Sécurité et résilience du DNS - 29 octobre 2024

Claire C. van Zwieten - Internet Society Foundation: Alors, bienvenue à tous.

Génial, d'accord, c'est parti. Alors, bienvenue à tous. Merci de nous rejoindre aujourd'hui pour ce webinaire très important sur la sécurité et la résilience du DNS. Il est co-organisé par l'ICANN et l'Internet Society, et tous nos intervenants sont des anciens élèves communs, donc ils sont tous anciens élèves de l'Internet Society et de l'ICANN.

Je parie que beaucoup d'entre nous connaissent le DNS, le système de noms de domaine, qui sert de colonne vertébrale à Internet, connectant les utilisateurs du monde entier aux services d'information, mais il est aussi une cible des cybermenaces. Il est important que, en tant que communauté, nous comprenions quelles sont les menaces pour la sécurité du DNS et comment nous pouvons être résilients, et surtout, le rôle des organisations multipartites pour s'assurer que nous pouvons déjouer les menaces dès qu'elles apparaissent.

Avant de commencer, j'aimerais inviter Jadiel qui va parler un peu de notre programme Pulse et de Jadiel. Alors, Jadiel, si tu veux venir et commencer.

Jadiel ADEFOULOU - Internet Society: D'accord, super. Je suis Jadiel Adefoulou, consultant en ingénierie des données pour Internet Society. C'est un plaisir pour moi d'être ici et de parler de la plateforme Pulse.

Alors, tout d'abord, qu'est-ce que l'Internet Society Pulse ? Il est important de savoir que l'Internet Society Pulse consolide les données de mesure de l'Internet de tiers de confiance provenant de diverses sources en une seule plateforme. Nous utilisons les

données présentées pour examiner les tendances de l'Internet et adapter les données aux besoins des utilisateurs.

Nous utilisons les données présentées pour examiner les tendances de l'Internet et raconter des histoires basées sur les données afin que les décideurs politiques, les analystes de recherche,

les opérateurs de réseau, les groupes de la société civile et d'autres peuvent mieux comprendre la viabilité, l'évolution et la résilience d'Internet.

Ainsi, sur Pulse, nous suivons les coupures d'Internet, estimons l'impact économique d'une coupure à l'aide du calculateur de pertes nettes Pulse, mesurons la résilience d'Internet, suivons le nombre de points d'échange Internet dans le monde,

et proposons un rapport par pays, un moyen simple d'obtenir un aperçu de l'état d'Internet dans chaque pays ISO du monde.

Alors, qu'en est-il du DNS ?

Spécifiquement ? Deux domaines sur trois avec des codes pays sont sécurisés avec DNSSEC. Un internaute sur trois est protégé par un résolveur validant DNSSEC. Une autre statistique sur DNSSEC, on peut dire que certains pays, comme la Suède, ont des incitations pour les fournisseurs à adopter DNSSEC. Par conséquent, nous observons un niveau relativement élevé de couverture de la sécurité des noms.

La plupart des domaines Internet ont un très faible niveau d'adoption de DNSSEC. Par exemple, le domaine .com n'est signé qu'à 4%.

Claire C. van Zwieten - Internet Society Foundation: Merci, Jadier. Merci beaucoup de nous avoir informés sur le programme Pulse et sur DNSSEC.

Maintenant, j'aimerais inviter nos panélistes pour ce webinaire. Nous avons Jackie Akello, Kanaan Ngutu, Lia Solis et Marko Paloski. Merci à tous de nous rejoindre aujourd'hui. Kanaan, je sais que c'est très tôt pour vous. Il est probablement environ 3 heures du matin à Kiribati, alors merci beaucoup.

Je voudrais donner à tous nos panélistes l'occasion de se présenter et de partager leur point de vue sur l'état actuel du DNS. Lia, aimeriez-vous commencer ?

Lia Solis Montaño: Bonjour à tous. Je suis Lia Solis. Mon parcours est technique. Je travaille chez un FAI depuis de nombreuses années. Je travaille avec le DNS pour le FAI, dans les résolveurs DNS. J'adore cet environnement DNS, et je suis ingénieure en systèmes. Merci.

Claire C. van Zwieten - Internet Society Foundation: Génial. Merci pour le partage.

Marko, voudrais-tu prendre la parole ensuite ?

Marko Paloski - Netcetera: Oui. Merci. Bonjour à tous. Je suis Marko Paloski, je viens de Skopje, en Macédoine, et je travaille comme ingénieur système dans une entreprise privée, principalement sur la partie infrastructure. En plus de cela, je suis également coordinateur du chapitre macédonien du Forum sur la Gouvernance de l'Internet, et j'ai fait partie de la bourse de la Société de l'Internet, ainsi que de la bourse de la prochaine génération d'ICANN.

Donc, je dirais que c'est à peu près tout pour moi. En tant que technicien, je suis plus intéressé par la cybersécurité, la confidentialité, la sécurité en ligne, la fragmentation de l'Internet et la régulation des plateformes, ce genre de sujets. Mais oui, merci beaucoup.

Claire C. van Zwieten - Internet Society Foundation: Merci, et j'adore que Marko souligne une fois de plus que tous les membres de ce panel sont à la fois des anciens de l'ISOC et de l'ICANN. Ce sont tous des experts dans ce domaine et ont suivi les meilleures bourses de l'industrie pour le prouver.

Alors, Jackie, pouvez-vous vous présenter et partager votre opinion sur l'état actuel du DNS ?

Jackie Akello - Research ICT Africa: Merci beaucoup pour cela, Claire.

Bonjour à tous. C'est un plaisir de vous rejoindre pour cet appel, il est six heures à Nairobi. C'est presque le soir ici, ou plutôt c'est déjà le soir.

Je suis chercheur en IA chez Research ICT Africa, et mon travail tourne principalement autour de l'IA et de la gouvernance des données. Je fais principalement de la recherche et de l'analyse des politiques sur des questions d'actualité liées à l'IA et à la gouvernance des données.

En dehors de cela, j'ai également eu le privilège d'être boursier de l'ISOC, donc j'ai fait partie de la cohorte 2020 et j'ai pu assister à l'IGF grâce à cette bourse. J'ai aussi été boursier avec l'ICANN à plusieurs reprises, notamment pour les réunions ICANN 73 et ICANN 77.

C'est un plaisir de vous rejoindre tous lors de cet appel, et j'ai hâte d'entendre vos opinions et de commencer la conversation sur la sécurité DNS. Merci.

Claire C. van Zwieten - Internet Society Foundation: Merci.

Kanaan, aimeriez-vous vous présenter et nous parler un peu de votre activité professionnelle, ainsi que de votre point de vue sur l'état actuel du DNS ?

Kanaan Ngutu - Digital Kiribati: Oui, absolument.

Tout d'abord, c'est un plaisir pour moi de participer à cette conversation, malgré le fait qu'il soit très tôt le matin de ce côté du monde.

Je m'appelle Kanaan, et comme vous l'avez déjà mentionné, nous faisons tous partie des anciens de l'ICANN et de l'ISOC. J'ai assisté à deux réunions de l'ICANN et également à deux réunions de l'ISOC par le passé, et actuellement je travaille sur plusieurs projets. Je fais des travaux de conseil dans le domaine des TIC, je collabore aussi avec l'UIT sur les projets d'îles intelligentes à Kiribati, mais en même temps, je dirige une ONG appelée Digital Kiribati qui œuvre pour promouvoir la cybersécurité et la littératie numérique au sein de la communauté ici à Kiribati.

Claire C. van Zwieten - Internet Society Foundation: Merci.

Je pense que ce que je veux partager, c'est que ce qui est très spécial à propos de ce groupe, c'est qu'ils viennent tous de groupes de parties prenantes très variés. Ils ont tous une opinion et une vision très différentes de la sécurité et de la résilience du DNS.

J'aimerais commencer avec vous, Lia. Quel est le rôle de la sécurité et de la résilience du DNS dans votre travail, et quel est votre avis sur notre position dans ce domaine en octobre 2024 ?

Lia Solis Montaño: D'accord. Le DNS est un service dont la fonction définie est de traduire les noms de domaine en adresses IP. Avec ces adresses, les paquets peuvent suivre le meilleur chemin défini par les équipements de routage. Pouvez-vous imaginer un monde où tous les utilisateurs doivent mémoriser des adresses IP ?

Précisément, l'un des facteurs qui a favorisé la croissance d'Internet en général est la facilité d'utilisation, grâce au DNS. Le DNS est un service crucial pour l'accessibilité à Internet, il mérite donc une attention particulière dans les contextes de sécurité. Pour en citer quelques-uns, nous pouvons mentionner l'empoisonnement des requêtes où les origines des réponses DNS sont modifiées et contiennent de fausses informations pour manipuler la destination des paquets.

La communauté technique travaille dur pour éviter ces menaces.

Claire C. van Zwieten - Internet Society Foundation: Merci. Et vous avez mentionné la communauté technique, ce qui me donne envie de m'adresser à Marko. D'après votre travail et ce que vous faites, comment pensez-vous que le DNS a évolué au cours des 10 dernières années ?

Comment les risques de sécurité, nos modèles de résilience et le DNS ont-ils changé ?

Marko Paloski - Netcetera: Oui. Merci pour la question. Je dirais que même au cours des deux ou trois dernières années, beaucoup de choses ont changé, pas seulement en 10 ans, car dans le monde d'aujourd'hui, chaque année apporte de nombreux nouveaux défis et opportunités, de nouvelles technologies, de nouvelles versions, tout change et va dans une meilleure direction.

Mais oui, je suis d'accord, c'est une bonne question. Nous sommes aussi, en tant que peuple, un peu plus conscients des choses, car nous utilisons maintenant la technologie tous les jours et de plus en plus, mais d'un autre côté, à cause de l'utilisation de certaines de nos compétences, nous manquons encore de connaissances ou peut-être pas de connaissances, mais peut-être de concentration sur les choses.

C'est pourquoi, ces dernières années, je pense que nous avons de plus en plus de cybermenaces, surtout du côté du DNS. Différents types d'attaques. Cela augmente parce que nous sommes maintenant plus dépendants de la technologie que nous avons dans chaque appareil. Même dans les voitures, nous avons de la technologie, des systèmes et un ordinateur, ce qui nous rend plus vulnérables aux attaques. Il y a 10 ans, les cibles étaient peut-être les institutions, les entreprises, les gouvernements. Maintenant, ils sont toujours des cibles, mais l'utilisateur final est également beaucoup visé.

C'est une période difficile.

Nous sommes plus conscients maintenant, car il y a beaucoup d'initiatives. Bien sûr, certaines viennent de l'Internet Society. L'ICANN fait également beaucoup de travail sur la sécurité du DNS, mais je pense toujours que nous sommes loin d'être toujours en sécurité. Le DNS est un système critique, mais c'est l'un des plus ciblés, je dirais, car comme Lia l'a mentionné, c'est l'un des éléments fondamentaux de l'Internet.

Vous ne pouvez pas imaginer Internet sans le DNS, en particulier la sécurité du DNS, qui est aujourd'hui par défaut. Dans le passé, peut-être que vous n'aviez pas besoin d'extensions de sécurité DNS ou de ce genre de choses, mais aujourd'hui, vous ne pouvez pas vous en passer.

Donc, je dirais qu'avec l'avancement de la technologie, il y a aussi l'avancement des attaques et des vulnérabilités. Nous avons maintenant l'intelligence artificielle, vous pouvez demander à GPT d'écrire, ou de vous donner des vulnérabilités d'un site, ou peut-être de vous créer un outil.

D'une part, c'est bien parce que vous pouvez voir et tester plus de systèmes, car vous pouvez voir comment les machines fonctionnent, mais cela donne aussi beaucoup de pouvoir à certaines personnes ou à celles avec de mauvaises intentions. Peut-être

qu'elles n'ont pas de mauvaises intentions, mais quand vous avez l'outil, vous pouvez l'essayer.

Donc, oui, c'est difficile, mais notre travail est très crucial, tant pour les techniciens que pour les décideurs politiques et toutes les autres personnes, car le sujet est important. Le multistakeholderisme ici est l'une des choses cruciales, car je pense que l'Internet est basé sur le multistakeholderisme et il devrait continuer ainsi. Chaque partie prenante, leur travail est très crucial, surtout en ces temps que nous traversons actuellement.

Je ne sais pas si j'ai directement répondu à toute la question ou si je me suis un peu égaré, mais j'ai voulu essayer de donner une réponse.

Claire C. van Zwieten - Internet Society Foundation: Vous avez certainement soulevé un point très important, à savoir que plus nos vies deviennent de plus en plus numériques, plus elles sont également vulnérables, car comme vous l'avez dit, dans nos voitures et tout, nous avons un ordinateur de nos jours, donc il est logique que plus nous utilisons ces choses, plus notre vulnérabilité augmente.

Et Kanaan, je veux m'adresser à vous, car je sais que vous travaillez beaucoup avec la communauté dans votre région. Et, comme vous faites également beaucoup de cybersécurité, je suis curieux de savoir comment vous avez pu parler de ce sujet aux gens de votre communauté, et si vous avez trouvé des moyens de combler un fossé technique pour les personnes qui connaissent évidemment Internet, mais qui ne savent pas nécessairement quelles infrastructures sont en place pour le maintenir aussi sûr qu'il l'est.

Comme l'a dit Marko, vous ne pouvez pas avoir Internet sans DNS, mais beaucoup de gens ne le savent pas, en fait. Alors, quand vous parlez de cybersécurité à votre communauté, comment parvenez-vous à intégrer cela ?

Kanaan Ngutu - Digital Kiribati: Ma discussion sur ce sujet tournerait autour de l'expérience du Pacifique, venant du Pacifique Sud.

Nous connaissons le DNS tel qu'il est, et son rôle dans toute l'infrastructure de l'Internet. C'est l'un des éléments cruciaux qui doit être protégé. Le DNS, nous connaissons son importance, car il peut déterminer le sort de l'Internet, et pour que les ressources soient accessibles sur Internet, nous avons besoin de cet élément critique.

C'est particulièrement vrai dans le contexte des îles du Pacifique. Nous avons opéré de l'autre côté du monde, pratiquement inconnus de la plupart des gens dans le monde occidental, mais entièrement dépendants d'Internet, et nous avons des parties prenantes impliquées dans la configuration d'Internet tel qu'il est, et pour l'avenir.

Mais, malheureusement, la plupart des gens, en particulier ceux qui sont censés jouer un rôle dans la maintenance de cette ressource, ne connaissent pas nécessairement cet élément crucial de l'Internet, n'est-ce pas ? Je pense que cela souligne l'importance d'impliquer de plus en plus de personnes, et je crois que l'engagement des gens commence par renforcer leurs compétences.

Comme vous l'avez justement mentionné, j'ai appris beaucoup de choses, et l'une d'elles est que la plupart des gens manquent de connaissances sur le DNS. Ils ne savent même pas quelles sont les vulnérabilités, quelles sont les menaces de sécurité qui compromettent les opérations DNS dans le Pacifique, et quand on parle de cybersécurité, les gens de ma communauté ont tendance à être très vulnérables par rapport aux personnes d'autres régions du monde. En partie parce qu'Internet est relativement nouveau dans notre horizon comparé à certaines personnes situées peut-être aux États-Unis ou en Europe.

Vous pouvez imaginer utiliser Internet pour la première fois, avec ses vastes ressources. Les gens croient que l'Internet est une très bonne chose, c'est un fait, mais ils ne connaissent pas les menaces qui se cachent à l'intérieur. Il y a des choses comme l'abus d'enfants en ligne, les escroqueries et les attaques qui sont menées sur les réseaux, ainsi que sur les individus.

Donc, ce sont les choses dont les habitants du Pacifique manquent de connaissances, ce qui les rend d'autant plus vulnérables à ce genre d'attaques. C'est la même chose avec DNSSEC, et je crois que les gens se rendront compte de l'importance de se perfectionner et de rester informés et engagés dans ce domaine très important lorsqu'ils seront attaqués.

Claire C. van Zwieten - Internet Society Foundation: Merci pour cette réponse. J'aime ce que vous avez dit et je pense que vous soulevez un excellent point en parlant de capacité : les gens ne savent pas ce qu'ils ne savent pas, et s'ils avaient les ressources pour apprendre les meilleures façons de se protéger, cela pourrait leur être plus facile.

Heureusement, en 2024, nous avons l'IA, ce qui offre de nombreuses nouvelles opportunités pour renforcer les capacités des gens dans divers domaines. J'aimerais passer à Jackie et voir si elle peut nous apporter des informations ou des éclairages sur le rôle de l'IA et du DNS, et si les gens utilisent l'intelligence artificielle pour s'auto-former ou pour se protéger davantage.

Jackie Akello - Research ICT Africa: Merci beaucoup pour cette question, Claire. Mes collègues ont partagé des informations très importantes sur la sécurité du DNS, ainsi que sur l'état actuel du DNS dans le monde. Je vais donc partager quelques réflexions sur le rôle de l'IA, en particulier pour maintenir le système DNS.

Ce que vous avez vu récemment, en particulier ces dernières années, c'est que l'IA a vraiment progressé et nous avons maintenant l'IA générative et ChatGPT. Le rôle que je

vois pour l'IA, en particulier dans le contexte africain et aussi pour les personnes au niveau local et dans les systèmes éducatifs, c'est qu'elle éduque désormais les gens sur les systèmes DNS. Les gens peuvent voir à quel point le système DNS est crucial, comment il fonctionne en tant qu'infrastructure, et aussi comprendre le rôle essentiel qu'il joue.

Un autre aspect est que l'IA, grâce aux outils éducatifs, expose également les gens aux dangers qui peuvent menacer les systèmes DNS. Les gens savent que, bien que l'infrastructure DNS soit cruciale, simplement communiquer et se connecter les uns aux autres comporte des risques lorsqu'on utilise d'autres systèmes. Ils sont également informés sur la manière de se protéger.

Un autre aspect est que l'IA est également utilisée pour causer de l'insécurité dans le système DNS, donc tout ce qui concerne la cybersécurité, les dommages et même les attaques, est créé simplement par l'utilisation de systèmes d'IA. C'est un risque crucial qui doit vraiment être abordé en ce qui concerne les systèmes DNS et l'IA.

L'IA joue également un rôle crucial en matière d'élaboration de politiques autour des systèmes DNS, car elle rassemble des parties prenantes essentielles impliquées dans le développement de ces systèmes d'IA, et permet le partage de connaissances sur la manière de prévenir et de réduire certains de ces préjudices.

Ainsi, l'IA joue un rôle crucial en matière de sécurité du DNS, ainsi que dans l'avancement de l'élaboration des politiques autour du système DNS.

Claire C. van Zwieten - Internet Society Foundation: Merci. C'était une excellente réponse. Je pense qu'il est vraiment important que les gens ordinaires, le caissier à l'épicerie, votre mère, votre père, que tout le monde sache comment se protéger et connaître les meilleures pratiques pour la sécurité DNS.

Si vous pouviez dire, j'aimerais que chacun de nos panélistes réponde à cette question, si vous pouviez donner un conseil pratique aux personnes qui veulent se protéger et s'assurer qu'elles maintiennent un système résilient avec une sécurité DNS robuste, que leur suggéreriez-vous ?

Et nous pouvons commencer avec Lia.

Lia Solis Montaño: Nous pouvons parler des meilleures pratiques, par exemple. Il est important de comprendre les recommandations pour le déploiement et l'exploitation du service de résolution de noms, mais aussi d'être ouvert au fait que ces recommandations sont des opérandes dynamiques basées sur chaque menace identifiée sur Internet.

Nous pouvons citer quelques bonnes pratiques, par exemple, avoir des DNS autoritaires et des DNS résolveurs dans des outils d'infrastructure différents, assurer la redondance des serveurs DNS de la manière la plus transparente possible pour l'utilisateur. L'une d'elles peut être l'utilisation de clouds anycast, qui nous permet d'avoir des serveurs avec la même adresse IP identifiant différents emplacements géographiques.

D'autre part, effectuez un bon dimensionnement de l'infrastructure en fonction du trafic généré par les utilisateurs du réseau. Ces mesures restreignent spécifiquement les requêtes récursives aux adresses IP des utilisateurs cibles, garantissent la véracité des réponses aux requêtes chargées dans DNSSEC ?

Le meilleur guide pour le DNS KIND est de se référer aux plateformes d'apprentissage fournies par l'ICANN, ainsi que par l'Internet Society, concernant ces sujets.

À ce stade, j'aimerais ajouter que toutes les parties doivent comprendre que le DNS n'est pas un outil de blocage. C'est un sujet très vaste qui pourrait être abordé dans un autre webinaire, mais je considère qu'il est important de le mentionner pour orienter la réflexion des différents acteurs.

Merci.

Claire C. van Zwieten - Internet Society Foundation: Merci, et merci d'avoir partagé que l'ICANN et l'Internet Society disposent de grandes ressources sur la sécurité DNS, ainsi que des meilleurs guides pour se protéger. Merci de l'avoir mentionné, je pense que c'est important pour le public de le savoir.

Et ensuite, Marko, j'aimerais aussi entendre votre réponse sur les meilleures pratiques en matière de sécurité DNS, et ce que l'utilisateur moyen peut faire pour se protéger.

Marko Paloski - Netcetera: Oui. Cela dépend du système, bien sûr, mais il existe de nombreuses bonnes pratiques. Comme vous l'avez mentionné, il y a beaucoup de ressources de la part de l'Internet Society et de l'ICANN qui vous aident à choisir ou à trouver ce qui est pertinent. Parce que, ce n'est pas toujours l'organisation, l'entreprise ou l'individu qui a les connaissances ou les ressources, et ces ressources ne sont pas toujours financières, mais aussi des personnes compétentes qui savent quoi faire.

D'un point de vue technique, la mise en œuvre de la sécurité DNS, DNS sécurisé, il y a 10 ans, c'était peut-être une fonctionnalité avantageuse ou quelque chose comme ça, donc de haut niveau, mais aujourd'hui, je pense que c'est l'une des bases que vous devez d'une certaine manière mettre en place, si vous voulez avoir un DNS sécurisé ou un système sécurisé, car le DNS est l'un des éléments essentiels que si un hacker parvient à compromettre, votre entreprise ou votre organisation devient vulnérable et ouverte aux attaques, ouverte à un hacker.

Il y a beaucoup d'autres choses qui existaient peut-être dans le passé, d'autres peut-être pas, mais avec l'essor des nouvelles technologies et leur utilisation quotidienne, beaucoup d'entre elles sont spécifiées et peut-être avancées. Je mettrais donc l'accent sur la surveillance et la journalisation du trafic DNS. Surtout avec l'IA aujourd'hui, il existe de nombreux systèmes capables d'analyser le comportement du réseau, de voir les requêtes, ce genre de choses, mais aussi de vérifier manuellement. Car, à mesure que les machines de défense ou l'intelligence artificielle progressent, les attaquants progressent également. Les deux côtés ont leurs bons et mauvais aspects, et toujours, quand un côté avance, l'autre finira par avancer aussi après un certain temps.

Il existe de nombreuses listes noires appliquant des limitations de taux, c'est-à-dire combien de requêtes peuvent être envoyées, reçues ou traitées dans un certain laps de temps. Selon les systèmes, on peut constater que, surtout lors des attaques DDoS, de nombreuses entreprises et sites limitent le nombre de requêtes sur une période donnée. Je pense que c'est une chose très intelligente et utile à mettre en place, en fonction du système et de l'objectif.

Ensuite, avoir des serveurs DNS redondants, les attaques DDoS, l'idée principale est de désactiver ou de retirer la capacité du serveur, donc si vous avez des redondances, c'est peut-être une meilleure infrastructure en un sens, ou plus résiliente.

Toujours, il est également important pour l'utilisateur final d'avoir toutes les mises à jour, ou l'application à jour, le système d'exploitation, le BIOS, le réseau, les commutateurs, cela dépend de la taille et de la nature de l'entreprise, mais tout doit être à jour. C'est une chose simple et facile, mais souvent les gens oublient de faire ce genre de choses. Surtout, même pour nos téléphones quand nous ne les mettons pas à jour ou que nous oublions de mettre à jour l'application, mais si vous regardez l'historique des attaques, ou ce qui se passe ou ce qui a fait la une, nous pouvons voir que beaucoup de choses étaient dues à des logiciels non mis à jour, des versions plus anciennes, et ce genre de choses.

Bien sûr, il n'est pas toujours possible d'être à jour en raison de certaines limitations ou des applications que vous utilisez, mais cela reste crucial. Si vous constatez qu'un logiciel n'a pas été mis à jour, je l'attribuerai toujours à une personne, une erreur, car quelqu'un doit effectuer la mise à jour, ce n'est pas comme si une IA le faisait automatiquement. Donc, la plupart des attaques qui se sont produites sont des erreurs des employés ou des personnes qui maintiennent ou travaillent sur les serveurs.

Il y a quelques autres choses. Liste noire, également filtrage DNS. Cela se produit aussi de temps en temps, parfois pour une bonne utilisation, mais parfois pour une mauvaise utilisation, certaines régions ou pays étant limités dans l'accès ou l'envoi. Dans un bon sens, je dis que vous pouvez limiter si des demandes malveillantes ou spécifiques arrivent, mais dans de mauvais moments, comme quelqu'un l'a mentionné parmi les panélistes, le DNS n'est pas un moyen de bloquer Internet ou d'empêcher l'accès, mais

de donner accès. Nous pouvons voir dans certains cas que parfois le DNS est utilisé par certains États pour bloquer.

Et, oui, toujours la liste de contrôle d'accès, et peut-être limiter les zones de transfert. Cela concerne plus spécifiquement les parties techniques, où le transfert d'adresses IP, ou la possibilité d'en obtenir une nouvelle, ou quelque chose comme ça.

Ce sont cinq, six, sept que j'ai mentionnés, mais ce sont les bases. Il y en a beaucoup de plus compliqués, et je sais qu'au travail, nous avons des logiciels, dont je ne savais pas qu'on pouvait appliquer ce genre de restrictions sophistiquées, mais cela a du sens après avoir vu le type d'attaques qui arrivent.

Donc, vous essayez toujours de vous protéger contre tout type de menace, même si ce n'est pas une menace, juste pour être protégé, car parfois, peut-être que demain, cela deviendra une menace, même si aujourd'hui ce n'en est pas une, donc je donnerai cela comme meilleures pratiques.

Claire C. van Zwieten - Internet Society Foundation: Je voudrais rapidement, pendant que nous vous avons, Marko, partager une question posée dans le chat par Sana. Elle dit : Merci à tous de partager vos connaissances importantes avec nous. Vous avez mentionné l'importance de la collaboration multipartite dans la sécurité DNS. Pourriez-vous partager vos réflexions sur les étapes pratiques spécifiques que différents acteurs tels que les entreprises privées, les agences gouvernementales et les experts techniques peuvent prendre pour améliorer la collaboration dans la sécurisation d'un système DNS ? Y a-t-il des domaines particuliers où le travail d'équipe peut être amélioré face aux menaces existantes et émergentes ?

J'aimerais en fait que le plus grand nombre possible de nos panélistes, s'ils se sentent à l'aise, partagent leur point de vue sur cette question, car c'est une excellente question. Alors, Marko, puisque la question vous était adressée, aimeriez-vous répondre ?

Marko Paloski - Netcetera: Je peux dire que c'est une très bonne question parce que parfois, surtout dans le cadre de la corrélation DNS, quand on parle des entreprises, car je travaille aussi dans une entreprise privée, ce n'est pas très bien compris. Si elles comprenaient les avantages que ce multistakeholderisme peut apporter, je pense que tout le monde le voudrait. Bien sûr, parfois, c'est un manque de connaissance sur le fonctionnement de cette chose.

Je pense que le multilatéralisme est une très bonne approche, surtout sur ce sujet, car l'Internet et la gouvernance de l'Internet sont basés là-dessus, surtout lorsque, comme vous l'avez mentionné, les entreprises privées, les agences gouvernementales, les experts techniques, n'ont pas toujours les ressources et les connaissances nécessaires.

Peut-être que certaines institutions ont de très bonnes connaissances en cybersécurité, d'autres ont peut-être les logiciels, mais elles n'ont pas les ressources, et il est très crucial d'avoir une coopération et une communication entre elles. De plus, je viens d'un petit pays, la Macédoine. Nous avons un CERT, mais il est très petit et n'est pas vraiment préparé pour de grandes attaques ou quelque chose de ce genre.

Souvent, ce que je vois, c'est que parfois les entreprises aident le gouvernement ou certaines organisations à atténuer ce genre d'attaques. Malheureusement, il n'existe pas de plateforme mondiale à laquelle chaque pays ou chaque entreprise peut adhérer, mais il y a beaucoup d'initiatives en cours auxquelles des individus, des gouvernements ou des entreprises privées peuvent participer.

C'est très agréable de mentionner, ici, parce que nous faisons partie de ce webinaire, je peux souligner qu'il y a quelques organisations qui font différentes choses sur le multilatéralisme, pour les meilleures pratiques et aussi l'établissement de normes. L'ICANN fait beaucoup, également le groupe de travail de l'ingénierie Internet développe les normes, ils développent les meilleures pratiques, que vous pouvez trouver sur le site.

La Société Internet en fait également partie, avec l'ICANN dans la défense des politiques et la sensibilisation. Il y a beaucoup d'initiatives de la part de la Société Internet auxquelles les gens peuvent participer, et il y a aussi un réseau d'experts où vous pouvez partager ou poser des questions sur les forums. Il y avait l'Institut de l'Abus des DNS, mais je pense qu'ils ont changé de nom, c'est plus axé sur la réponse aux incidents, la mitigation et la collaboration sur ce genre de choses.

Donc, il existe de nombreuses plateformes ou peut-être des forums qui peuvent être utiles pour les entreprises, les organisations, et ce genre de choses. Pour les organisations, je ne dirais pas tant que ça, mais pour les entreprises et les gouvernements, je vois un manque de bénéfice à les rejoindre ou à les utiliser autant.

L'entreprise, parfois elle dit non, nous ne pouvons pas payer quelqu'un, nous pouvons résoudre cela, nous ne voulons pas collaborer, ou parfois l'entreprise ne veut pas partager ce qui s'est passé, même publiquement.

Et le gouvernement, cela dépend du gouvernement, bien sûr, parfois ils veulent juste gérer les choses eux-mêmes. Nous avons eu un cas dans notre pays où un serveur a été attaqué, mais il s'est avéré qu'ils étaient ceux qui avaient organisé cela, pour voler ou blanchir de l'argent.

Donc, parfois c'est un problème, mais c'est une chose très cruciale, car si tout le monde coopère, il sera beaucoup plus facile de réduire les attaques et aussi d'être plus sûr et sécurisé.

Claire C. van Zwieten - Internet Society Foundation: Je suis d'accord avec vous, ce que vous dites sur le fait que les gouvernements essaient de le faire seuls. Bien sûr, ils ont probablement une grande variété de compétences au sein de ce gouvernement, mais en réalité, rien de formateur, rien de véritablement robuste ne se produit seul.

Donc, j'aimerais vraiment inviter Jackie et lui demander son avis sur l'approche multipartite de la sécurité et de la résilience du DNS, et où il y a des opportunités accrues de collaboration qui devraient probablement être explorées.

Jackie Akello - Research ICT Africa: Merci beaucoup, Claire.

Le multilatéralisme joue en fait un rôle très important dans la sécurité et la résilience des systèmes de noms de domaine. Ces organisations rassemblent divers acteurs, y compris les gouvernements, les entités privées, les organisations de la société civile, ainsi que des experts techniques.

Lorsque ces organisations se réunissent, elles veillent à ce que des perspectives diverses et les intérêts qui façonnent les politiques, les normes techniques et les cadres soient partagés. Elles permettent ainsi une gouvernance d'Internet de manière significative et fructueuse, ce qui renforce la sécurité de notre DNS.

L'importance réside en fait dans le maintien d'un Internet ouvert, inclusif et résilient qui reflète les besoins de tous les utilisateurs, tout en abordant les complexités d'un réseau mondial interconnecté.

Je pense que le modèle multipartite joue un rôle clé dans la sécurité du DNS en raison des valeurs uniques qu'il apporte à l'élaboration des politiques. Par exemple, il permet l'inclusivité et la représentation. Ce qui se passe, c'est que les organisations multipartites rassemblent en fait différentes voix provenant des gouvernements, du secteur privé et des entités techniques. En fin de compte, cette inclusivité garantit que la gouvernance de l'Internet reflète réellement les besoins diversifiés et les priorités, plutôt que de favoriser un groupe particulier dans l'écosystème du DNS.

Un autre avantage du multistakeholderisme est qu'il permet la transparence et la responsabilité. Les décisions sur le DNS prises par des processus multipartites sont généralement plus transparentes et responsables lorsque diverses entités ont été impliquées dans la formulation de ces décisions.

Des organisations telles que l'IGF créent des forums ouverts où les politiques et pratiques peuvent être débattues. Elles peuvent être discutées et examinées par des personnes ayant différentes expertises dans les systèmes DNS. Ce qui se passe en fin de compte, c'est que les gens partagent les meilleures pratiques pour gouverner les systèmes DNS de la meilleure manière possible à l'avenir.

Un autre avantage du multilatéralisme est l'innovation et la réactivité. Comme nous le savons tous, la technologie progresse à un rythme très rapide. Ainsi, lorsque vous impliquez des personnes de différents secteurs, par exemple des organisations de la société civile, ce qui se passe, c'est que les gens partagent leur expérience et même leur expertise sur les technologies actuelles que nous avons, cela garantit que les lois actuelles que nous avons sont également en phase avec les avancées technologiques.

Les gens peuvent partager ce qui se passe dans le domaine technologique, quelles nouvelles technologies sont lancées, et quelles considérations et mesures politiques doivent être mises en place pour assurer la sécurité du DNS.

Un autre avantage de cela est qu'à la fin de la journée, tous les intérêts ont été pris en compte, ce qui garantit un équilibre en termes d'intérêts présentés lors des débats sur les questions DNS. Nous avons différents secteurs, nous avons la société civile, nous avons le gouvernement et les décideurs politiques. Lorsqu'ils sont tous réunis autour de la table, qu'ils discutent et qu'ils s'accordent sur des questions clés, ce que nous obtenons à la fin de la journée, c'est que leurs intérêts sont équilibrés et que chacun a été pris en compte en termes d'opinion sur la sécurité du DNS.

Une dernière chose que je peux dire sur le multilatéralisme est qu'il renforce également la confiance et la légitimité du système, car toutes les voix ont été prises en compte. Chacun a pu exprimer son opinion en matière d'élaboration des politiques sur le DNS et même sur la sécurité du DNS.

Ce qui se passe, c'est que quelles que soient les règles et politiques adoptées à la fin de la journée, elles peuvent être considérées comme légitimes parce que la voix de chacun a été prise en compte dans l'élaboration de ces politiques, et l'avis de chacun a également été considéré.

Donc, ce que nous obtenons au final, c'est une garantie de légitimité par rapport à un groupe isolé qui prendrait des décisions sur les questions de DNS et adopterait des politiques. Quand cela se produit, il y a beaucoup de méfiance, et les gens ne considèrent pas ces politiques et décisions comme légitimes.

En résumé, je dirais que ce sont quelques-uns des avantages que nous avons avec le multilatéralisme dans le système.

Merci,

Claire C. van Zwieten - Internet Society Foundation: et merci d'avoir évoqué l'aspect important de la confiance par conception. Lorsque nous élaborons des politiques et des systèmes en tenant compte de la sécurité et de la confiance, cela a un effet d'entraînement sur les utilisateurs et la communauté qui utilise ces systèmes. Donc, merci d'avoir soulevé ce point et d'avoir également mis en lumière l'aspect politique.

C'est une transition parfaite pour faire intervenir à nouveau Kanaan. Il est consultant en politiques, et j'aimerais beaucoup entendre votre expérience en matière de création de politiques et de consultation sur des politiques telles que le DNS, ainsi que les défis et les opportunités que vous avez rencontrés dans ce processus.

Kanaan Ngutu - Digital Kiribati: Encore une fois, en parlant des îles du Pacifique, je veux m'exprimer dans mon propre contexte, et je pense que l'expérience est similaire avec le DNS et dans tous les autres domaines de la politique.

Cela a commencé par impliquer les parties prenantes, qui sont censées être impliquées, pour mieux comprendre la nature du travail, et cela afin de s'assurer qu'elles puissent contribuer de manière significative à la discussion et à la formulation des aspects politiques du DNS dans le Pacifique. Comme je l'ai mentionné auparavant, peu de gens comprennent cela.

Je comprends qu'il existe un certain nombre de plateformes créées sur la scène internationale qui favorisent l'engagement dans ce domaine, mais l'un des principaux défis que nous avons à Kiribati et dans les îles du Pacifique, c'est que nous avons un fuseau horaire très différent de celui des autres pays.

Il est donc clair que nous devons créer notre propre espace, comme un sous-espace, qui encouragerait les parties prenantes locales à s'impliquer à un niveau personnel. Ce que je veux dire par là, c'est qu'à Kiribati, nous essayons d'identifier des champions, des champions qui encourageraient les artistes à se joindre à nous et à discuter de ces sujets. C'est là que le soutien de l'ICANN et de l'ISOC pour produire les ressources que nous pouvons utiliser localement, et que nous pouvons traduire, est crucial, afin de garantir que les personnes intéressées aient une compréhension complète, car c'est à partir de là que nous commencerons à renforcer les capacités au niveau local.

Au fur et à mesure qu'ils mûrissent ou qu'ils acquièrent les connaissances nécessaires, ils pourront utiliser cela et porter les engagements au niveau régional, puis au niveau mondial ou international, en termes de discussion des questions liées à la politique.

Je pense que c'est ainsi que nous devrions commencer dans le Pacifique, et cela s'applique également à d'autres parties du monde qui se considèrent isolées de la communauté mondiale. Vous devez commencer au sein de votre propre société, impliquer les parties prenantes et renforcer leurs capacités, car à partir de là, vous pouvez vous assurer que, lorsqu'elles voudront passer à l'étape suivante, elles seront plus pertinentes et efficaces dans ce domaine.

Cela s'applique au DNS, et cela s'applique également à tous les domaines où vous devez développer des politiques et adopter un modèle multipartite.

Claire C. van Zwieten - Internet Society Foundation: Le rôle des champions dans la création de systèmes et de politiques robustes qui protègent et défendent Internet est crucial. Un petit coup de pub ici, c'est quelque chose de vraiment formidable chez l'ICANN et l'Internet Society, c'est que nous sommes capables d'avoir ces programmes que tous ceux qui participent à cet appel ont suivis, et grâce à cela, vous avez pu devenir des champions à part entière, et des champions de l'Internet.

Qu'il s'agisse de technique ou de politique, ou de quoi que ce soit, vous avez pu prendre ces compétences et les ramener dans votre communauté pour les mettre en œuvre de manière positive. Il est important que nous continuions à créer et à développer des champions comme vous quatre, afin que vous puissiez vraiment faire, honnêtement, le travail de défense de l'Internet. C'est vraiment vous, sur le terrain, dans vos postes, dans vos emplois et dans votre vie, qui protégez l'Internet et faites tout ce qu'il faut faire.

Merci beaucoup à vous tous pour tout ce que vous faites, et merci infiniment pour tout ce que vous avez apporté à cette conversation.

Avant de devoir conclure en raison du temps, j'aimerais répondre aux trois questions que nous avons dans la session de questions-réponses, et je commencerai par la première de Ryan Uddin. Quelles vulnérabilités dans le DNS le rendent susceptible aux attaques de spoofing ? Voulez-vous répondre à celle-ci, Lia ?

Lia Solis Montaño: D'accord. Lorsque nous devons vérifier l'adresse IP, nous devons mettre en œuvre ces méthodes de falsification dans notre infrastructure, et le principe pour cela est DNSSEC.

Claire C. van Zwieten - Internet Society Foundation: Merci.

Ensuite, nous avons une autre question de Nicolas, qui est l'un des anciens de l'Internet Society. Il demande : Comment le cadre KinDNS peut-il être optimisé pour prendre en charge des algorithmes cryptographiques résistants aux quanta, quelle collection de mots, wow ! et DNSSEC, alors que les avancées en informatique quantique, comme le recuit quantique, menacent les méthodes de chiffrement traditionnelles comme le RSA 2048.

Nicolas, tu mets à l'épreuve ma capacité à parler aujourd'hui. Wow !

Alors, Marko, voudrais-tu t'en charger ?

Marko Paloski - Netcetera: Je vais essayer, car je ne suis pas très versé dans l'informatique quantique et ce genre de cryptographie, mais je sais que Nicolas l'est beaucoup. L'année dernière, au FGI à Kyoto, il en discutait et posait des questions à ce sujet.

Je ne suis pas sûr, mais je sais que ce cadre KinDNS, qui vient de l'ICANN, incarne l'idée dont j'ai parlé précédemment, le multilatéralisme et un lieu pour les meilleures pratiques. C'est un exemple de ce que fait l'ICANN avec ce cadre.

Mais, comment optimiser les algorithmes cryptographiques résistants aux quanta ? C'est une bonne question.

Claire C. van Zwieten - Internet Society Foundation: Tu as dit ça avec une telle aisance. Tu rends ça tellement facile.

Marko Paloski - Netcetera: Oui, il parle comme dans une conversation de café normale, mais je pense que la cryptographie, surtout maintenant avec l'informatique quantique, nous sommes encore loin de ce genre de gros traitements, mais un jour nous y arriverons. L'informatique quantique joue un grand rôle maintenant, surtout en cryptographie pour ceux qui sont moins sécurisés, car il sera beaucoup plus facile, avec l'informatique quantique, de déchiffrer ou de trouver la clé de cryptage.

Cette technologie est relativement nouvelle. Elle est encore en phase de recherche, il y a quelques projets commerciaux qui s'y consacrent activement, mais je pense que la plupart des systèmes vont devenir plus avancés et qu'il sera plus facile de les mettre en œuvre ou de les optimiser.

Comme je l'ai mentionné, je ne suis pas vraiment sûr parce que je ne suis pas tellement impliqué dans l'informatique quantique, et surtout dans le chiffrement avec l'informatique quantique, mais mon idée est qu'avec le temps, les systèmes seront plus avancés, plus faciles à optimiser ou à configurer avec les deux choses, car il y aura plus de possibilités pour cela.

Je ne suis pas sûr d'avoir répondu. Connaissant Nikolas, je sais que ce n'est pas la réponse complète.

Claire C. van Zwieten - Internet Society Foundation: Malheureusement, Jackie doit nous quitter, mais merci beaucoup, Jackie, pour toutes vos précieuses informations aujourd'hui, et merci d'avoir apporté votre expertise en DNS et en droit à cette discussion.

Nous avons maintenant une autre question : Quelles mesures peuvent être prises pour encourager l'adoption généralisée des pratiques de sécurité ?

Je voudrais aller à Canaan pour celui-là.

Kanaan Ngutu - Digital Kiribati: La réponse est évidemment que nous devons sensibiliser davantage les gens, en particulier les organisations. Elles doivent être plus

conscientes des menaces et aussi être guidées et formées sur les mesures à prendre pour commencer à mettre en place des sécurités autour de l'infrastructure DNS.

C'est ce qui est très important pour moi, car, d'après ce que je sais, dans de nombreuses organisations avec lesquelles j'ai travaillé, la plupart des gens, même dans le département TIC, ne savent même pas comment prendre des mesures pour protéger leur infrastructure DNS, surtout dans le contexte spécifique.

Encore une fois, leur réseau est si simple, il n'y a aucune sophistication, alors comment peuvent-ils mettre en œuvre le DNS s'ils n'ont pas une infrastructure réseau adéquate ?

Donc, pour encourager les gens à adopter et mettre en œuvre les meilleures pratiques, nous devons les éduquer et leur montrer comment cela se fait.

Je pense qu'à partir de là, ils peuvent développer leurs connaissances pour aller de l'avant.

Claire C. van Zwieten - Internet Society Foundation: C'est une excellente question et une excellente réponse. J'aimerais que Lia aborde également ce sujet, et je pense que ce sera la dernière question à laquelle nous répondrons avant de devoir malheureusement clôturer le webinaire. Mais Lia, j'aimerais savoir ce que nous pouvons faire pour augmenter les taux d'adoption du DNS.

Et quel était l'autre acronyme amusant ? Le KinDNS.

Lia Solis Montaño: KinDNS nous offre un guide standard pour utiliser le DNS. C'est ce avec quoi nous pouvons commencer pour ceux d'entre nous qui cherchent un guide. Les bonnes pratiques sont dynamiques et s'adaptent aux besoins du moment. Nous pouvons certainement apporter des contributions dans chaque situation qui peut se présenter. N'oubliez pas que nous avons des communautés préoccupées par cette utilisation.

Claire C. van Zwieten - Internet Society Foundation: Merci beaucoup. Et je pense que ce que cette personne a également demandé, c'est ce que nous pouvons faire pour nous assurer que nous établissons des normes de sécurité adéquates pour ce type de systèmes.

L'un de vous a-t-il des idées sur l'importance ou la capacité d'établir des normes ?

Marko Paloski - Netcetera: Consultez les meilleures pratiques, vérifiez ce qui est connu au niveau international et auprès d'organisations comme l'ICANN ou l'Internet Society.

Vérifiez également auprès de votre pays ou de votre communauté locale ce que font les autres, les institutions ou les gouvernements, ou s'il existe une loi. Je ne sais pas à ce sujet, mais vérifiez quand même. Même s'il n'y a rien, essayez de proposer quelque chose et voyez si c'est bon. Sinon, changez-le.

Ce genre de choses ne se fait pas une fois pour toutes, il faut constamment les revoir et les mettre à jour car la technologie évolue, les attaques changent, donc il faut que ce soit à jour.

C'est tout.

Claire C. van Zwieten - Internet Society Foundation: Génial. Et, sur cette note parfaite, nous devons mettre fin à ce webinaire. Un grand merci à nos intervenants. Merci d'avoir pris le temps, dès le matin, de partager votre expertise et votre temps avec nous.

Merci à tout notre public. Merci d'être venus. J'espère que vous avez pu apprendre un peu, et j'ai hâte de vous voir tous à notre prochain événement. Nous nous assurerons de le partager dès que possible. Je vous souhaite à tous une excellente journée.