuvre ces meilleures pratiques.

Alors, cette semaine, nous allons justement tenir un programme de KINDNS qui est un entretien, un rendez-vous de KINDNS, que vous pouvez avoir avec un de nos techniciens pour discuter de votre cas spécifique d'activité DNS dans toutes ces catégories. C'est-à-dire que vous allez recevoir un support très dédié pour mettre en œuvre KINDNS, pour vous aider à faire l'autoévaluation, pour lire et interpréter le rapport, et puis pour travailler avec l'équipe pour savoir comment mettre en œuvre ce rapport. Quelles sont les mesures que vous pouvez prendre. Et puis par la suite vous resterez également en contact avec l'équipe. Au-delà de la réunion de Porto Rico, vous allez continuer à travailler avec notre équipe sur vos pratiques KINDNS.

Les programmes en cours en backend ont énormément évolué. Et l'idée est que notre autoévaluation puisse être un peu plus technique, avec cet aspect d'aller au-delà de répondre à des réponses et de nous fournir des informations. Au contraire, l'idée est de pouvoir vous armer d'outils qui vous permettent de mettre à l'épreuve votre opération DNS et contribuer à l'outil d'autoévaluation avec vos retours pour que l'on puisse vérifier la mise en œuvre de ces meilleures pratiques.

Nous avons également commencé à travailler avec les masters de zone, ceux qui exploitent le DNS, et en particulier les opérateurs de DNS et les opérateurs de serveurs faisant autorité vont connaître ce master de zone. On veut travailler avec eux pour connaître spécifiquement leur avis par rapport aux pratiques KINDNS. Donc vous aurez la possibilité de vous autoévaluer en utilisant les zonemasters et en utilisant le cadre KINDNS de sorte que le zonemaster et les résultats que vous recevez seront spécifiques à votre opération et à KINDNS en général.

Nous avons commencé à travailler également avec Manners, parce que notre KINDNS reprend ce que fait Manners pour le routage. Et l'idée est de pouvoir promouvoir tout cela ensemble entre les deux. À KINDNS, en essence, on fait également allusion aux pratiques de Manners, parce que certaines des pratiques de Manners sont tout à fait pertinentes pour le KINDNS. Donc on s'est associé à Manners. On a déjà organisé des ateliers conjoints pour promouvoir les meilleures pratiques de DNS et les meilleures pratiques de routage. Parce qu'il y a des points communs entre les deux. Et on veut être sûr de pouvoir comprendre tout l'écosystème.

Nous sommes également en train de travailler activement avec un groupe de chercheurs pour savoir comment mesurer la mise en œuvre de ces meilleures pratiques et voir comment ils évoluent à mesure que le programme de sensibilisation avance. Donc, c'est une initiative tout à fait dynamique qui évolue. Et nous tenons à intégrer de plus en plus de personnes et de communautés pour améliorer ce projet et pour faire en sorte que le niveau d'adoption augmente.

Voilà ma partie de la présentation. La deuxième partie de la présentation sera assurée par Nicolas, qui va vous montrer le site Web et en particulier l'outil d'autoévaluation. On verra de quoi à l'air le résultat, le rapport. Et on discutera si besoin de cela. Mais avant de passer à Nicolas, je voudrais savoir si vous avez des questions pour que j'y réponde. Non ? Il paraît que ce n'est pas le cas.

NICOLAS ANTONIELLO : Je ne vois pas de questions sur le chat ni sur la fonction « questions-réponses » non plus. Donc oui, pardon, dites votre nom.

ABDALMONEM GALILA : Merci. Je suis Abdalmonem Galila. Je pense que j'aurai besoin de lire à propos de KINDNS un peu plus. C'est la première fois que je vous entends parler de ce projet. Est-ce que cette évaluation pourrait se faire pour les ccTLD également ? Je ne suis pas tout à fait sûr, parce que si j'ai bien compris KINDNS s'applique a. Alors u cadre DNS. Ou alors est-ce qu'on pourrait aider les administrateurs de résolveur ou les administrateurs de DNS ? Comment renforcer la sécurité à travers ce programme ? Voilà les questions que je me pose, mais je pense qu'il faudrait que j'en lise davantage et un peu plus en détail.

ADIEL AKPLOGAN : Oui. Vous allez voir maintenant dans le type d'autoévaluation, mais c'est surtout à propos de TLD pour savoir – parce que vous savez ce que vous faites dans votre TLD. C'est individuel. Chacun fait son autoévaluation et les résultats seront en lien avec vous et vos opérations. Or le cadre vous donnera une idée de ce que vous devez faire. Et au moins, vous pourrez suivre tout cela pour améliorer la manière dont vous exploitez votre TLD parce que c'est ça l'idée d'avoir un écosystème qui soit plus sécurisé, résilient, etc. Donc l'une des pratiques par exemple de l'opérateur de TLD sera l'activation [des] DNSSEC. Une des pratiques est de signer et de valider DNSSEC. Ce n'est pas qu'avec le DNSSEC [on aura tout]. Mais c'en est une des pratiques.

Et l'activation de la validation du côté du résolveur est une autre pratique. Mais puis il y en a d'autres bien sûr.

Mais vous allez voir tout cela sur l'outil à travers la démonstration de Nico.

NICOLAS ANTONIELLO : Merci Adiel. Nous allons aborder ce sujet. Tout d'abord, je m'appelle Nicolas. Je suis responsable de la relation avec la communauté technique pour l'Amérique latine et les Caraïbes. Et je fais donc partie de cette équipe dirigée par Adiel, chargée de la relation avec la communauté technique donc. Mais dans le cadre de l'ICANN, nous faisons partie donc du Bureau du directeur de la technologie (OCTO) au sein de l'ICANN.

Donc l'idée, maintenant, c'est de vous montrer le site Web. Ça va être un tout petit peu plus technique. Je vais essayer d'utiliser un langage que vous puissiez comprendre, que vous connaissiez deux ou trois choses sur le DNS ou rien du tout.

Donc ce programme est pour les opérateurs DNS. Qui sont-ils ? C'est quelqu'un qui exploite un serveur DNS, ni plus ni moins. Vous êtes opérateur si vous avez votre propre résolveur ou si vous faites partie d'un centre dans un centre de fournisseurs de services Internet. Donc voilà.

Il y en a deux types d'opérateurs. Si vous exploitez donc un résolveur ou donc un serveur faisant autorité. Donc vous pouvez être opérateur de tous types de serveur DNS.

Donc je vais résumer certains des concepts proposés par Adiel. Tout d'abord, parlons un petit peu des catégories d'opérateurs que nous avons sur notre page Web. Donc nous avons, comme l'a dit Adiel, nous avons séparé tout cela en cinq types d'opérations. Ces cinq types d'opérations donc se recoupent en deux groupes. Alors, revenons donc.

Nous allons commencer par les opérateurs de serveurs récursifs. Ici, nous en avons trois de ces opérateurs donc de type récursif. Les résolveurs privés. Donc un résolveur privé, c'est un serveur récursif qui a un but d'être utilisé par celui qui l'utilise. Donc mon organisation a une équipe qui gère ce résolveur qui sera utilisé par les appareils au sein de cette organisation. Et si vous souhaitez [être] donc un résolveur de ce type, il sera utilisé uniquement par l'organisation. Ça, c'est un résolveur privé. Il est privé.

Ensuite, nous avons donc un deuxième type de serveurs récursifs que nous appelons les résolveurs privés partagés. Ce sont des résolveurs qui sont utilisés par des clients, les clients d'une organisation ou d'une entreprise. Par exemple, si vous exploitez donc un FSI, alors, tous les clients du FSI donc auront accès à ce résolveur. Il est privé, parce qu'il n'est pas accessible à tous sur Internet. Il n'est pas public. Mais il n'a pas pour but d'être utilisé par d'autres que par les clients donc de l'organisation.

Ensuite, nous en avons un troisième type. C'est le résolveur public qui est exploité par certains organismes. Et tout le monde sur Internet peut accéder à ces résolveurs, et peut les utiliser. Par exemple, il y en a un qui est connu. Donc le 8888, c'est Google. Il y a l'adresse IP 1111 ou

9999. Le Google, le cloud. Donc il n'y en a pas des centaines, mais il y en a beaucoup. Et toute personne connectée à Internet peut.

Pourquoi distingue-t-on les résolveurs [inaudible]. Les meilleures pratiques ou les pratiques les plus courantes et qui sont les meilleures sont communes aux trois, mais il y a des différences en termes opérationnels. Pour le résolveur public qui est accessible à tous, vous allez probablement devoir réviser très judicieusement vos politiques de sécurité et de mesure parce que vos serveurs seront exposés à tout l'Internet. Et ils peuvent être utilisés donc à bon escient ou à mauvais escient. Et il faut donc aller les protéger des activités malveillantes. Et donc, ils pourraient être utilisés pour des attaques. On ne parle pas d'attaques qui ciblent le résolveur lui-même, mais ils utilisent leur résolveur pour attaquer un tiers. En langage courant, il y a des types d'attaques DNS qui peuvent utiliser ces résolveurs ouverts comme voie pour attaquer une tierce partie. Si vous gérez un résolveur privé, vous n'aurez probablement pas ce problème, car vous avez votre propre sécurité au sein de votre organisation. Et si quelqu'un utilise – ou souhaite utiliser – votre serveur, eh bien, l'attaque proviendra probablement de l'intérieur et non pas de l'extérieur. Et là, ça sera facile de prendre des mesures. Donc il y a des différences d'exploitation dans les opérations. Et donc nous avons classé ces résolveurs en trois groupes.

Ensuite, nous faisons donc aux opérateurs – nous passons aux opérateurs faisant autorité.

Il y a les TLD et les éléments critiques, ce sont des opérateurs faisant autorité, en charge de TLD. Donc, les serveurs donc de domaines de premier niveau. Donc ce sont les ccTLD. Et donc, il y a les ccTLD et les gTLD. Donc ces serveurs faisant autorité. Et il y a donc -- il y a les éléments critiques. Ça, c'est ce qui est considéré par l'opérateur comme étant critique.

Pour certains pays, les opérations continues des serveurs faisant autorité, pour les services de gouvernement, ils sont critiques. Car s'ils sont défaillants, eh bien, il ne sera plus possible d'assurer les services. S'il y a des pannes, cela donc peut poser de gros problèmes. Donc ils peuvent être de deuxième niveau. Donc dans les domaines de l'éducation, par exemple, il y aura probablement ces éléments critiques. Dans les domaines liés aux services sanitaires, pour les services liés au secteur financier. Donc, il peut s'agir du premier niveau, du deuxième niveau, peu importe. Et ensuite, il y a tous les autres. Donc tous les domaines de deuxième niveau. Les zones. Donc, ce sont les catégories de zones SLD.

ADIEL AKPLOGAN : Donc si vous êtes sur le site Web, vous pouvez cliquer sur la catégorie des opérateurs *operators category*. Et donc Nicolas vous a montré les différentes catégories.

NICOLAS ANTONIELLO : Merci Adiel. Donc voilà la classification. Donc si vous faites partie de ce programme, vous allez devoir passer en revue tout ce qui s'applique à

votre opération. Donc vous pouvez être un opérateur de serveur récursif, par exemple, et vous suivez donc la marche à suivre.

Donc ça, il s'agit du durcissement de la plate-forme. Cela va au-delà de la classification que nous avons utilisée. Il s'agit de prendre des mesures supplémentaires pour la sécuriser ou augmenter la sécurité et la résilience de votre serveur et de vos opérations DNS. Il y a beaucoup de pratiques ici qui sont bonnes à mettre en œuvre pour renforcer votre infrastructure, durcir votre plate-forme. Donc cela va du simple au recommandable, aux pratiques recommandées. Et il y a donc les plus avancées de ces procédures que vous devriez envisager de mettre en place lorsque vous déployez une plate-forme.

Ici, vous dites – vous voyez *must*, c'est-à-dire que c'est très fortement encouragé. Quand il y a *must*, obligation donc, c'est fortement recommandé. Et puis d'autres ne sont pas aussi fortement recommandés. Donc c'est quelque chose que vous devriez mettre en place. C'est recommandé, mais pas obligatoire. Donc il y a des mesures qui sont facultatives et d'autres qui sont recommandées.

Bien. Il y a ces outils. Donc c'est la section des outils et des lignes directrices. Tout d'abord, nous avons l'évaluation et les outils. Ici, c'est la partie essentielle du programme. Donc il y a l'autoévaluation évoquée par Adiel. Et nous allons nous plonger dans ce sujet, donc cette autoévaluation est facultative. Il est facultatif de fournir des informations sur qui a fait cette autoévaluation. Vous pouvez le faire. Vous pouvez donner le nom de l'entreprise, le nom de l'organisation qui a fait cette autoévaluation. Si vous ne souhaitez pas divulguer ces

informations, vous pouvez tout de même faire l'autoévaluation sans révéler ces informations. Donc à la fin, donc pendant l'autoévaluation, nous allons le faire. Vous allez voir une série de questions.

Ici, il y a le nom de l'organisation. C'est facultatif. Je peux mettre Nico. C'est mon organisation. Ou je peux donc ne pas répondre à cette question. Vous pouvez, dans un cas comme dans l'autre, faire l'autoévaluation. Donc on me demande pourquoi est-ce que vous suivez cette autoévaluation. Donc, par exemple, pour savoir où j'en suis en matière des meilleures pratiques du DNS. Ensuite, je dois sélectionner quel type d'opérations DNS j'ai : est-ce que j'ai un serveur faisant autorité, un serveur récursif ou bien les deux. Si mon infrastructure est donc gérée par un tiers, ou alors que je gère mon propre serveur. Par exemple, s'il s'agit d'un FSI j'ai un serveur récursif pour donner à mes clients – donc, offrir à mes clients de la récursion DNS.

Donc après, il y a le type d'opérations de résolveur récursif. Par exemple, si je suis un FSI, donc j'ai privé et public. Ici, il y a l'autoévaluation. Il a toutes les questions auxquelles vous allez répondre pour faire cette autoévaluation. Donc c'est une série de pratiques. Vous en avez six ici et vous allez cocher toutes les pratiques que vous mettez en place actuellement. Par exemple, pratique numéro 1.

Donc j'ai la validation du DNSSEC allumée pour mes résolveurs. Et j'ai la capacité de valider le DNSSEC. Donc je peux cocher cela. C'est bon. Pratique numéro deux. J'utilise des listes d'accès pour restreindre qui

peut envoyer des requêtes récursives à mes résolveurs. Donc ça, c'est un résolveur privé partagé. Et là, [inaudible] un système de sécurité [inaudible] de sécurité. Une liste d'accès, c'est comme ça qu'on les appelle, qui bloque tout le monde sauf mes clients. Donc je dis oui. Je coche. C'est bon. C'est une pratique très commune. Si je ne veux pas avoir [inaudible] aspect public dans mon résolveur. Si vous avez quelque chose qui est public-privé, donc vous avez une liste d'accès. Pratique numéro trois, j'ai eu une minimisation Q name des requêtes de nom. Alors, je ne sais pas vraiment ce que c'est. Donc je n'ai pas besoin de cocher, parce que j'ignore un petit peu ce que c'est. Pratique numéro quatre. Mes résolveurs ne fonctionnent pas sur le même serveur que des services DNS « autoritatifs ». Chez un serveur alternatif, je n'ai pas beaucoup de ressources financières. J'ai un serveur physique, ma propre machine. J'ai bâti tout cela. J'ai un serveur qui fait autorité ou j'ai juste une machine vraiment très simple, un système d'opération. Et j'ai une seule machine pour les deux. Donc je n'ai pas répondu à cette pratique. Donc je ne vais pas cocher cela. Pratique numéro cinq. Mes services de récursion sont résilients. J'utilise au moins deux serveurs distincts. Non, ce n'est pas le cas. Je ne coche pas. Pratique six. L'infrastructure qui dessert mon service DNS est contrôlée de manière active. Oui, c'est exact. Je vais donc cocher cela. Donc je suis en conformité par rapport à cette pratique numéro six. Ensuite, est-ce que vous avez un portail interne ou public pour les clients ? Non. Pour l'accès de gestion de services DNS, la réponse était non.

Alors, c'est tout. J'ai terminé mon autoévaluation. C'est ce que cela me dit. Je peux continuer à faire une deuxième évaluation qui va rentrer

plus dans le détail des pratiques de sécurité, qui ne sont pas uniquement pour les serveurs DNS. C'est des pratiques de sécurité qui sont pour beaucoup d'autres services, y compris les opérations de serveur du DNS. Par exemple, Adiel a mentionné Manners, un programme de meilleures pratiques, pas pour le DNS, mais pour le routage. Et comme l'a dit Adiel, ces programmes KINDNS proviennent un petit peu de Manners. C'est le même concept à la base. Et c'est ISOC [sur Internet] qui a développé cela pour les meilleures pratiques de routage. Et à partir de cela, on a bâti pour le DNS les meilleures pratiques KINDNS. Donc il y a beaucoup d'éléments communs, mais il y a beaucoup d'autres mesures de sécurité, de recommandations qu'on pourrait mettre en œuvre avec le routage, par rapport à la sécurité physique de l'infrastructure du DNS en particulier, et ainsi de suite.

Et voilà. Donc le rapport avec Manners, c'est vraiment la clé parce que, vous le savez, pour les serveurs du DNS.

ADIEL AKPLOGAN : Donc nous avons donc la sécurisation des routages, l'accès au DNS qui est également critique. Donc vous voyez à quel point c'est essentiel, tout cela. Vous voyez les liens qui s'instaurent entre les deux systèmes.

NICOLAS ANTONIELLO : Oui. Donc parfois, plus fréquemment que nous le désirons, nous faisons du développement des capacités sur le routage, sur le DNS, sur les réseaux Internet en général. Mais on se concentre sur un thème

spécifique, comme aujourd'hui on se concentre sur le DNS. Et on risque de perdre certains points de vue.

Donc le DNS, ce n'est pas isolé. [Il y a] besoin d'adresses de protocole Internet IP. On a besoin d'un réseau. On a besoin de routeurs qui sont utilisés pour faire passer les informations d'un endroit de l'Internet à un autre. Vous avez besoin de protocoles de routage, de sécurité, d'équipement de sécurité, et ainsi de suite. Donc c'est un petit peu l'idée derrière tout cela. C'est connecter les opérations du DNS avec le reste des opérations et des exploitations. Donc c'est tout un écosystème, dirions-nous. Donc on ne va pas trop entrer dans les détails, parce que ça prendra beaucoup de temps.

Donc j'ai cliqué, et maintenant j'ai une évaluation. J'ai un score qui m'est donné. Et le score total est 50 %. On est à une mise en œuvre de 50 %. De quoi ? De ce programme [commettant] les meilleures pratiques, sur [lequel] on peut tomber d'accord pour ce type d'opérations du DNS. Je vais sélectionner. Vous vous rappelez que [inaudible] opérations de résolveur public-privé. Donc sur ces six, si vous vous rappelez, ces six pratiques, j'en ai 50 % qui sont au niveau. Et là, j'ai deux options. Je peux télécharger mon rapport. Je vais cliquer là-dessus, et ça va générer un rapport en PDF, avec toutes les informations. Il y a quand même plus d'informations. Ça va me donner clairement un sens d'où j'en suis au niveau d'opérations du DNS. Et ça va me dire, vous devriez mettre ça en œuvre, ça en œuvre, ça en œuvre.

Et j'ai des ressources également pour que je mette en œuvre d'autres pratiques. Si je ne télécharge pas le rapport, je ferme cette page. Et c'est

important donc de télécharger à ce moment-là le rapport. Sinon, vous allez devoir un petit peu repartir à zéro pour obtenir le rapport. Donc, c'est bien. Je ne vais pas le faire maintenant. Mais télécharger le rapport à ce niveau-là – et j'ai le choix également de reprendre l'autoévaluation.

Ah ! Maintenant, je me rappelle ce que c'est que l'anonymisation Q name – la minimisation Q name plutôt. Ça, c'est pour vous ; uniquement pour vous. Personne ne va regarder cela. Donc vous n'avez pas à mentir à ce niveau parce que c'est vraiment quelque chose qui vous indique vos meilleures pratiques. Si vous cliquez sur tout, ça ne sert à rien. Ça va être comme si vous n'avez rien fait ; sauf si vous êtes en conformité, évidemment, avec toutes ces meilleures pratiques.

Donc voilà, ça, c'est la partie autoévaluation. Et nous avons également pour tout type d'opération une autoévaluation qui est possible.

Voilà, voyons un petit peu le rapport. On a téléchargé le rapport. Il va être donc en PDF. Nous avons des rapports d'autoévaluation que nous allons voir. Un instant. Je vais partager avec vous le rapport en PDF. Voilà. Voilà le rapport d'autoévaluation KINDNS. Comme vous le voyez ici, c'est avec une date d'évaluation, le type d'évaluation et d'autoévaluation que j'ai effectué, les pratiques opérationnelles que j'ai sélectionnées pour ce résolveur public-privé, les pratiques de sécurité du DNS. Vous voyez – vous vous rappelez que j'ai coché 1 et 2 parce que j'ai mis en œuvre 1 et 2, mais que je n'ai pas mis en œuvre la pratique numéro 3, parce que je ne sais pas ce que c'est que la minimisation Q name. Je suis sûr que beaucoup d'entre vous sont au courant de ce que c'est. Mais là, dans ce cas-là, je ne l'ai pas coché ;

donc c'est un score de zéro. Meilleures pratiques concernant la disponibilité, la résilience, la sécurité du DNS. 5, 6 – pratiques 5 et 6. 6, c'est mis en œuvre, pas 4 et 5. Voilà ce qui me donne ce score de 50 %.

Et là, vous vous rappelez de la minimisation. Ça m'explique là. C'est une technique pour améliorer donc la confidentialité des requêtes DNS. Ça explique cela. Vous avez une ligne de conduite et des explications pour savoir comment mettre en œuvre cette minimisation Q name, qui est tout à fait recommandée pour les résolveurs. Peut-être que vous utilisez un software *bind, outbound ;* c'est les plus communs. C'est les logiciels les plus communs à ce niveau dans le monde pour gérer un résolveur. Et ça va vous montrer des exemples précis de comment configurer la minimisation Q name dans *outbound* et dans ces logiciels. Ça explique beaucoup de choses. Ça donne beaucoup de détails. Ça explique les pratiques et ça vous donne plus de liens, plus de sources d'information, et ainsi de suite. Bien.

Même chose pour la pratique numéro 4, et ainsi de suite. Et la pratique numéro 5, là aussi, vous avez eu un score de zéro. Donc si je vois que je peux mettre cela en œuvre, eh bien, on le met en œuvre. Et ça permet, si on refait l'autoévaluation, d'arriver à un score de 100 %. Donc voilà le programme KINDNS, qui est très utile, qui permet de bâtir quelque chose, qui vous donne une fenêtre ouverte sur toutes les informations qui vous donnent accès à tous les liens nécessaires.

On ne gère pas de normes, de standard. On collecte donc ces meilleures pratiques parce que, comme Adiel l'a mentionné, si vous êtes un nouveau technicien et que vous déployez un serveur DNS – que vous

soyez au niveau « autoritatif » ou récursif, vous avez 150 normes et meilleures pratiques. Donc ça peut représenter une centaine de pages pour chaque norme.

Et vous allez à l'IETF, sur le site de l'IETF, vous avez tous les standards. Mais pour les meilleures pratiques, on les trouve un petit peu partout. Donc il va falloir savoir quelles sont les sources sur lesquelles on peut avoir confiance, et ainsi de suite. Et donc on va revenir au système Manners, collecte des meilleures pratiques, et présenter cela donc dans un endroit plus centralisé pour les opérations du DNS.

Donc permettez-moi de fermer cela. Et je vais donc revenir à la présentation, et au site plutôt KINDNS, au site Web. Je vais revenir sur le site Web. Je crois que j'ai dû fermer le navigateur. Voilà, c'est bon. J'ai trouvé. Je vais à nouveau le partager.

[Inaudible] site Web de KINDNS. Et vous voyez que vous pouvez télécharger le rapport à partir de cette page. On revient à la page d'accueil, et on a [inaudible] des outils et des [directrices] auxquels vous pouvez accéder à partir de cet onglet. Nous avons déjà parlé des outils d'évaluation. On a un tableau de bord qui montre certaines statistiques à propos du programme. C'est ce qu'Adiel a déjà montré. Et puis nous avons les directrices. C'est également une bonne source d'information pour ceux qui souhaitent connaître les pratiques qu'ils n'ont pas encore mises en place ou alors les pratiques qui sont déjà mises en œuvre, mais à propos desquelles ils souhaiteraient avoir plus d'informations ou s'ils veulent rafraîchir comment ça fonctionne. Et

donc on a ici les [directrices] d'intérêt, en fonction du type d'opération que vous avez.

Et finalement, vous avez ici ces ressources relatives à la sécurité du DNS. Et là, encore une fois, c'est un recueil de différents documents de meilleures pratiques, de normes, etc. Ici, nous les avons organisés suivant l'organisation qui les a élaborés. Et donc nous avons toute une série de documents qui ont été élaborés par l'ICANN, des normes élaborées par l'IETF, des ressources d'information d'autres organisations comme DNS-OARC, RIPE, APNIC, NANOG, donc des groupes d'opérateurs de réseaux venant de différentes parties du monde.

NANOG est l'opérateur de réseau de l'Amérique du Nord, mais chaque région a un groupe. Et puis il y a des sous-régions, comme les Caraïbes, qui ont leurs propres opérateurs de réseaux, comme CaribNOG, qui a également ses propres sources d'information. Et puis on a des sociétés privées, comme Google, ISC, ou d'autres, qui élaborent aussi des documents informatifs et qui vont donc publier des recommandations pour savoir comment configurer vos serveurs. D'accord ?

On est donc à l'heure de conclusion de cette [source]. Nous allons faire une pause de 15 minutes. Et puis nous allons prendre quelques minutes de la séance suivante. Donc nous allons faire une pause. Nous allons arrêter l'enregistrement et nous reprenons dans 15 minutes, d'accord ? Merci.

Donc l'interaction, les questions–

[FIN DE LA TRANSCRIPTION]