CLAUDIA RUIZ : Bonjour, bon après-midi et bonsoir à tous. Soyez les bienvenus au cinquième et dernier webinaire des cinq webinaires obligatoires pour ATLAS III. Aujourd'hui, nous allons parler d'une introduction à la cybersécurité. Notre présentateur est David Huberman, spécialiste sénior engagement technique.

Nous n'allons pas faire d'appel nominal pour ce webinaire. Toutefois, nous prenons en considération la participation dans les dix premières minutes de cet appel, à la suite de quoi votre participation ne sera pas prise en compte pour les mesures de participation obligatoire. Si vous êtes uniquement connecté sur le phone bridge, veuillez rejoindre Zoom étant donné qu'il s'agit d'un critère obligatoire.

Nous avons l'interprétation en espagnol et en français, donc veuillez vous rappeler d'indiquer votre nom lorsque vous intervenez pour permettre aux interprètes de vous identifier sur les autres canaux ainsi que pour la transcription. Veuillez également parler à un rythme raisonnable pour permettre une interprétation précise.

Toutes les lignes seront sur muet pendant la présentation puis seront ouvertes pour une séance de questions et réponses à la fin de la présentation.

Comme vous l'aurez remarqué, nous organisons ce webinaire sur la plateforme Zoom dont les caractéristiques sont semblables à Adobe Connect. Mais afin de pouvoir voir la liste des participants et de participer au chat, veuillez cliquer en bas de l'écran sur l'icône. Vous

verrez les échanges sur le chat à partir du moment où vous rejoignez l'appel mais pas avant. Pour lever la main, il suffit de cliquer sur l'icône « Lever la main ».

Je vais maintenant céder la parole à Joanna Kulesza, coprésidente du sous-groupe de travail sur le renforcement des compétences pour ATLAS III. À vous Joanna.

JOANNA KULESZA : Merci beaucoup Claudia. Merci à tous de nous avoir rejoints pour le dernier webinaire pour ATLAS III où la participation est une condition *sine qua non* pour la sélection des participants à ATLAS III.

Sans plus attendre, je vais céder la parole à David, spécialiste sénior engagement technique à l'ICANN. Merci beaucoup David de nous faire cet honneur et on attend avec impatience d'écouter votre présentation. J'ai cru comprendre que les participants sont invités à poser leurs questions sur le chat pendant la présentation. Et je vous laisse le soin, David, de décider d'y répondre pendant la présentation ou bien à la fin. C'est à vous David.

DAVID HUBERMAN : Bonjour à tous. Je vais vous faire une présentation relativement brève aujourd'hui et ensuite, nous aurons une séance assez étendue de questions et réponses. Pendant cette présentation, je ne vais pas laisser mon chat ouvert sur mon écran puisque je veux me concentrer sur la présentation.

Soyez les bienvenus. Aujourd'hui, je vais vous parler de cybersécurité dans l'écosystème ICANN. Je m'appelle David Huberman, je suis spécialiste senior engagement technique au bureau de l'ICANN du CTO. J'ai été aux avant-postes de la cybersécurité depuis environ 21 ans.

Ce webinaire va compléter les cours officiels qui existent déjà sur ICANN Learn. Ce webinaire et cette présentation, c'est notre contribution pour relever les défis en termes de cybersécurité dans l'écosystème ICANN. Et d'autres à l'intérieur de l'organisation ICANN peuvent faire des présentations légèrement différentes et cela n'est pas un problème.

Pour commencer, j'aimerais vous inviter à réfléchir aux choses qu'on peut couramment trouver dans un réseau, un réseau d'une entreprise, un réseau d'une université ou un réseau gouvernemental. Et certaines des choses qu'on va trouver, ce sont les serveurs courriels. Les serveurs courriels, ce ne sert pas uniquement pour les courriels. Les serveurs courriels modernes ont des courriels, évidemment, également des calendriers, toutes les réunions qu'on planifie, les rendez-vous, et incluent aussi les contacts, donc des informations nous concernant et concernant les personnes sur notre réseau.

Un autre élément qu'on trouve couramment dans les réseaux, ce sont les serveurs de base de données qui ont toute une panoplie d'informations, des données sur les biens, sur les clients et parfois sur les employés.

Un autre élément commun qu'on trouve sur les réseaux, ce sont les serveurs fichier, c'est-à-dire les informations financières, les tableurs, les documents de design. Et c'est là qu'on trouve des informations sur nos processus et procédures en termes d'organisation.

Cela semble très simple. Voilà le genre d'informations qu'on trouve dans tout type de réseau. Alors, ensuite derrière ces éléments, il y a des choses très intéressantes. On a la gestion d'identité. Pour avoir accès à nos courriels, aux serveurs fichiers et aux base de données, on doit passer par des processus qui nous autorisent à le faire, des processus qui permettent de nous identifier, savoir quel est notre identifiant, mot de passe et pour plus d'authentification, quel est le jeton d'identité qu'on présente. Et lorsque vous gérez ces systèmes, il faut également gérer les clés, l'identifiant et le mot de passe bien entendu mais aussi les *keys fobs*, les clés cryptographiques et les jetons supplémentaires qui permettent de maintenir et de garantir la sécurité des systèmes. On a également des systèmes d'ingénierie qui sont gérés par des hardware, software, qui ont tous deux besoin d'un patching.

Et ensuite, il y a toute l'infrastructure de routage. Il s'agit d'une activité qui est importante pour notre réseau mais aussi pour les réseaux extérieurs au nôtre. Et dans cette infrastructure, il s'agit des adresses IP et du DNS, le système des noms de domaine.

Et enfin, il y a la composante gouvernance, c'est-à-dire la politique concernant la sécurité ; qui peut avoir accès à ces données et de quelle manière ? Également la politique concernant le stockage des données, où est-ce qu'on stock et pendant combien de temps on stock les données ?

Alors pourquoi est-ce que je vous parle de tout cela ? C'est parce que ce sont ces éléments justement qui font l'objet d'attaques constantes de la part de gens qui essaient de trouver des vulnérabilités dans chacun de

ces éléments que vous voyez à l'écran, des vulnérabilités parce qu'ils peuvent les attaquer et ainsi voler des données.

De quelle manière s'y prennent-ils ? Par exemple, par le biais du hameçonnage. Et là, je vous donne des définitions que j'ai trouvées sur dictonnary.com. Le hameçonnage, il s'agit de la pratique frauduleuse qui consiste à envoyer des courriels qui sont supposés provenir d'une entreprise ayant une bonne réputation afin d'induire les individus à révéler leurs informations personnelles tels que leur mot de passe et numéros de carte de crédit.

Autre type d'attaque, le logiciel malveillant. Il s'agit d'un logiciel qui est spécifiquement conçu pour endommager ou obtenir un accès non autorisé à un système informatique, par exemple les rançons logiciel, les keystroke loggers c'est-à-dire enregistrement de frappes, root kiss, etc.

Ensuite, on a les réseaux zombies. Il s'agit d'un réseau d'ordinateurs privés infectés par un logiciel malveillant et contrôlé par un groupe sans connaissance vis-à-vis de qui contrôle cela. Il s'agit d'une personne qui contrôle tout cela pour mener des attaques.

Autre type très important de délits en termes de cybersécurité, d'attaques cybernétiques, c'est ce qu'on appelle l'utilisation malveillante du DNS. Le DNS est partout. On utilise le DNS à chaque instant pour résoudre des noms, pour obtenir des adresses IP. Et il s'avère que si on modifie, si on dérange le DNS, alors cela a des incidences sur les transactions commerciales, les services gouvernementaux, les réseaux sociaux et bien d'autres choses encore. Si vous exploitez le DNS, alors vous pouvez décevoir les utilisateurs, les tromper. Vous pouvez enregistrer de manière malicieuse les noms de

domaine, vous pouvez pirater la résolution de noms ou les services d'enregistrement et vous pouvez corrompre les données du DNS à la source.

Alors je ne veux pas être trop abstrait, je préfère vous donner des exemples concrets. Et aujourd'hui, j'aimerais partager avec vous deux exemples de cyberattaques très récentes qu'on a pu observer. Et ces deux cyberattaques incluent le ciblage de vulnérabilités dans le système de routage internet et dans le système courriels géré par les compagnies qui ont fait l'objet de ces cyberattaques et l'utilisation malveillante du DNS avec une modification de la résolution de noms dont la personne qui a fait l'objet de l'attaque n'était même pas consciente.

D'abord, il s'agit d'une attaque sur une plateforme de cryptomonnaie où des gens peuvent stocker leur cryptomonnaie. Et les attaquants on pu utiliser un piratage de rouage pour rediriger des requêtes DNS et ce faisant, ils ont pu tromper et décevoir les utilisateurs en volant leurs identifiants de connexion. Et une fois que les attaquants ont pu tromper les utilisateurs, ils ont pu voler près de 21 millions de cryptomonnaie de ce site web.

Le deuxième exemple d'attaque très récente a deux noms, DNSpionage qui a eu lieu en 2018 et une attaque qui est encore en cours et que la communauté de sécurité a baptisé Sea Turtle. Comme beaucoup de cyberattaques, la motivation, c'est l'argent. Il s'agit d'attaques de protocoles. C'est ce qu'on appelle des prépositionnements d'attaques cybernétiques militaires qui connectent des informations relatives aux renseignements nécessaires pour lancer des attaques cybernétiques

militaires. Quarante organisations dans 13 pays en Afrique du Nord et au Moyen-Orient, des organisations de sécurité nationale, ministères des Affaires étrangères et grandes compagnies pétrolières ont été les premières victimes de cela. Infiltration du DNS, courriels et autorités de certification ont été utilisés comme jetons de vérification.

Ce genre d'attaques de grande envergure dont je viens de parler n'est pas très fréquent. Mais en raison de l'ampleur de ces attaques, elles finissent par impliquer des gouvernements souverains, des multinationales, les autorités d'application de la loi sont impliquées aussi. Et finalement, on finit par apprendre ce genre d'attaques de grande envergure dans les journaux.

Mais sachez qu'il y a des incidents en termes de cybersécurité bien plus mineurs qui se produisent au jour le jour. Et aujourd'hui, la communauté de l'ICANN et les membres de l'organisation ICANN, donc le personnel, ont un rôle à jouer dans le domaine de la cybersécurité. Et on a un rôle avant, pendant et après les incidents.

Donc pendant ce séminaire, nous allons décrire le rôle de la communauté et de l'organisation ICANN dans cet écosystème. Et je vais également vous familiariser avec certaines technologies courantes.

Donc commençons avec tout ce qui se passe avant que ne se produise un incident en termes de cybersécurité. Selon les statuts constitutifs de l'ICANN, l'ICANN a une mission très importante à jouer par rapport à la cybersécurité. Et je cite : « La mission de l'ICANN est de garantir un fonctionnement stable et sûr du système d'identifiants uniques de l'internet. »

Dans le cadre de ces statuts constitutifs, l'ICANN a pris un certain nombre d'engagements dont, et je cite : « Préserver et renforcer l'administration du DNS et la stabilité, la sécurité, l'interopérabilité mondiale, la résilience et l'ouverture du DNS et de l'internet. »

Donc, nous avons ces termes que j'ai mis en grands ici sur la diapositive, la sécurité, la stabilité et la résilience. Ce sont des termes que vous allez entendre une fois et encore une fois que vous serez plus familiers de l'écosystème ICANN. Que ce soit dans les discussions, dans les réunions, dans les conférences, on parle toujours de la sécurité, de la stabilité et de la résilience de l'internet et du système des identifiants uniques que l'ICANN aide à coordonner. Et on utilise un acronyme pour ces trois termes avec l'acronyme SSR pour sécurité, stabilité et résilience.

Que veulent dire ces termes ? En fait, c'est assez simple. Sécurité, il s'agit de la capacité à protéger et éviter la mauvaise utilisation ou l'utilisation malveillante des identifiants uniques de l'internet. La stabilité, c'est la capacité de garantir que le système fonctionne tel que prévu et que les utilisateurs des identifiants uniques ont confiance dans le système. La résilience, c'est la capacité du système d'identifiants uniques à faire face à des attaques malicieuses ou à d'autres évènements qui mettent en danger le système.

Et pour répondre à nos engagements vis-à-vis du SSR pour le système des identifiants uniques, l'ICANN a concentré ses efforts dans trois domaines bien distincts. Le premier, c'est l'élaboration de politiques, ensuite les opérations d'identifiants et chaque jour, toutes les semaines, on participe aux efforts de renforcement des capacités pour sensibiliser

et informer les gens des technologies et des tendances dans le domaine de la cybersécurité.

Dans l'écosystème ICANN, il y a tellement de communautés qui travaillent très dur pour mettre en place des politiques de manière ascendante et les procédures afin d'améliorer la sécurité, la stabilité et la résilience du système des identifiants uniques. J'ai mis en exergue la participation de trois organes en particulier. Le GAC a un groupe de travail sur la sécurité publique, le PSWG, qui se concentre sur des aspects, des politiques et procédures de l'ICANN qui impliquent la sécurité du public. La sécurité du public, cela inclut développer la capacité d'atténuation des attaques cybernétiques et la participation des autorités chargées de l'application de la loi.

Outre ce groupe de travail sur la sécurité publique du GAC, il y a le SSAC, le comité consultatif sur la sécurité et la stabilité. Il s'agit d'ingénieurs et d'experts de sécurité qui ont été sélectionnés pour siéger sur un comité et faire des évaluations de menaces et aider l'ICANN à évaluer et à voir où est-ce qu'il y a des menaces potentielles.

La troisième communauté que je souhaitais vous présenter, c'est une toute petite communauté. Il s'agit des opérateurs des serveurs racine. Ils sont rassemblés au sein du RSSAC, donc du comité consultatif sur le système des serveurs racine. Le RSSAC donne des conseils au Conseil d'Administration de l'ICANN et à la communauté sur les questions relatives au fonctionnement, à l'administration, à la sécurité et à l'intégrité du système de serveurs racine.

Alors, autre partie en matière de développement de politiques, il s'agit des contrats, des contrats entre l'ICANN, les bureaux d'enregistrement

et les opérateurs de registre. Et ces contrats sont des outils très importants. Alors je vais passer à la diapositive suivante et j'y reviendrai.

Nous avons beaucoup de contrats dans l'écosystème de l'ICANN. Si vous regardez de gauche à droite en partant d'en bas, vous voyez donc qu'entre l'ICANN et l'opérateur de registre d'un domaine de premier niveau, nous avons donc l'accord de registre, le RA. Et entre l'opérateur de registre et le bureau d'enregistrement, lorsqu'il y a enregistrement des noms de domaine pour des particuliers, vous avez le RAA, l'accord opérateur de registre et bureau d'enregistrement. Et en haut, vous avez l'accord d'accréditation de bureau d'enregistrement qui définit ce que vous devez faire dans vos liens avec l'ICANN si vous êtes bureau d'enregistrement. Et puis vous avez d'autres accords, d'autres contrats entre les revendeurs, les titulaires de noms de domaine, etc.

Je reviens à la diapositive précédente pour souligner les deux contrats les plus importants pour vous expliquer un petit peu en quoi il est important d'en parler aujourd'hui dans le cadre de notre discussion. Donc l'accord entre l'ICANN et les bureaux d'enregistrement en fait impose un devoir de faire une enquête en cas d'abus. L'accord de registre entre l'ICANN et le TLD inclut une disposition comme quoi cet accord bureau d'enregistrement et opérateur d'enregistrement, les bureaux d'enregistrement doivent inclure dans les accords d'enregistrement une disposition qui interdit aux détenteurs de noms de domaine de diffuser des programmes malveillants, d'avoir des réseaux botnet, des réseaux zombies, de diffuser toute opération de hameçonnage, de piratage, d'être en infraction par rapport aux marques de commerce ou au droit relatif à la propriété privée, etc.

Deuxième domaine dans lequel l'ICANN a un engagement, c'est dans le cadre d'une société, une filiale qui s'appelle la PTI, les identificateurs techniques publics. Cette filiale est responsable des aspects opérationnels de coordination du système d'identificateurs uniques de l'internet. Il s'agit là des fonctions IANA.

Les fonctions IANA sont composées de trois volets importants. Premièrement, les ressources en numéros. Il s'agit d'allouer les adresses IPv4, les adresses IPv6 et ce qu'on appelle les numéros AS, système autonome, aux RIR, aux registres qui distribuent ces adresses dans le monde entier.

Deuxième volet important qui est géré par la PTI, ce sont les opérations DNS. Donc il y a beaucoup de travail qui est fait à ce niveau-là et j'ai souligné ce qui était le plus important. Premièrement, entretenir la zone racine pour le fonds DNS ; administrer la zone RPA pour le DNS inversé ; et entretenir l'ancre de confiance pour les DNSSEC. Là-dessus, je rentrerai un petit peu dans les détails pour que vous compreniez mieux en quoi c'est important.

Troisième tâche de la PTI, c'est ce qu'on appelle les registres de paramètres de protocole. Vous avez l'IETF, le groupe de travail sur le génie internet, qui crée les protocoles. Ces protocoles définissent comment l'internet fonctionne. Ces protocoles ont des paramètres, donc un veut dire telle chose, deux veut dire telle chose, trois veut dire autre chose. Donc il est très important de définir les paramètres et de publier ceci quelque part de manière à ce que tout le monde y ait accès. Donc la PTI publie ces registres de paramètres et il y en a plus de 3 000

que vous pouvez trouver sur le site de la PTI ; tous les paramètres des protocoles qui sont publiés.

Je vais parler rapidement des DNSSEC. Il s'agit des extensions de sécurité du système de noms de domaine. L'objectif des DNSSEC, c'est d'empêcher tout abus du DNS. Cela est effectué grâce au chiffrement, à la cryptographie. Ceci permet d'assurer aux utilisateurs du DNS que les données qu'ils voient sont valides et authentiques. Les titulaires de nom de domaine qui ont un nom de domaine signent leurs données DNS. Ils disent : « Voici mon nom de domaine et voici les données qui correspondent à ce nom de domaine et que j'ai publiées. » Les opérateurs de DNS valident ces informations au fur et à mesure que les données de DNS passent par le résolveur.

Le DNSSEC utilise des clés. Il s'agit de l'infrastructure de clés publiques, PKI. Il y a pas mal de termes qui se rapportent à ceci mais la KSK, la clé de signature de clé, c'est donc la clé supérieure, la clé chiffrée la plus élevée dans la hiérarchie du DNSSEC. Il y a la clé publique/privée qui est à un niveau inférieur qui est une [inintelligible] qui permet de signer dans l'objectif d'avoir une chaîne de confiance. Donc il y a une succession de clés et de signatures qui peuvent être utilisées par tout le monde pour valider l'authenticité des données signées par les DNSSEC. Et en signant les données, en fait en validant les données, on empêche énormément d'abus du DNS.

Avec tout ceci, vous avez donc à définir le rôle de la PTI dans les DNSSEC. La PTI a reçu de tout l'internet le devoir d'émettre, de gérer, de changer et de distribuer toutes ces clés. Et en plus, c'est la PTI qui signe cryptographiquement tout ceci. La PTI le fait en suivant les meilleures

pratiques de cryptographie qui ont été mises au point par l'IETF, le groupe de travail sur le génie internet.

Troisième volet dans le cadre de notre engagement, il s'agit donc du renforcement des capacités. Le personnel, les membres de la communauté de l'ICANN, tous les jours pratiquement participent à différents efforts qui permettent de communiquer auprès de différentes organisations dans le monde sur les questions relatives au système d'identificateurs uniques et sur la cybersécurité. Nous le faisons en utilisant des webinaires comme celui que nous avons aujourd'hui de manière à mieux faire connaître notre travail.

Lors des réunions de l'ICANN, vous avez également des séances qui sont organisées et qui rentrent dans le détail des différentes technologies pour mieux comprendre de quoi il s'agit, comment cela fonctionne, on parle des [inintelligible]. Parfois, nous avons des ateliers techniques sur plusieurs journées. Nous organisons des formations pour différents organismes d'application de la loi du monde entier pour qu'ils comprennent la méthodologie, pour qu'ils comprennent comment arrêter ce type d'attaques. Et puis il y a évidemment d'autres méthodes que nous utilisons pour communiquer là-dessus. Donc voilà ce qui se passe dans l'écosystème de l'ICANN au jour le jour. Tout ceci, c'est au cas où quelque chose se passe.

Maintenant, quel est le rôle de l'ICANN pendant un incident relatif à la cybersécurité ? Lorsqu'il y a une cyberattaque, ce qu'il faut faire évidemment, c'est de l'interrompre. Donc l'interrompre nécessite de coordonner des interventions de la part de différents acteurs. Ces

acteurs sont les suivants : les opérateurs de réseaux, les réseaux d'entreprise utilisés par les pirates.

Bien sûr, nous avons besoin de l'aide des agences internationales d'application de la loi et puis également nous avons des équipes d'intervention en cas d'incident qui sont organisées au niveau national. Et nous avons également besoin de l'aide des opérateurs de registre de noms de domaine et des registres RIR également. Et nous avons besoin de l'aide de ces registres parce que pour interrompre une attaque, il faut savoir qui est en train d'effectuer cette attaque, quels sont les réseaux, quelles sont les ressources qui sont utilisées. Nous devons savoir qui est titulaire des noms de domaine des adresses IP qui sont utilisées dans le cadre de l'attaque, et puis qui est le titulaire du nom de domaine ou des noms de domaine utilisés dans l'attaque. Et nous avons besoin également des données d'enregistrement. Ce sont donc ces sources de données qui nous donnent l'attribution. Il s'agit des enregistrements des adresses IP et des numéros AS. Nous avons également besoin des données d'enregistrement pour les noms de domaine.

ICANN Org a un rôle de coordination. L'ICANN a une équipe au sein du bureau de la technologie. Donc si vous vous rendez aux réunions de l'ICANN ou si vous faites partie des listes de diffusion, vous verrez que le nom de bureau, le petit nom que nous utilisons, c'est OCTO, *office of the CTO*. Il s'agit de professionnels qui comprennent très bien tout ce qui est relatif à la cybercriminalité. Ils comprennent ce qui se passe du point de vue des attaques et du point de vue des équipes d'intervention.

L'ICANN travaille en étroite collaboration avec les agences d'application de la loi et avec l'OPSET, qui est la communauté de sécurité opérationnelle. Il s'agit des opérateurs de réseau qui sont vraiment sur la ligne de front en matière de cybersécurité. Donc l'ICANN comprend très bien les différents liens qui existent dans la communauté et coordonne le travail des différentes parties pour interrompre ces attaques.

Notre rôle de coordination inclut un processus qui a été mis en place et qui s'appelle le processus de divulgation coordonné. Donc il s'agit des chercheurs de matière de sécurité, des registres, des bureaux d'enregistrement et d'autres personnes dans la communauté qui peuvent utiliser ce processus pour signaler les vulnérabilités et les bugs à l'ICANN. L'idée, c'est de communiquer pour éviter les attaques futures.

Lorsque tout a été fait, on regarde un petit peu ce qui s'est passé exactement. Alors que s'est-il passé ? Qu'est-ce qui n'a pas bien fonctionné ? Pourquoi avons-nous eu un problème de cybersécurité ? On essaie de voir un petit peu les vulnérabilités, les bugs, il y a des recherches qui sont effectuées, il y a des analyses qui sont rédigées. Nous en parlons en face-à-face ou alors lors de réunions virtuelles de manière à vraiment comprendre ce qui s'est passé et identifier les vulnérabilités qui doivent être traitées.

Je voulais mentionner trois conférences importantes dans ce domaine. Il y a déjà le colloque annuel de l'ICANN sur le DNS où les experts du monde entier sur le DNS se retrouvent pour parler un petit peu la cybersécurité et du DNS. Autre conférence, le DNS OARC et il y a le

concept très important des NOGS, des groupes d'opérateurs de réseau. Il s'agit donc de groupes régionaux, nationaux, locaux qui en fait rassemblent les différents opérateurs de réseau pour discuter, pour se sensibiliser les uns les autres et pour permettre aux réseaux de mieux fonctionner.

Une fois qu'on a parlé de ce qui s'était passé lors d'une attaque, lorsqu'on a identifié les bugs et les vulnérabilités, le moment est venu d'ajuster l'écosystème pour durcir l'internet de manière à ce qu'il soit plus résilient en cas d'attaque. Il y a plusieurs choses qui entrent en jeu. On peut peut-être mettre à jour certaines politiques, il faut peut-être s'adresser au SSAC, au RSSAC, au PSWG ou à d'autres groupes de la communauté parce que parfois, lorsque des lacunes sont découvertes, on peut s'en occuper grâce à de nouvelles politiques. On peut peut-être mettre à jour les contrats de manière à ce que les gens se responsabilisent davantage par rapport à la cybersécurité ou alors peut-être qu'il faut rédiger de nouveaux protocoles ou remettre au point certains protocoles existants. Nous allons donc en parler à l'IETF pour voir quels sont les protocoles qui ont été exposés et comment solutionner ce problème.

Et toujours dans tout ceci, la chose la plus importante, c'est le renforcement des capacités, donc parler à la communauté, parler aux opérateurs de réseau, parler à la société civile, parler de ce qui s'est passé de manière à ce que tous comprennent vraiment ce qui se passe et ce qu'il faut faire à partir de maintenant.

Donc, ce qu'il faut retirer par rapport à ce dont on vient de parler, c'est en fait les choses suivantes. Premièrement, le DNS, c'est vraiment

important. Peut-être que cela peut vous faire un petit peu rire parce qu'évidemment, le DNS est une technologie importante mais ce qu'il faut se dire, c'est qu'il ne s'agit pas uniquement d'une fonction technique, ce n'est pas uniquement ce système qui a été mis en place par des ingénieurs que vous ne connaissez pas qui fonctionne et tout va bien. Non, c'est beaucoup plus important que cela parce que le DNS est une infrastructure technique qui est utilisée partout, pour les courriels, pour les navigateurs, pour les applications, pour les systèmes bancaires, etc. Donc le DNS, c'est vraiment le portail à tout système interne ; nous en avons parlé au début du webinaire. Vos courriels, vos bases de données, vos serveurs de fichiers, etc., donc il faut protéger tout ceci. Vous devez le faire. Mais si votre DNS reste ouvert, si votre DNS peut être compromis, tout vos systèmes, tous vos réseaux sont vulnérables. Donc il est absolument critique que les preneurs de décision prêtent attention à leur infrastructure de DNS.

L'ICANN a de nouvelles recommandations par rapport à cela. L'ICANN recommande fortement un ensemble de mesures sur la cybersécurité pour durcir l'infrastructure de DNS local par rapport aux attaques. Il y a différentes étapes, je ne vais pas vous donner tout le détail mais il y a l'autorisation, l'authentification, il y a le chiffrage, le patching, que votre matériel et vos logiciels soient à jour avec le bon patch. Ceci est vraiment critique pour durcir l'infrastructure. Et il y a également d'autres étapes importantes en matière de sécurité des courriels. Mais au-delà de ceci, je crois qu'une des recommandations les plus importantes que fait l'ICANN, c'est de vraiment mise en œuvre les DNSSEC. Les procédures de signature au sein du DNS permettent

réellement d'empêcher les abus et les attaques et protègent l'infrastructure.

Dernière leçon à tirer de tout ceci, c'est le concept général de SSR de l'internet, donc sécurité, stabilité et résilience de l'internet, parce que la cybersécurité, c'est un domaine de focalisation pour la communauté de l'ICANN et pour le personnel de l'ICANN. L'ICANN définit la cybercriminalité comme tout ce qui est distribution de programmes malveillants, tentatives d'hameçonnage, réseaux zombies, piratage, etc. Le temps, les efforts que nous investissons au sein de l'ICANN dans l'écosystème avec la communauté et le personnel, tout ce que nous faisons a pour objet d'améliorer la stabilité, la sécurité, la résilience de l'internet et de son système d'identificateurs uniques.

J'ai suffisamment parlé. Je vais maintenant ouvrir mon chat et je vous invite à poser toutes les questions que vous souhaitez. Allons-y.

JOANNA KULESZA : Je ne sais pas si vous pouvez voir le chat room. On a trois questions à la fin de la discussion.

DAVID HUBERMAN : Merci. Alors voyons, je vais partir du bas pour remonter.

« Est-ce que le DNSSEC qui fonctionne très vite a besoin de beaucoup plus de ressources ? Est-ce que vous recommandez d'utiliser AXFR dans le cas du déploiement du DNSSEC ? »

En fait, il y a des raisons pour permettre l' AXFR mais des raisons qui vous poussent à ne pas le faire aussi. Mais au-delà de ces raisons, il y a

une forte recommandation pour mettre en œuvre le DNSSEC pour permettre aux titulaire de nom de domaine à l'intérieur d'un TLD à signer leur domaine, signer leur données de DNS de telle sorte que tous ceux qui sont en dehors de ce registre puissent le valider. Et là, il s'agit de deux problèmes différents. Donc en fait, c'est une décision qui revient aux opérateurs de registre à titre individuel

Deuxième question : « Pourquoi il y a de plus en plus de menaces à la cybersécurité ? »

C'est une très bonne question. C'est parce que les gens ont différentes motivations. Beaucoup des menaces qu'on voit sont liées à l'argent. Si vous pouvez gagner de l'argent, c'est une bonne source d'argent. Il y a des gens qui sont très futés, créatifs et qui ont trouvé le moyen d'utiliser leur infrastructure cybernétique pour mettre en œuvre des attaques cybernétiques. On ne connaît pas leurs noms très souvent et ce genre d'attaques fait que les gens, comme on ne connaît pas leurs noms, leur identité, pensent qu'ils ne vont pas être punis et donc peuvent continuer à faire ce genre d'attaques. Ensuite, il y a des motivations politiques dans les attaques aux organisations gouvernementales. Et bon, la question politique, c'est toujours une question qui passionne.

Une question de Vanda : « Dans quelle mesure les DNSSEC devrait être mis en œuvre de manière approfondie ? »

Alors le DNSSEC est habilité par un opérateur de registre d'abord, opérateur de registre qui est chargé de l'administration d'un nom de domaine de premier niveau. Une fois que le nom de domaine est signé par les opérateurs de registre, alors cela permet à tout le monde qui a

un nom de domaine dans ce registre, dans ce TLD, de faire sa propre validation de signature. Donc le DNSSEC, c'est fait par les opérateurs de registre. Une fois que c'est fait, tous les titulaires de nom de domaine devraient signer. Et ensuite, tous les autres qui n'ont rien à voir avec ce TLD, tous ceux qui opèrent les résolveurs, les résolveurs récursifs, ont simplement besoin de valider le DNSSEC. À chaque fois qu'il y a une réponse qui passe par le résolveur qui va le passer à l'utilisateur final, alors il va valider, il va vérifier que c'est vrai et que la motivation est bonne.

Question suivante : « Quelle est la responsabilité des titulaires de nom de domaine en termes d'utilisateur qui fait l'objet d'une attaque ou qui est compromis ? Le fournisseur de service punit les utilisateurs pour quelque chose qui échappe à leur contrôle. »

En fait, je ne sais pas si le titulaire de nom de domaine exemple.com, je ne sais pas quelle est leur place dans cette discussion si un utilisateur fait l'objet d'une attaque ou si un nom de domaine est compromis parce que s'il est compromis, cela se passe à un niveau plus élevé que celui du titulaire du nom de domaine. Cela se situe au niveau du bureau d'enregistrement, parfois cela se situe plus haut, parfois cela se situe au niveau de l'opérateur de registre. Il y a également le système de contrat entre opérateur de registre et bureau d'enregistrement qui sont parfois vulnérables. Mais tous ces niveaux sont en amont. Donc il y a énormément de responsabilités dans toute cette question.

Alors, question suivante : « Le DNSSEC peut être responsable de la réflexion distribuée et d'attaques amplifiées. Est-ce qu'il y a de nouvelles idées outre BCP38 pour nous aider à ce niveau-là ? »

Les attaques de réflexion et d'amplification ont eu lieu en raison des vulnérabilités à l'intérieur du système qui n'avait pas été suffisamment renforcé pour faire face à ces attaques. Le DNSSEC, cela consiste à valider les données DNS et s'assurer que ces données soient précises. Donc je ne suis pas sûr que le DNSSEC puisse nous aider là-dessus. Mais mettre un terme aux attaques de réflexion et d'amplification, finalement, c'est un autre type de pratiques.

Est-ce qu'il y a de nouvelles idées outre le BCP38 ? Cela, c'est une excellente question. Alors laissez-moi y réfléchir. Une bonne hygiène, c'est important au-delà de faire un filtre. Il s'agit également de renforcer les systèmes de l'intérieur et éviter toutes les vulnérabilités de réflexion et d'amplification. Mais c'est une bonne question que vous posez là.

Alors question suivante : « Est-ce qu'il y a des modèles de sécurité qui offrent des politiques de sécurité plus efficaces autre que le DNSSEC ? »

Oui. Vous pouvez protéger vos données DNS et vous permettre à vous, utilisateurs, de savoir que la réponse que j'obtiens, c'est celle que j'attendais. Mais il y a d'autres modèles et politiques en termes de sécurité que les opérateurs de registre doivent mettre en œuvre. Il y en a beaucoup en fait. Le filtre, les pare-feux, certaines de ces modèles sont fondamentaux et d'autres sont très simples et d'autres plus compliqués et cela permet aux opérateurs de mieux renforcer leur sécurité et d'être mieux armés face aux attaques.

Une question de David : « En tant que membre de NARALO, je suis intéressé par la perspective des utilisateurs finaux non techniques. Qu'est-ce que les utilisateurs finaux devraient connaître par rapport à la

sécurité ? Est-ce que les utilisateurs finaux laissent le soin aux experts de s'occuper des questions de sécurité ? Est-ce que les utilisateurs finaux peuvent faire quelque chose ? »

Oui, effectivement, c'est une bonne question. Il y a des choses qu'on peut faire pour nous aider à nous protéger pour qu'on ne soit pas victimes et qu'on ne soit pas une partie du problème. L'un des gros problèmes, c'est les réseaux zombies. Les réseaux zombies sont constitués d'ordinateurs compromis, mon ordinateur portable chez moi, mon téléphone portable. Si l'un de ces dispositifs est compromis, alors il peut être utilisé en tant que réseau zombies qui peut être utilisé pour une attaque.

Donc pour moi en tant qu'utilisateur final, il est important que je me sécurise, que je n'installe pas des logiciels que je ne connais pas. Et il est réellement important que je me forme pour ne pas être victime d'hameçonnage parce que c'est une manière que les méchants viennent dans nos ordinateurs, infectent nos ordinateurs de logiciels malveillants ou nous incitent à cliquer sur un lien qui vole des informations sur notre ordinateur, nous orientent vers des sites web faux où on nous demande nos identifiants et nos mots de passe. Donc il s'agit d'être intelligent, il s'agit d'être un internaute intelligent, futé, prudent par rapport à ce sur quoi vous accédez sur vos dispositifs. Voilà pour une première réponse à votre question, David. Mais il y en a d'autres. Et ensuite, il faut exiger une meilleure cybersécurité de la part de nos fournisseurs de service, être conscients des problèmes et en faire rapport, les signaler. Si vous voyez quelque chose, il faut le dire, il faut le signaler.

Une autre question : « Est-ce que la chaîne de délégation peut supporter la surface d'attaque soulevée par la validation de certification TSLA ? »

Oui, effectivement, si vous l'avez bien conçue, oui. Alors, vous êtes opérateur de registre, vous êtes bureau d'enregistrement, revendeur et vous pensez à comment construire un système entre vous et celui qui est à côté de vous. Si vous le créez bien, vous le mettez bien en place, alors vous pouvez ensemble faire face à cette attaque. Mais ce n'est pas facile et je pense que cela est dit implicitement dans votre question, ce n'est pas simple parce que les auteurs d'attaques cybernétiques sont très intelligents, donc il faut être très futés en retour.

Question suivante : « Est-ce que vous pensez que les techniques d'encryptage de messagerie peuvent être réduites par rapport au hameçonnage et au logiciel malveillant ? »

En fait, oui, je pense qu'il faut mieux protéger la confidentialité. Si quelqu'un peut obtenir des copies des messages qu'on s'envoie, si ces messages sont chiffrés, c'est plus difficile. En fait, il s'agit de protéger la confidentialité, la vie privée.

Pour lutter contre le hameçonnage et le logiciel malveillant, rien ne me vient vraiment à l'esprit pour l'instant mais c'est une bonne question.

Alors il nous reste quelques minutes pour ce webinaire de 60 minutes. Si vous avez encore des questions, je serais ravi d'y répondre.

Joanna me demande : « Est-ce que vous seriez disposé à partager avec nous votre opinion par rapport au fait que WHOIS passe au dark ? Est-ce

que cela a un impact sur la capacité d'attribuer d'un point de vue technique les cyberattaques ? »

En fait, WHOIS, qui a été disponible pendant très longtemps, n'est plus totalement disponible. Il n'est plus aussi disponible qu'avant. En fait, il s'agit d'une conclusion qui découle du bon sens qui pourrait compromettre la capacité de ceux qui répondent pour attribuer ce qui se produit.

Toutefois, si vous examinez dans le détail une attaque, vous n'allez pas trouver dans le WHOIS ce que vous recherchez parce qu'il y a beaucoup de données qui ne sont pas cachées, comme par exemple les adresses IP qui sont enregistrées. C'est le cas des fournisseurs de service internet. Et cela, c'est toujours disponible sur WHOIS. Et également, un identifiant très technique et cela n'est pas caché dans WHOIS. Vous pouvez y avoir accès. De très bons ingénieurs peuvent trouver des informations fondamentales. Et en dehors de WHOIS, vous pouvez commencer à poser des questions en disant : « Cette adresse IP a été utilisée à cette heure-ci pour faire telle chose. Est-ce que vous pouvez nous aider à découvrir qui c'est ? » Et si vous êtes une organisation gouvernementale ou si vous êtes une autorité chargée de l'application de la loi, vous pouvez poser ces questions. Donc les informations sur WHOIS ne sont pas aussi disponibles qu'avant mais il faut simplement essayer de chercher ces informations ailleurs.

Dernière question gentiment traduite par Claudia : « Est-ce que l'ICANN pourrait avoir un centre de renseignements pour les techniciens, les ingénieurs, les organisations, etc. ?

Effectivement, le site web de l'ICANN est très complet. Je sais, il est parfois un peu difficile de naviguer sur ce site, de s'y retrouver mais sachez qu'il est plein de ressources, ce site web de l'ICANN, qui va vous mener vers d'autres liens de telle sorte que tout le monde pourra être tenu informé. Et nous en tant que membres de la communauté, moi comme mes collègues, tout le personnel de l'ICANN, on communique sans cesse avec l'ensemble de la communauté, avec NARALO, les utilisateurs finaux, avec les décideurs politiques qui travaillent dans les groupes de travail, dans nos organisations de soutien. On organise des échanges courriels, des téléconférences, des réunions physiques, etc. Les ingénieux aussi travaillent énormément. D'ailleurs, c'est ce qu'on a fait avec mon collègue, on va voir les différents groupes d'ingénieurs et on essaie d'aider à résoudre les problèmes.

Bien, voilà tout ce que j'avais à vous dire pour aujourd'hui. Je cède la parole à Joanna.

JOANNA KULESZA : Merci David. Très intéressante, votre présentation. Je suis sûre que tous les participants en auront bien profité. Merci de cette excellente présentation. Petit rappel. La présentation et le webinaire seront disponibles sur la page wiki d'At-Large.

Pour ceux qui souhaitent obtenir plus d'informations sur la cybersécurité, il y aura une autre édition de ce webinaire demain mercredi 22 mai à midi UTC. Ce sera Patrick Jones qui va faire la présentation. Il me semble que c'est à midi UTC.

Merci beaucoup David, merci à tous ceux qui ont participé aujourd'hui, merci à nos excellents interprètes et à notre personnel extrêmement utile. N'hésitez pas à nous contacter si vous avez des questions sur ce webinaire. Merci à tous, merci à David et bonne soirée à tous.

[FIN DE LA TRANSCRIPTION]