MARRAKECH – Séance de renforcement des capacités d'At-Large : enjeux actuels en matière de cybersécurité
Mercredi 26 juin 2019 – 12h15 à 13h15 WET
ICANN65 | Marrakech, Maroc

JOANNA KULESZA : Bonjour à toutes et à tous. Bon après-midi. Merci de vous joindre à nous. Je m'appelle Joanna Kulesza et je suis à l'ALAC et je suis EURALO, membre individuel, et je suis également coprésidente du groupe de renforcements des capacités de la communauté AT-LARGE. Alfredo Calderón n'a pas pu venir à Marrakech, et donc je souhaite la bienvenue aux membres de AT-LARGE et à toutes les parties prenantes.

Cet atelier fera partie d'une collaboration conjointe avec le GAC pour le renforcement des capacités des membres et j'espère qu'il y a des membres du GAC qui sont présents avec nous dans cette salle. Je souhaite la bienvenue à toutes les parties prenantes qui sont représentées dans cette salle.

Le thème de la présentation aujourd'hui sera le suivant : les problèmes de cybersécurité. Comme je l'ai mentionné auparavant, pendant la séance du GAC, nous tentons de prioriser à la fois le respect de la vie privée et la cybersécurité. C'est dans le cadre de notre EPDP de l'ICANN, et ce que nous essayons de

faire ici, c'est de mieux comprendre les différentes problématiques de la cybersécurité. Et nous avons divers webinaires qui ont été consacrés à cela, la cybersécurité.

Il y aura trois conférences à Montréal qui seront consacrées en partie à la cybersécurité. Nous avons plusieurs webinaires, donc c'est en préparation d'ATLAS III à Montréal. Les webinaires étaient ouverts à toutes et à tous, à toutes les personnes qui voulaient y participer, surtout disponibles en ligne. Si cela vous intéresse, nous serons très heureux de vous montrer comment vous y rendre.

Ce qui a particulièrement retenu l'intérêt, c'était un séminaire que Patrick va vous présenter aujourd'hui et qui est consacré à la cybersécurité. Nous avons beaucoup apprécié le travail de Patrick parce que ça parle de technologie et ça parle également de politiques. Donc nos invités aujourd'hui, c'est Patrick Jones notre invité qui travaille dans le cadre de l'engagement des parties prenantes mondiales à ICANN. Et j'apprécie beaucoup son point de vue parce que moi je ne suis pas une personne qui soit une experte technique. Mais il représente également le travail fait avec les sociétés civiles et le gouvernement. Et dans ce contexte, je suis très heureuse d'écouter votre présentation Patrick. Merci beaucoup de bien vouloir la présenter ici pour nous à la suite de votre webinaire.

Tout est sur le wiki de l'ICANN. nous allons poster les liens hypertextes qui sont disponibles. Nous avons une heure pour cette séance. Patrick va assurer qu'il laissa beaucoup de temps aux débats et aux questions. Gardez à l'esprit qu'il s'agit d'une séance de renforcement des capacités, donc je crois cela peut être utilisé comme plateforme pour nous, pour notre approche sur la cybersécurité.

Donc je vois que tout le monde est maintenant avec son déjeuner et prêt à écouter la présentation de Patrick. Patrick, vous avez la parole.

PATRICK JONES : Merci beaucoup Joanna. Merci beaucoup de m'avoir invité une nouvelle fois à AT-LARGE. Cette mise à jour par rapport au binaire qui a eu lieu, j'ai impression que c'était il y a plusieurs mois, mais c'était le mois dernier. Et vous savez, on utilise de nouvelles informations parce que tout avance très vite. Il y a toujours des attaques nouvelles. Il y a toujours des inquiétudes de cybersécurité.

Et donc nous avons eu un symposium du DNS à Bangkok. Et vous avez vu peut-être des annonces sur Twitter de la part d'ICANN ces dernières semaines qui vous ont parlé de cybersécurité. Donc sans plus attendre, nous allons passer au transparent suivant.

Je m'appelle donc Patrick Jones. Je suis directeur. Depuis 13 ans, je suis à l'ICANN. Je suis des services d'engagement des parties prenantes au niveau mondial. J'ai beaucoup travaillé à la sécurité, l'équipe sécurité de l'ICANN également. Donc je fais beaucoup de formation technique. J'étais en Lettonie, en Lituanie, en Pologne récemment. Je travaille étroitement avec le responsable informatique de l'ICANN. Je vais donc commencer aujourd'hui ma présentation en présentant des exemples. Et la résolution peut-être n'est pas très bonne, mais vous pouvez voir à l'écran que chaque semaine il y a de nouvelles attaques informatiques.

On en entend parler dans les journaux. Ces attaques sont très fréquentes. Et par exemple, il y a eu un botnet qui a eu des programmes, des impacts graves sur l'Internet. Et les caméras Web du monde entier ont été attaquées. Et il y a déni de service qui a été noté au niveau de l'Internet, qui a été créé en 2016, par trois simples étudiants qui ont créé ce botnet pour s'attaquer à des serveurs de Minecraft. Minecraft, c'est un jeu vidéo auquel jouaient ces jeunes. Et ça a eu un effet collatéral sur le système du nuage, du cloud, et ça a impacté des millions de sites Web. Ça a été véritablement grave comme attaque.

Donc une heure de déni de service, ça coute plus de 200 000 USD. Et lorsqu'on y pense à ces chiffres pour les entreprises et pour les utilisateurs finaux, c'est absolument grave.

Donc c'était cette semaine, cette semaine avant Marrakech ; nous avons eu un laboratoire de la NASA qui a été piraté en utilisant un tout petit ordinateur. C'était ce qu'on appelle un *Raspberry Pi*. Et dans tout le réseau de la NASA, il y a ce piratage qui a fonctionné, qui a réussi. Ça arrive constamment, ces attaques, ces piratages. C'est un exemple pour vous.

Ça a un impact fort pour les gouvernements, pour les universités et les chercheurs qui sont constamment attaqués à ce niveau. Donc vous avez eu également en février des attaques importantes dans le monde entier. Ça, ça impactait le DNS et c'est assez majeur comme problème. Des plateformes ont été sévèrement attaquées.

Lors du symposium du DNS en Thaïlande, on en a parlé et ils ont décrit les attaques sur le système. Qu'est-ce qu'ils ont fait pour communiquer au niveau de ces attaques par rapport à leur clientèle ? Et donc vous vous rappelez. Ça, c'était l'ICANN qui avait parlé de menaces significatives sur le DNS.

Le directeur informatique de l'ICANN a parlé de ces menaces au niveau mondial et il a lancé un avertissement à toute la

communauté de l'Internet mondial. Donc j'ai plus d'informations à ce sujet d'ici peu à vous communiquer.

Donc on en a parlé dans les informations internationales, dans toute la presse. Les médias en ont beaucoup parlé : il y a cet hameçonnage, qu'est-ce qu'on peut faire pour se protéger de l'hameçonnage ? C'est l'ICANN qui essaie de communiquer à ce sujet. Vous savez, on fait des annonces ; on envoie des avertissements pour faire prendre conscience à la communauté de ces menaces, de ces risques qui existent.

Donc une des raisons pour laquelle cela se passe, c'est qu'on a beaucoup confiance en l'Internet. On a entre 30 et 50 milliards d'appareils qui sont branchés et connectés sur l'Internet entre plusieurs juridictions. C'est très complexe. Et ce sont des cibles très attirantes.

Une nouvelle fois, vous pouvez voir que les cibles, ce que ces pirates ciblent, ce sont les données, vos données, vos données entre différents appareils que vous utilisez, les logiciels.

Donc la commission sécurité et stabilité, le document SAC105, c'est un document très utile pour apprendre les rapports, pour en savoir plus sur les rapports entre l'Internet des objets et le système de noms de domaine DNS. Il va y avoir une séance de cette réunion qui sera ouverte à la communauté pour parler de ce

document, SAC105, et on aura une mise à jour. Vous savez, SSAC vient souvent à AT-LARGE vous parler. Et ça pourra vous intéresser d'en savoir plus, d'en apprendre plus à ce sujet.

Alors à l'intérieur d'un réseau, qu'est-ce que nous avons. Les éléments communs que nous avons dans un réseau d'entreprise, d'une université, d'un gouvernement, d'une entreprise ? Eh bien ils ont tous des serveurs ; des serveurs pour leur courriel. Ils ont des calendriers. Ils ont des contacts, ils ont une liste de contacts qui sont sur le serveur ; elles ont des bases de données de leurs clients, de leurs employés, de leurs actifs, de leurs biens, les informations fiscales, des choses et des éléments importants, des données importantes pour ces entreprises et entités. Ils ont des serveurs avec des fichiers qui ont des informations financières, des documents, parfois des secrets de fabrication, des processus industriels organisationnels, des procédures, vous voyez. C'est des choses qui peuvent être très recherchées. Donc il y a les noms d'utilisateur, mots de passe des leaderships, des directeurs, des cadres. Vous avez des dépôts de données, diverses pratiques qui existent de gouvernance, la structure qui existe pour protéger leurs documents et leurs données.

Si vous êtes une organisation, vous devez vous reposer sur le DNS pour avoir une présence Web et pour avoir des rapports avec vos clients par exemple. Donc ils sont attaqués constamment. Les

pirates essaient de pénétrer, d'extraire des données et de travailler au niveau des vulnérabilités pour obtenir des informations.

Alors dans le contexte de l'ICANN, je vais vous donner quelques définitions. Définition du phishing ou hameçonnage, nous parlons donc de diverses pratiques d'envoi de courriels qui semblent venir d'une organisation en laquelle on a confiance, et en fait on a des mots de passe qu'on essaie d'attaquer, d'hameçonner, d'obtenir ; et pour cela, on envoie des e-mails et on essaie de se présenter comme étant une personne de bonne réputation. Donc il y a des logiciels malveillants qui sont conçus spécifiquement pour obtenir un accès non autorisé à un système informatique. Donc vous connaissez peut-être les systèmes d'hôpitaux qui peuvent être attaqués dans les grandes villes, à Baltimore. C'est un système de rançon. Ça peut être absolument. On nous demandait des rançons sinon l'hôpital avait son système informatique bloqué à Baltimore aux États-Unis. Et les mots de passe étaient connus. C'était vraiment très très grave.

Nous avons également ce que l'on appelle les botnets. Il peut y avoir les caméras Internet qui sont attaquées. Ces réseaux zombie comme on les appelle, botnet. Il peut y avoir- sans connaissance du propriétaire, ces réseaux sont des zombies qui sont inconnus et ils peuvent être en mesure de mettre des

logiciels malveillants. Donc il y a beaucoup d'abus et d'utilisation malveillante du DNS. Il n'y a pas de définition acceptée au niveau mondial. Il y a des variances, on parle de cybercriminalité, on parle de piratage, ça dépend des secteurs de l'ICANN.

En général, on parle d'utilisation malveillante, de piratage, de menaces au DNS qui rentrent dans trois catégories : la corruption des données, le déni de service et la violation de la vie privée.

Donc c'est une exploitation, si vous voulez, du DNS pour obtenir des données.

Donc quelques nuances. On parle beaucoup au niveau du directeur informatique de l'ICANN d'utilisation malveillante, d'attaque, d'abus du DNS, de l'infrastructure du DNS, mais aussi une mauvaise utilisation du DNS, l'exploitation si vous voulez du protocole DNS, des processus d'enregistrement de noms de domaine. Et ça, on les utilise d'une manière malveillante lorsqu'on enregistre un nom de domaine par exemple.

Donc la semaine dernière, nous avons eu notre spécialiste des noms de domaine à SSAC, Merike Kaeo, qui nous a présenté cela, toutes ces menaces en rapport avec le DNS, les différents types d'attaques que nous voyons au niveau du protocole, au niveau des serveurs et ainsi de suite. Ils sont décrits en détail ici. Vous pouvez trouver sur la session AT-LARGE, quand vous allez sur le

site de l'ICANN, vous pouvez obtenir cette présentation. Ça peut beaucoup vous intéresser, c'est assez complexe, les différents types d'attaques qui existent.

Alors le rôle de l'ICANN dans tout cela, eh bien, il y a de plus en plus- parfois c'est limité, mais nous sommes un point de contact entre différentes entités et communautés parce que ces attaques prennent une ampleur de plus en plus large contre le gouvernement, les multinationales, les forces de l'ordre. Et on en parle beaucoup dans les médias. Vous savez, nous avons eu des débats entre le groupe de travail du GAC et l'ALAC. On parle beaucoup de cela. C'est très très médiatisé.

Donc il y a un rôle pour l'ICANN à jouer là-dedans pour la communauté de l'ICANN et les membres du personnel de l'ICANN lorsqu'il y a des incidents de cybersécurité.

Vous savez, à Kobe, nous avons parlé de ce piratage des enregistrements de domaine , de nom de domaines, qui sont arrivés récemment. Et ça, ça s'est passé en fin d'année dernière. Et je ne vais pas me répéter.

Donc on parle de DNS-espionnage, d'espionnage DNS, et de *Sea Turtle*, et c'est difficile d'attribuer évidemment ces cyberattaques. Parfois, c'est au niveau militaire, au niveau du renseignement que l'on travaille. Il peut y avoir des États entiers

qui utilisent la cybersécurité pour faire des attaques cybernétiques, ça peut être très très grave.

Il y a des prépositionnements, donc il y a tout un travail de renseignement qui est fait pour limiter et voir au niveau militaire qui lance ces attaques cybernétiques. Ça, ça, c'est contre les banques, les réseaux aériens, les compagnies aériennes. Et ça, au départ, c'était 40 organisations dans 13 pays d'Afrique du Nord et du Moyen-Orient. Ça se passait dans ces pays d'Afrique du Nord et du Moyen-Orient. Ces attaques et les cibles, c'était les bureaux d'enregistrement, les registres. Donc Net Node a été attaqué. Vous avez Packet Clearing House qui a été attaqué également. Il y a des ccTLD qui ont été attaqués.

Pour vous donner un exemple de cela, ça s'est passé par exemple au niveau primaire et secondaire. Durant l'attaque l'année dernière, vous avez les cibles et vous avez cibles primaires et cibles secondaires. Il y a eu compromission des enregistrements, modification des noms de serveurs et des zones pour ces noms de serveurs ; il y a eu des modifications des archives pour les adresses e-mail et une redirection des zones.

Donc on pensait avoir affaire à un bon serveur, mais ce n'était pas le serveur auxquelles on pensait avoir affaire. Alors ç'a été présenté lors de la réunion de Kobe, cela en novembre 2018. Cisco a identifié- Cisco Talos et son équipe de sécurité ont identifié les

cibles de cette campagne. C'était le Liban ; c'était les Émirats arabes unis ; c'était d'autres entreprises des Émirats arabes unis.

Il y avait donc FireEye en janvier 2019 qui a lancé des attaques et il y a eu des annonces au niveau des États-Unis qui ont existé. Ça, c'était présenté également au printemps à Kobe de la part de RSSAC.

Donc quel est le rôle de l'ICANN dans tous ces incidents de cybersécurité ? Eh bien nous avons nos textes statutaires. Nous savons que l'ICANN met l'accent fortement sur la cybersécurité puisque la mission de l'ICANN s'est d'assurer un Internet stable et sûr, un système d'identifiants uniques de l'Internet.

Nous avons donc notre mission, la stabilité de l'Internet, la sécurité, l'interopérabilité mondiale, la résilience et l'ouverture du DNS et de l'Internet. Donc il y a des communautés qui sont impactées négativement, et ça, ce n'est pas acceptable pour l'ICANN qui veut renforcer la sécurité du DNS, du système de noms de domaine, et du système de serveurs de la zone racine du DNS. Ça, c'est notre premier objectif, absolument.

Nous devons renforcer cette sécurité et nous devons faire évoluer le système d'identifiants uniques, en coordination et en collaboration avec les parties pertinentes. On continue à servir les besoins des communautés.

On développe des politiques également. Il y a des groupes qui travaillent donc à la sécurité, à la stabilité et la résilience. Il y a ce groupe du GAC qui travaille sur les procédures et les politiques en rapport avec les sécurités, en rapport avec l'utilisation malveillante qui peut exister du DNS. Nous avons le comité consultatif SSAC sur la sécurité et la stabilité qui fait beaucoup d'analyse des risques, qui présente des documents et qui travaille avec le Conseil d'administration, mais aussi avec la communauté au sens large. Il y a également le RSSAC qui s'occupe de la zone racine, le système de zone racine. Et les comités consultatifs, vous connaissez leur travail et leur document. Vous savez que nous avons de nombreux commentaires publics à ce sujet. Nous avons une évolution du système de zone racine. C'est très important pour AT-LARGE. Ce sont des documents essentiels.

Nous avons donc divers contrats qui existent, qui sont signés par l'ICANN. Il y a des rapports qui s'instaurent, des rapports contractuels qui existent. Nous avons donc des accords entre l'ICANN et les opérateurs des registres de premier niveau. Il y a des rapports avec les bureaux d'enregistrement qui existent également, ces noms de domaines qui sont gérés par les bureaux d'enregistrement. Nous avons le RAA, ce contrat qui existe avec nos bureaux d'enregistrement. Et nous avons des revendeurs. Il y a des rapports avec les revendeurs, entre les bureaux

d'enregistrement et les revendeurs. Les revendeurs et les bureaux d'enregistrement peuvent également avoir et ont en général des accords entre eux, des accords entre le bureau d'enregistrement et les titulaires de nom de domaine. On n'a pas un rapport avec le titulaire direct ; l'ICANN ne l'a pas. Ça passe par ces bureaux d'enregistrement. Mais voilà sur l'écran comment ces liens entre ces diverses entités existent.

Et il y a des outils importants qui existent en rapport avec la sécurité et la stabilité. Le contrat d'accréditation de bureau d'enregistrement impose des obligations pour éviter l'utilisation malveillante. Ces contrats contiennent également des dispositions similaires dans le cas des contrats d'accréditation des opérateurs de registre pour protéger les titulaires de nom de domaine du malwares, des réseaux zombies qui veulent faire de l'hameçonnage, pour manquer au droit de la propriété intellectuelle, pour les pratiques frauduleux remonte ou d'autres types de pratiques qui manquent à la loi.

Diapo suivante. À l'ICANN, nous avons également la PTI, l'organisation des identificateurs techniques publics, qui est une subsidiaire qui responsable de l'aspect opérationnel de la coordination et de l'attribution des ressources de numéros aux Registres Internet régionaux.

Nous avons également la responsabilité d'entretenir la zone racine du DNS. Nous sommes le gestionnaire de la zone .ARPA et nous entretenons l'ancre de confiance des extensions de sécurité du DNS [inaudible] DNSSEC.

Diapo suivante. On a ici quelques informations sur le DNSSEC. Je ne vais pas y consacrer beaucoup de temps et j'espère que vous comprendrez que lorsque le DNS a été développé par des ingénieurs, dans la moitié des années 80, la sécurité ne faisait pas partie des protocoles. Donc le DNSSEC a par la suite été développé, surtout à la suite de certaines recherches qui voyaient que les utilisateurs des noms de domaine et les titulaires pouvaient ne pas arriver là où ils voulaient aller. Donc le DNSSEC est censé les assurer des informations qu'ils voient lorsqu'ils se rendent sur une page Web à partir de la page à laquelle il voulait arriver. Ce qui permet que les titulaires de nom de domaine puissent signer leurs données, mais de même ça permet aux opérateurs de registre de bien garantir que les informations qu'ils sont en train de transmettre appartiennent à l'organisation.

Vous verrez qu'il y a un petit gamin ou une coche verte sur le navigateur lorsque vous accédez à un de ses sites Web qui est signé comme étant le site Web où vous voulez aller.

Diapo suivante. Alors, lorsqu'il y a une occurrence d'un cas de manquement à la cyber sécurité ou une cyberattaque, il est

important de savoir que l'ICANN à une équipe qui est le principal point de contact des différentes organisations qui coordonne les réponses, donc l'ICANN coordonne la réponse avec ces autres organisations. Il s'agit d'un groupe de l'ICANN qui travaille avec les différentes entités et différents acteurs et avec différentes communautés à qui on fait confiance et qui utilisent leur expertise pour aider à mettre en rapport les différents groupes.

En cas de cyberattaques, il faut coordonner pour résoudre ce problème. Nous sommes membres du forum des équipes de réponse en cas d'attaque, ce qui comprend des professionnels de la sécurité ou [IRST] qui travaillent ensemble pour partager des informations. Il y a également une liste de l'ICANN qui a été élaborée par les opérateurs de code de pays qui peuvent échanger et se mettre au courant lorsqu'il y a des attaques en cours.

Le personnel et la communauté et l'organisation ICANN participent ensemble aux initiatives d'éducation d'autres organisations sur les questions qui ont un impact sur le DNS et sur le système d'identificateurs uniques, ce nous faisons à travers les séminaires Web. Nous avons également des séances de travail lors des réunions de l'ICANN, à travers des ateliers techniques comme le symposium du DNS, et également avec des formations sur l'application de la loi et les forces de l'ordre.

Cette année d'ailleurs, nous avons organisé un tel séminaire dans cette région. Et le but est toujours de partager des informations, échanger des meilleures pratiques, les aider à savoir comment résoudre ces problèmes et leur donner les informations nécessaires en général. Dans cet exemple en particulier, il y a des membres de notre équipe qui ont travaillé en collaboration avec l'autorité des télécommunications du Pakistan pour avoir un atelier de plusieurs journées sur le renforcement des capacités pour améliorer leur compétence et pour faire la sensibilisation sur certains aspects avec les secteurs techniques et avec d'autres parties prenantes.

En général, il s'agit de séances qui sont ouvertes, où les différentes entités commerciales peuvent participer. Ces dernières semaines, d'ailleurs, nous avons beaucoup échangé avec des membres de la communauté technique, avec des équipes de réponse aux urgences techniques. Il y avait des gestionnaires de CCT entre autres. Et tout cela, c'est fait également à distance à travers des webinaires [inaudible].

Voici certaines informations que j'ai partagées lors de la journée technique, *Tech Day*. Nous avons souvent des formations sur le rôle du DNSSEC dans la région pour faire la sensibilisation sur des problèmes liés à la sécurité du DNS, mais également expliquer

simplement de manière à ce que ça puisse être compris toutes par les parties prenantes.

Parfois, on a des formations un peu plus pratiques. On a un programme de formation de formateurs également où les personnes qui sont dans une région peuvent par la suite faire leurs propres séances de formation, sachant que l'ICANN ne peut pas se rendre partout. Donc c'est très utile pour pouvoir former les partenaires de la communauté pour qu'ils puissent eux-mêmes former les autres. Et cela, nous le faisons pour aider à faire passer un message pour renforcer la chaine de confiance du système des noms de domaine et donc nous encourageons tous les gestionnaires de TLD à mettre en œuvre le DNSSEC. Les FSI à avoir la validation des sites Web. Et en général, à ce qu'il y ait une conscience sur les bonnes pratiques.

Il y a deux jours, nous avons constaté qu'il y avait 3898 DNS qui étaient signés par le DNSSEC sur un total de 1730 TLD qu'il y a dans la racine. C'est-à-dire bien que 50 % des TLD de codes de pays sont signés également. Et il y a beaucoup de demandes autour du monde pour avoir cette expertise relative au déploiement du DNSSEC. Il est difficile de pouvoir voir directement le rapport entre la formation et la décision d'un opérateur ou d'un gestionnaire d'un TLD de faire signer ces noms de domaine, mais récemment on a vu qu'il y avait certains TLD

qui commencent à avoir le DNSSEC, et ce au cours des trois derniers mois. Et les chiffres que nous avons constatés ont montré qu'à travers la formation, les personnes sont plus conscientes et finissent par mettre en œuvre le DNSSEC. Je pense que l'exemple du Koweït en est un très bon cas, parce que le gestionnaire du ccTLD du Koweït était présent à un atelier qu'on a organisé en Turquie l'année dernière et en rentrant ils se sont occupés de mettre en œuvre le DNSSEC dans leur propre ccTLD.

D'ailleurs, le ccTLD du Koweït a fait partie de la délégation de formation au Pakistan ; ils nous ont aidés à faire la formation des autres. Ce qui montre que lorsqu'on forme les autres, les personnes finissent par bien comprendre de quoi il s'agit et mettre en œuvre le DNSSEC.

Au cours de l'exercice fiscal 2018, nous avons voyagé un peu partout. Pour que vous sachiez donc, nous organisons différentes formations. Des formations des communautés locales qui passent des aspects de base du DNS à la compréhension de l'écosystème du DNS. On aborde également l'utilisation malveillante du DNS, les noms de domaine génériques des noms de domaine internationalisés, l'acceptation universelle ; on essaie de travailler sur des sujets d'actualité également, comme par exemple les questions de domaine en Émoji. Et nous leur donnons des directives sur les attaques récentes.

Donc on a ici également des formations que nous avons organisées pour le groupe des opérateurs de réseaux, les réunions des RIR, et avec les organisations de TLD régionales.

Il est toujours difficile de démontrer l'impact de ces formations pratiques, mais je pense qu'au long terme on a ici un bon exemple qu'à travers cette sensibilisation directe on voit toujours des bénéfices. Il y a 10 ans, on a beaucoup collaboré pour faire la sensibilisation sur les réseaux zombie et d'autres comme Avalanche et des réseaux zombie qui généraient leurs propres codes. Et nous avons mis en œuvre des sécurités. On a dès lors créé un système de demandes pour faire passer cela, et donc on a maintenant des moyens pour gérer ces conduites malveillantes.

L'ICANN a son propre processus que vous aurez tous vu lorsqu'un membre de la communauté a identité une vulnérabilité avec Adobe Connect. Au cours d'une réunion de l'ICANN, vous vous souviendrez, les systèmes d'Adobe Connect de l'ICANN ont cessé de fonctionner, ce qui est un exemple du fait que lorsque quelqu'un identifie une vulnérabilité ou un problème, il peut nous l'informer. Et à ce moment-là, les différentes parties de l'organisation et l'équipe de sécurité de l'ICANN vont travailler avec cette organisation pour faire une divulgation gérée de ces problèmes. Et nous comptons avoir plus de coordination et plus

de collaboration avec les forces de l'ordre, les forces de la sécurité publique entre autres.

Diapo suivante. Une fois qu'il y a déjà eu un incident de cybersécurité, les représentants de l'ICANN et les membres de la communauté présentent souvent à des moments différents. Donc par exemple, on a organisé un symposium en Thaïlande, mais également un autre groupe auquel l'ICANN participe qui s'appelle le Centre des opérations de l'analyse et de la recherche liés au DNS qui participe aux réunions des opérateurs de réseaux et à d'autres réunions aussi. Mais l'idée étant toujours que d'autres organisations puissent utiliser ces informations pour donner des mises à jour de politique pour les contrats et pour redévelopper des protocoles souvent.

On est à la fin de la présentation. Je voudrais qu'on ait un moment pour les questions. J'espère être à l'heure. Alors, le message principal ici est qu'il faut que vous gardiez à l'esprit que le DNS n'est plus simplement une fonction technique, mais qu'il est devenu une partie clés de notre structure des organisations. Et faites attention à votre structure DNS, à l'information et aux données de tous vos systèmes qui pourraient être à risque si vous n'avez pas fait.

Voilà, le moment des questions est donc venu. Merci.

JOANNA KULESZA : Merci. C'était fort utile. Vous avez fait un très bon travail de combiner les défis pour la communauté et les défis techniques.

J'utiliserai cette présentation en termes de renforcement des capacités pour faire un appel à des rapporteurs ou des personnes qui veulent proposer des rapporteurs pour le système de serveurs racine, appel qui est toujours ouvert. On a beaucoup décidé d'élaboration de politiques hier, et vous avez maintenant la possibilité de vous joindre à ces travaux. Donc si la cybersécurité vous passionne, vous intéresse, vous pouvez les rejoindre.

Je félicite l'équipe de sociétés qui fait un très bon travail au partage de ces informations. Patrick fait un travail formidable de coordination avec l'équipe européenne. Si vous avez besoin de ce type d'information, je suis sure que l'équipe vous donnera autant d'informations que nécessaire, ou que possible. Je sais que le Conseil d'administration est également impliqué au travail de cybersécurité. On a ici Leon Sanchez. On va lui demander s'il a quelque chose à ajouter par rapport au travail que fait le Conseil d'administration à ce sujet. Puis on passera aux questions.

Leon.

LEON FELIPE SANCHEZ AMBIA : Merci Joanna. J'irai vite pour pouvoir avoir du temps pour les questions qu'il pourrait y avoir dans la salle. Vous avez tout à fait raison. Il s'agit d'une des principales priorités pour le Conseil d'administration. Sachant que la mission de l'ICANN est bien sûr de garantir la stabilité et la sécurité du fonctionnement de l'Internet. Cela fait partie de notre plan stratégique quinquennal, et il s'agit d'un des cinq objectifs stratégiques. Et nous avons défini des objectifs stratégiques et des buts, des cibles qui feront partie du plan opérationnel qui sera adopté par le personnel pour pouvoir mettre en œuvre notre plan.

Donc oui. Ce principe de garantie du fonctionnement stable et en sécurité est l'un des principaux objectifs du Conseil d'administration.

JOANNA KULESZA : Merci Leon. J'imagine qu'il sera également utile d'avoir des gens qui connaissent et qui comprennent mieux cette partie de la mission pour vous. Merci.

J'ai des intervenants qui ont levé la parole. Je me demande s'il y a des interventions. Ah oui. Excusez-moi. Est-ce qu'il me manque quelqu'un d'autre ? Eduardo, très bien. Et Holly et Hadia et Javier.

Super. Il y a-t-il quelqu'un d'autre qui n'est pas autour de la table qui ne soit pas membre de l'équipe de directions d'AT-LARGE qui puisse avoir des questions ?

Je vous laisse réfléchir. J'ai Hadia, Holly, Judith, Eduardo et Javier.

Je vais demander à ce que l'on ait un compte à rebours à l'écran. On commence par Hadia et puis on avance et on passe toute la liste.

HADIA EL MINIAWI : Merci. Je voudrais d'abord vous féliciter de tout le travail que vous avez fait, de l'organisation de toutes les séances de renforcement des capacités et tous les ateliers que vous donnez.

Compte tenu du fait qu'on a des accords internationaux comme la convention de Budapest sur la cybercriminalité, l'ICANN a-t-elle des obligations qui l'obligent à travailler avec ceux qui luttent contre le cyber délit, pas avant l'occurrence d'un incident, mais pour collaborer ou travailler avec ceux qui luttent de manière proactive contre le cyber délit ?

PATRICK JONES : Vous savez, l'ICANN n'est pas un acteur. Si on travaille beaucoup avec les différentes institutions, les différents gouvernements

lorsque ces types d'attaques nous sont signalés. Ça fait partie de nos statuts constitutifs, comme je disais, mais nos parties contractantes sont aussi assujetties à différentes juridictions donc lorsqu'il y a des évènements et que cela nous est demandé, nous collaborons.

Nous ne sommes pas [signataire de séances de législation], mais j'espère avoir apporté une clarté, avoir répondu.

HADIA EL MINIAWI : Oui, ma question était liée à la collaboration au niveau des données et aux informations.

JOANNA KULESZA : Hadia on prend note. Holly, vous avez une autre question ?

HOLLY RAICHE : Ce sont deux questions que j'ai à poser, surtout parce qu'il y a beaucoup de débats et surtout par ce qu'on a tellement de données ; comment définit-on qui a accès à ces données. D'après ce que vous dîtes, ce n'est pas tout simplement les forces de l'ordre. Je voudrais savoir. Et vous parlez sur qui peut le faire.

Mon autre question porte sur le fait que la présentation DoT/DoH hier présente deux menaces : il y a des paquets qui passent par-

dessous les systèmes de sécurité soi-disant, qui ont été créés par des grandes sociétés. Donc il semblerait qu'il y a beaucoup de sécurité qui n'est plus garantie parce que les paquets passent par-dessous les protections qui existent, qui dépassent ces mesures de sécurité.

À Kobe, monsieur, vous avez également fait une présentation. Et si je ne me trompe, on a vu que le problème était que ce soit à travers le DoT soit à travers le DoH, vous verrez qu'il y a des résolveurs qui prendraient le dessus par rapport aux autres.

Si on commence à avoir moins de résolveurs, on commence donc à créer des grandes cibles. Vous avez une réponse ?

PATRICK JONES : Si cela n'a pas déjà été dit, le SSAC vous dira qu'ils ont une équipe de travail qui s'occupe du DoH, du DoT et d'autres questions associées. Ils n'en sont qu'au début, mais il y aura un essai pour essayer de donner à la communauté une idée de ce que sont ces technologies et puis ça sera à chaque communauté de prendre les mesures nécessaires pour les prochaines étapes.

Dans notre communauté, il y aura des informations qui essaieront d'aider à orienter les différents groupes là-dessus.

JOANNA KULESZA : J'ai Judith, Eduardo et Javier. J'espère que c'est le bon ordre. On commence par la dame.

JUDITH HELLERSTEIN : Merci. Merci de cette présentation ; j'ai deux questions. D'une part , on voudrait que le DNSSEC soit mis en œuvre par énormément de groupes différents. Peut-être que l'ICANN pourrait collaborer avec les autres organisations Internet, I-stars comme on les appelle, pour créer des campagnes de sensibilisation pour que le DNSSEC soit mis en œuvre comme ce qu'on a eu pour [l'ALAC DNSSEC]. Mais il y a toutefois des parties du DNSSEC qui sont très sécurisées, mais il y a des organisations, des petits groupes, qui ne sont pas en train de déployer le DNSSEC. Donc qu'en pensez-vous ?

D'autre part, une campagne de sensibilisation pour voir comment protéger le système et pour peut-être travailler avec les responsables informatiques et d'autres pour mettre en place une politique pour ne pas envoyer des liens sur les mails.

PATRICK JONES : Comme Leon vous le disait, et comme je l'ai dit moi-même dans la présentation, la sécurité est une partie essentielle du nouveau plan stratégique. Il y a du travail au niveau de l'encouragement et la sensibilisation par rapport au DNSSEC. Donc, faites attention à

notre travail. Suivez-nous. Vous allez voir qu'il y a du travail dans ce domaine.

JUDITH HELLERSTEIN : Oui, et Leon qu'en pensez-vous, peut-être que vous avez d'autres informations sur le fait de savoir qu'il y a eu d'autres groupes, d'autres organisations I-Stars qui ont travaillé sur la mise en œuvre du DNSSEC avec une version moins couteuse.

LÉONFELIPESANCHEZ AMBIA: Mais vous parlez de quoi ? Du déploiement du DNSSEC ?

Ça fait partie du plan stratégique. En ce concernant la sécurité, je ne suis pas le membre du Conseil qui a le plus de connaissance technique pour en parler, mais je suis sûr que mes collègues du comité technique du Conseil d'administration en ont discuté et qu'ils échangeront et coordonnent vont bien sûr avec le personnel pour essayer de trouver la meilleure manière possible d'avoir un déploiement plus large du DNSSEC de la manière la plus efficace au niveau des couts.

PATRICK JONES : t une réponse rapide aussi. C'est pour savoir qu'il y a une réponse qui n'est pas liée à l'ICANN qui s'appelle CRYPTTECH. Il s'agit d'une initiative pour développer un module de sécurité moins

couteux que les différentes organisations pourront utiliser pour mettre en place le DNSSEC. C'est vrai que ça pourrait être assez couteux aujourd'hui d'acheter les modules qui existent. Et cette initiative vise à avoir un processus qui soit plus efficace au niveau des couts. Merci.

EDUARDO DIAZ : Merci. J'ai une question. C'est une question de curiosité.

Outre l'incident Adobe, est-ce que l'ICANN a déjà fait l'objet d'une attaque de cybersécurité ?

PATRICK JONES : Je ne parlerai pas au nom de l'équipe de sécurités du DNS, mais il y a eu des annonces de différents problèmes qui ont eu lieu par le passé. Je vous conseille de leur demander si ça vous intéresse.

JOANNA KULESZA : Merci Eduardo et Judith. Ce sont des discussions qu'on pourra avoir entre nous. Javier.

JAVIER RUA-JOVET : Oui merci beaucoup ; présentation très intéressante. Est-ce que vous pourriez nous en dire un petit peu plus sur ce que font les gouvernements souverains et ce qu'ils demandent à l'ICANN. Est-

ce qu'ils collaborent avec l'ICANN ? Est-ce qu'il envoie des lettres à Goran ? Comment ça se passe ? Est-ce qu'il y a des étapes à ce niveau ? Est-ce qu'ils demandent un soutien ?

PATRICK JONES : Oui. J'ai mentionné que l'ICANN est membre du forum pour la sécurité de l'Internet et la réponse, ça concerne la sécurité. Donc ça s'appelle FIRST, comme acronyme. On nous envoie des demandes. En effet, le personnel technique de l'ICANN est en rapport avec des groupes de la communauté à qui on fait confiance, des groupes de confiance. Et on partage avec eux des informations, on travaille avec certains groupes de maintien de l'ordre et vous avez peut-être reçu une lettre qui a été publiée sur différents canaux de communication. Tout tourne en fait autour des services techniques du responsable technique de l'ICANN.

JOANNA KULESZA : D'autres questions ? Moi j'ai une question générale.

Il ne nous reste que quelques minutes. Vous avez mentionné que le DNS n'est plus seulement un problème technique. Ça va plus loin. La sécurité, les problèmes techniques deviennent des problèmes plus larges, des problèmes de, des problèmes sociétaux. Il y a des personnes dans la salle qui sont très intéressées par le contenu par exemple, la cybersécurité dont on

parle, ça semble dépasser un petit peu les questions techniques. Donc ma question précisément est où est-ce que l'on met la frontière ? Comment on délimite les aspects techniques de sécurité et les aspects plus larges de sécurité Internet ? Donc celle-là où il faut bien comprendre les rapports contractuels qu'a l'ICANN.

Donc ça dépend du rôle que l'on donne à l'ICANN, et tout cela a un impact pour les bureaux d'enregistrement et les titulaires de nom de domaine donc doivent identifier où on en est à ce niveau. Ça, on en débat au niveau de la GNSO, au niveau du GAC, au niveau de ce groupe.

Je crois qu'il devrait y avoir des dialogues là-dessus. En effet. Et ce qu'il faut bien comprendre, c'est que ces attaques existent de plus en plus fréquemment et qu'on se repose sur nos téléphones pour contacter notre système. Donc il faut faire les mises à jour des logiciels. Il faut protéger le mot de passe. Il faut bien connaitre les dernières tendances, se protéger au niveau numérique et ensuite parler de ces problèmes.

JOANNA KULESZA : Donc ce sont des lignes de conduite qui sont tout à fait pratiques. Donc je ne vais pas trop rentrer dans le débat ; je vais m'arrêter

là, à moins qu'il nous reste quelques minutes si vous voulez dire quelques mots.

HADIA EL MINIAWI : Non je n'ai rien à rajouter. Merci.

JOANNA KULESZA : Donc je vais m'arrêter là. Ah ! Pardon. Je ne vous avais pas vu. Pardon. Je ne vous avais pas vu Evin.

EVIN ERDOGDU : Oui merci beaucoup. Je parle au nom de Remmy Nweke qui a une question.

Bonjour. J'aimerais savoir si l'ICANN à un soutien, un plan de soutien pour les ALS qui promeuvent le DNS pour les femmes en Afrique.

PATRICK JONES : Donc l'équipe d'engagements en Afrique a travaillé avec la communauté pour avoir une stratégie d'engagement régional. Et je crois que la sécurité , ça fait partie de cela. Donc, partager des informations sur le DNS, c'est dans leur cadre de référence. Donc, nous avons Pierre Dandjinou. Nous avons Yaovi Atohoun et Bob [Otchien]. Ils sont basés à Nairobi, au Kenya. Et c'est vraiment le

bureau qui va vous donner des informations pour les communautés locales et pour la sécurité.

JOANNA KULESZA : Moi je crois que ces équipes GSE sont toujours très agréables. Partagez avec eux ; communiquez avec eux et facilitez le débat que nous avons.

Je vois une question dans la salle. Nous allons vous apporter un micro ou s'il n'y a pas de micro, je vais vous demander de vous rapprocher de la table et de parler dans un micro. Merci monsieur.

CRAIG JONES : Oui bonjour je m'appelle Craig Jones d'Interpol. Je suis détecteur de la cybersécurité et je m'intéresse beaucoup à l'approche de prévention parce que ça coute très cher de réagir. Je crois qu'il faut faire beaucoup plus de prévention. C'est ce que nous essayons de faire au niveau d'Interpol. Merci.

PATRICK JONES : Oui tout à fait. Merci. Je suis sûr que vous êtes en communication avec John Crain et les autres personnes. M. Champika à APAC a

présenté à Interpol, en Corée. Il y avait Interpol café, une conférence à laquelle ICANN a participé. Donc voilà.

JOANNA KULESZA : Donc je vois des questions, quelques questions supplémentaires. Oui, utilisez le micro, monsieur, puisque nous l'avons trouvé.

MATOGORO JABERA : Oui bonjour. Merci. Je m'appelle Matogoro Jabera et j'apprécie beaucoup cette présentation excellente. Je voulais mentionner que je représente également ALAC au niveau de l'équipe sécurité et résilience, et que nous faisons une révision sur les identifiants uniques et sur le travail de notre groupe. Et je crois qu'on peut beaucoup travailler ensemble.

JOANNA KULESZA : Oui, merci beaucoup. Nous avons d'autres questions. Donc pas d'autres questions. Je veux remercier Patrick pour son excellente présentation, pour toutes les informations qu'il a apportées. Et j'aimerais remercier Leon également qui s'est joint à nous. J'aimerais remercier toutes les personnes ici présentes. Si vous avez des questions et que vous êtes timide, eh bien, dites-nous par e-mail. Contactez-moi. Venez me parler. N'hésitez pas. Nous allons avoir besoin de rédacteur sur ces thèmes de cybersécurité,

et vous pouvez vous lancer dans le développement de politique et la rédaction de politiques ICANN de cette manière. Donc, n'hésitez pas à nous contacter. Nous remercions également nos interprètes. Merci beaucoup. Bon après-midi.

[FIN DE LA TRANSCRIPTION]