CLAUDIA RUIZ : Bonjour ou bonsoir. Bienvenue à cette réunion mensuelle de LACRALO. Nous sommes le 18 avril 2022 à 23 h UTC.

Nous avons sur le canal espagnol Augusto Ho, Alfredo Lopez, Carlos Aguirre, Gerardo Martinez, Harold Arcos, Laura Margolis, Rodrigo Saucedo, Sergio Salinas Porto et Vrickson Acosta. Nous avons Claire Craig sur le canal anglais et Sindy Obed sur le canal francophone. Nous avons reçu des excuses de Sylvia Herlein Leite.

Nous avons avec nous du personnel Claudia Ruiz et Silvia Vivanco. Claudia Ruiz gère l'appel. Nous avons Marina et Paula comme interprètes espagnoles, Esperanza et Bettina pour le portugais et Jacques et Claire pour le canal francophone. Nous avons également Alberto Soto qui vient de se joindre à l'appel.

J'aimerais vous rappeler de bien vouloir indiquer votre nom avant de prendre la parole pour l'interprétation et de parler lentement et clairement également.

AUGUSTO HO : Bonjour ou bonsoir à vous tous. J'aimerais tout d'abord vous remercier de vous joindre à nous à cette réunion mensuelle de LACRALO. Je vous souhaite tout le succès possible aujourd'hui. Bienvenue donc et je vais donner la parole à Claire pour l'approbation de l'ordre du jour. Allez-y Claire.

CLAIRE CRAIG : Oui, merci beaucoup Augusto. Bienvenue à toutes et à tous. Bienvenue à notre réunion mensuelle LACRALO.

Aujourd'hui, à l'ordre du jour, nous allons avoir le plaisir de d'accueillir Nicolas Antoniello qui va nous parler du DNS, comment on peut le rendre plus résilient et sécurisé. Il y aura un webinaire en deux parties. Nous aurons la possibilité de poser des questions à Nicolas Antoniello de l'ICANN. Nous aurons ensuite un rapport sur le Conseil d'Administration de l'ICANN de la part de León Sanchez. Nous aurons également des rapports de nos représentants de l'ALAC de la part de Carlos Aguirre et également, nous avons le projet LAC numérique avec Sergio Salinas Porto qui va nous parler des progrès de la planification de cette initiative LAC numérique. Nous allons avoir nos mises à jour régionales avec un rapport des représentants régionaux. Nous allons également parler des élections en 2022.

J'aimerais savoir s'il y a d'autres points que vous voudriez rajouter à l'ordre du jour. Donc levez la main si vous voulez rajouter quelque chose à l'ordre du jour. Bien, je ne vois pas de demande de prise de parole, donc cet ordre du jour nous convient, nous tombons d'accord sur cet ordre du jour pour cette réunion. Très bien.

Je redonne donc la parole à Augusto. Merci

AUGUSTO HO : Merci Claire.

Comme cela a été mentionné par Claire, dans notre ordre du jour, nous allons avoir un webinaire de la part de Nicolas Antoniello qui, en 45 minutes, va nous parler du DNS et de la manière dont on peut le rendre

plus résilient et sécurisé. J'aimerais souhaiter la bienvenue à Nicolas Antoniello. Vous avez la parole, Nicolas.

NICOLAS ANTONIELLO : Merci à Augusto.

Tout d'abord, j'aimerais vous remercier de m'avoir invité pour présenter aujourd'hui et pour vous parler de ce thème. Pour ceux qui ne connaissent pas, je m'appelle Nicolas Antoniello, je travaille à l'ICANN en tant que responsable régional pour l'Amérique latine en ce qui concerne la participation technique et l'engagement.

Nous aimerions avoir aujourd'hui des discussions sur le DNS, le système de noms de domaine, et les questions qui se posent sur différents protocoles et comment peut-on renforcer ce DNS pour qu'il soit plus résilient.

Comme nous allons le voir dans certains cas, il y a eu des problèmes de confidentialité sur certaines fonctionnalités du DNS. La confidentialité des données notamment peut parfois poser des problèmes. Je vais partager mon écran. Je ne sais pas si je peux partager mon écran, Claudia, ou si vous voulez gérer peut-être cela. Voilà, très bien. Vous voyez bien mon écran, je l'espère, que je contrôle maintenant.

Nous allons parler du renforcement du DNS pour qu'il soit plus sûr et plus résilient. N'hésitez pas à me poser des questions, vous pouvez m'interrompre avec des questions le cas échéant et je crois que ce sera plus intéressant si nous posons des questions au cours de ma présentation. Claudia, n'hésitez pas à m'interrompre, je ne regarderai pas le chat pendant que je présente, mais dites-moi s'il y a une question

ou une intervention, un commentaire. Ne soyez pas timide, posez des questions. Merci.

Alors, nous allons commencer avec l'internet aujourd'hui. Il semble qu'il manque quelque chose. Il n'y a pas de données, mais il y a un cadre. Il y a un navigateur sans données. Ce que je veux illustrer ici, c'est que lorsque nous voulons accéder à un site web sur l'internet, avant que le navigateur puisse télécharger tous les éléments pour que vous puissiez avoir accès à un site, vous devez vous connecter à des serveurs et vous devez télécharger les différents éléments pour avoir accès à ce site web. Il y a un ensemble de serveurs. Vous obtenez des informations de dix ou vingt différents services et serveurs. Donc vous devez faire des requêtes nombreuses à ces serveurs. Il y a une authentification qui est nécessaire, il faut authentifier ces requêtes avant de pouvoir avoir accès à un site web par exemple et vous devez utiliser le système de noms de domaine, le DNS.

En général, vous avez un nom de domaine avec un URL et vous avez des adresses protocole internet IP, mais le DNS joue un rôle essentiel. Et au niveau des utilisateurs, il y a pour le moment une requête sans données, l'utilisateur ne voit pas ce qui se passe. Du côté de l'utilisateur, c'est tout à fait neutre et transparent, il ne sait pas vers quels serveurs ces requêtes vont partir et être gérées.

Les requêtes sont envoyées au DNS et la recherche se fait à ce niveau avec les adresses IP. Et le navigateur qui est utilisé va me permettre d'avoir accès au site web par exemple et je pourrai avoir accès de cette manière au site web et à tout le contenu qu'il y a dans ce site web. Donc

c'est très caché, ce n'est pas visible pour l'utilisateur final tout ce qui se passe à ce niveau. Il faut que l'adresse IP soit l'adresse correcte.

Il y a parfois des attaques qui se déroulent sur certaines adresses et cela peut donc changer l'adresse IP et le client va penser accéder au bon site alors que c'est un site parfois néfaste avec une utilisation malveillante qui peut apparaître.

Certains des éléments à considérer aujourd'hui en général dans des systèmes auxquels on accède, qu'on utilise sur internet, on utilise le service du courrier, de calendrier, de contacts, on a nos contacts sur notre téléphone. Si demain je change de téléphone, si mon téléphone se casse et si je veux changer mon calendrier, je peux le retrouver en ligne, la même chose pour les contacts ; tout cela se trouve dans le nuage et je vais pouvoir accéder à ces informations sans problème.

Service de base de données, données commerciales, données clients dans le cas des entreprises, données sur les fonctionnaires, inventaire, serveur de fichiers, formations financières à l'intérieur, documentation interne de l'entreprise, processus, procédures de l'organisation, tout cela, système de contrôle et de fonctionnement, par exemple le contrôle des équipements, s'il s'agit d'une entreprise, tous types de services, pas seulement un service lié à internet, cela peut être un service d'énergie, d'eau, donc des systèmes de surveillance qui à un moment donné vont être interconnectés et qui vont avoir des points de contact avec internet pour que l'on puisse y accéder de l'extérieur ou faire une surveillance à distance, mécanisme de sécurité avec les mots de passe, les contrôles d'accès, etc., les systèmes d'enregistrement et d'audit et beaucoup d'autres systèmes.

Moi, j'ai ici réfléchit en utilisant un peu mon bon sens. Et en Uruguay, on dit que des fois, le bon sens, c'est justement le sens le moins commun de nos sens, il faut donc l'entraîner. Donc ce qui peut paraître le bon sens n'est pas toujours quelque chose d'évident pour les autres et cela requiert une formation pour savoir qui est-ce qu'on peut trouver en face de nous, quels sont les moyens de résoudre le problème ou d'atténuer le problème si on ne peut pas le résoudre.

Donc tous ces éléments dont nous avons parlé, en général, ces éléments auxquels j'accède en ligne, commencent d'abord par une consultation DNS ou impliquent une consultation du nom de domaine. Donc on va revoir un petit peu le système de noms de domaine. Il s'agit d'un système qui est distribué. En ce qui concerne le stockage de l'information, cette information est distribuée à différents endroits dans différents serveurs. Et l'administration est aussi distribuée. Il n'y a pas une seule organisation administrative, il y a une administration distribuée et un protocole conçu pour que cela fonctionne.

Ces divisions administratives dans l'espace du nom de domaine sont appelées zones. Chaque administrateur d'une zone va administrer une partie du système mondial du DNS. On sait aussi qu'un administrateur d'une zone peut déléguer l'administration dans le sous-arbre puisque le DNS a une forme d'arbre renversé. À partir de la racine, on a les branches. L'administrateur, d'un point à l'intérieur de cet arbre, peut déléguer ce qui est en dessous en créant une nouvelle zone et en déléguant, il va créer des zones.

Et puis ensuite, on a d'autres types de serveurs, serveurs autorisés, serveurs récursifs, etc., ces serveurs faisant autorité et les serveurs

récursifs. Les serveurs qui font autorité sont ceux qui stockent l'information. L'information de chaque zone, de chaque domaine figure là-dedans. Et les serveurs résolveurs vont chercher les informations dans le système des noms de domaine dans des endroits, dans des représentations du client. Donc ce n'est pas le dispositif qui réalise la requête, la recherche, mais il va poser la question au serveur résolveur, au serveur récursif qui va faire la recherche à son tour.

Pourquoi est-ce que nous disons tout cela ? Il s'agit d'un exemple rapide avec un graphique sur lequel figure ces arbres. Nous faisons une petite révision parce que ma présentation va commencer à entrer dans différents points concernant ce système du DNS et nous allons essayer de voir comment les menaces agissent, quelles sont les menaces les plus courantes, s'il existe des mécanismes pour résoudre ces menaces, pour éviter ces menaces, ou s'il y a des menaces que l'on ne peut pas éliminer, est-ce qu'on peut au moins les atténuer, est-ce qu'il y a des protocoles, des mécanismes permettant d'atténuer ces menaces si on ne peut pas les faire disparaître.

Lorsque nous parlons de menaces, nous allons voir quels sont les types les plus courantes de menaces. Ce ne sont pas les seules, mais ce sont les plus courantes. Ce que l'on appelle le hameçonnage, c'est la pratique frauduleuse qui consiste à envoyer des courriels qui prétendent provenir d'entreprise ou de service que l'on connaît pour inciter les gens à révéler des informations personnelles. Ce hameçonnage va essayer de faire croire à la personne que cette personne accède à un service connu alors qu'en réalité, on va pousser l'utilisateur à révéler ses mots de passe, son numéro de carte de crédit, ses informations importantes pour ensuite utiliser ces informations

pour extraire ou injecter des informations ou accéder de manière non autorisée au système, aux comptes bancaires d'un utilisateur ou autres pour commettre un délit ou autre. Voilà donc le hameçonnage.

Les logiciels malveillants. Un logiciel malveillant est un logiciel destiné à un dispositif qui est conçu pour perturber une fonctionnalité d'un dispositif, pour endommager ce dispositif directement de manière provisoire ou permanente. Ou encore, ce logiciel malveillant est destiné à passer inaperçu de façon à obtenir un accès non autorisé à un système informatique pour extraire des informations. Donc si je veux des informations dans un site, je vais passer inaperçu. Et ensuite, je vais donc à travers ce logiciel malveillant accéder à ce site sans que personne ne le sache et sans qu'on sache que j'ai obtenu ces informations ou que ce soit trop tard et que je les ai déjà obtenues. Par exemple, on a le type de logiciels de rançon, de demande de rançon et autre.

Ensuite, on a le botnet. Le bonnet, il s'agit d'un réseau d'ordinateurs et moi, en tant qu'agresseur, je vais organiser ce réseau d'ordinateurs. C'est ce qui va me permettre de commettre une attaque sur un tiers. Et je vais avoir cette petite armée de dispositifs qui vont me permettre d'infecter un logiciel malveillant. Et si je veux faire par exemple un déni de service distribué, je vais envoyer un ordre à tous ces ordinateurs qui peuvent être des milliers d'ordinateurs que j'ai infectés, je vais envoyer un ordre, je vais réveiller ce logiciel et tous ces ordinateurs vont faire quelque chose de manière simultanée contre un tiers, par exemple envoyer de nombreuses données à un tiers. Et si on a un grand nombre de dispositifs qui envoient des données à cette même personne, ce qui va se passer, c'est que ce tiers va se retrouver avec une largeur de

bande complètement saturée et le service ne pourra plus être fourni de manière normale par cet usager. Donc on a ce type d'attaque. Il y a d'autre attaques beaucoup plus élaborées qui se basent souvent sur ce type de botnet.

Pourquoi est-ce que l'on parle de menaces du système de noms de domaine ou qui utilisent le système de noms de domaine ? Le système des noms de domaine, on l'utilise tous. Par conséquent, c'est intéressant de l'utiliser pour porter atteinte au service du DNS et par là, porter atteinte à l'ensemble des transactions puisque tout commence par une adresse IP. Donc les [inaudible] sont représentés par des adresses IP et je peux par ce biais interrompre des transactions commerciales, des services gouvernementaux et non gouvernementaux, des réseaux sociaux, des e-mails. Tous ces services passent d'une certaine façon par internet et une interruption peut être très grave ou catastrophique même dans certains cas. Si l'on parle de système de santé par exemple, cela peut être catastrophique, dans le cadre de l'énergie, de l'eau potable aussi. Exploiter le DNS permet de tromper, d'escroquer les utilisateurs pour accéder à des sites bancaires ou autres.

Certains vecteurs d'attaque que l'on peut utiliser qui sont les plus courants seraient l'enregistrement malveillante de noms de domaine. On enregistre dans les noms de domaine des sites qui disaient contenir des informations sur la COVID, les gens y accèdent et par là sans le savoir, en téléchargeant un fichier, ils téléchargent des virus et on accède à des informations. Mais en même temps, on met dans son propre ordinateur un logiciel malveillant.

Le détournement des services d'enregistrement de résolution de noms pour les personnes qui enregistrent les noms de domaine, l'altération générale des données DNS, la collecte de données par le biais de sites compromis dans le but de collecter des données sur l'utilisateur et l'extraction de données à l'aide du service DNS. Nous ne rentrerons pas dans le détail aujourd'hui, nous le verrons plus tard. Mais c'est un type d'attaque qui profite du fait que le DNS utilise le port 53 qui est connu pour transférer des informations et qui utilise ce même canal comme mécanisme pour extraire certaines informations qui doivent maintenir ce canal ouvert et qui, par conséquent, ne vont pas pouvoir résoudre le DNS et les attaquants vont tirer profit de cela pour extraire des informations et mettre en danger le système de ces organisations.

Cette diapositive que vous voyez ici est un aperçu général de ce qui serait le système du DNS dans son ensemble avec les registres, les utilisateurs, les bureaux d'enregistrement, les titulaires de nom de domaine, les opérateurs de registre.

Ici, vous voyez celui qui envoie la requête, celui qui la cherche et ensuite, vous avez tous les autres acteurs de cet écosystème. Ici, vous avez ces croix rouges et cela montre plusieurs points où une attaque peut survenir, où il peut y avoir une attaque à ce niveau. Ce sont des points d'attaques potentielles.

Ce que nous allons étudier maintenant, c'est une description de certains de ces mécanismes qui existent dans le DNS, dans cet écosystème, pour opérer à ces points et éviter ou limiter les attaques lorsqu'on ne peut pas totalement les annihiler. Donc c'est une course sans fin et il y a une motivation des attaquants qui recherchent toujours de nouvelles

vulnérabilités. Et plus le logiciel est complexe, plus il va être facile d'attaquer et plus il y aura de vulnérabilités. On peut réparer ces vulnérabilités, mais cela prend du temps.

Les attaquants sont très créatifs et parfois très sophistiqués. Il n'y a pas de héros ici. Les attaquants ont toujours un coup d'avance et il y a des mesures de prévention, mais très souvent, ce sont des mesures réactives et il faut que l'intrusion soit détectée et gérée rapidement. Il y a beaucoup de recherches qui sont faites à ce niveau pour trouver de nouveaux mécanismes à mettre en œuvre pour avoir plus de prévention. Donc il y a toujours de nouveaux mécanismes et des solutions de mitigation, d'atténuation en cas d'attaque.

Il y a des mécanismes pour limiter ces attaques. Nous allons parler tout d'abord de ces serveurs faisant autorité. Imaginez que vous ayez l'autorité pour un nom de domaine. Mon nom de domaine est je ne sais pas, nicolas.com. Si j'avais ce nom de domaine, je pourrais mettre en œuvre mes serveurs DNS et j'ai les fichiers de zone pour nicolas.com, j'ai mon sous-domaine, j'ai différents documents à nicolas.com sur mon site web, etc. Je maintiens donc cette zone. Cette zone peut être emmagasinée sur plusieurs serveurs, un seul serveur possiblement ou bien plusieurs serveurs. C'est ce dont nous parlons ici. Plutôt que d'avoir un seul serveur, avoir plusieurs serveurs qui soient identiques, qui ont toutes les données pour ma zone nicolas.com.

À chaque fois qu'un serveur récursif essaye de résoudre une adresse IP de mon domaine nicolas.com, ils vont être en mesure d'envoyer des requêtes à ces serveurs faisant autorité parce que les données sont les mêmes dans ces serveurs. Comme je l'ai expliqué, si j'ai un seul serveur,

je peux également répliquer ces données. Donc cela, c'est une réplication, un doublon de zone et cela peut être un mécanisme qui permet à chaque serveur que vous choisissez, pour toute application que vous choisissez, que toute ces applications mettent en œuvre cette fonctionnalité.

C'est relativement simple de créer plusieurs serveurs et d'activer ces protocoles pour que chaque serveur ait toutes les données et j'exécute les modifications dans un serveur et je fais des copies pour tous les autres serveurs pour qu'il y ait toutes les données dans tous les serveurs. Cela a un avantage. Lorsqu'il y a une attaque sur un serveur, je sais qu'il va avoir un échec, une attaque, je vais le noter, ce serveur est hors service. Mais si j'ai trop de requêtes qui arrivent – c'est un type d'attaque – et un nombre important de requêtes, ce que je peux faire, c'est que la charge peut être mise sur plusieurs serveurs et non pas sur un seul. Donc cela va permettre d'atténuer la charge, de limiter les problèmes et là, le système devient plus résilient.

Il y a une autre technique également que je peux utiliser qui s'appelle AnyCast. Lorsqu'il y a une réplication avec ces serveurs faisant autorité, je peux mettre cela en œuvre de deux manières. D'abord, avoir plusieurs serveurs pour la même zone lorsqu'un nom de domaine est délégué. Il y a des sous-domaines au niveau parent et au niveau enfant, il y a des délégations, donc il y aura des archives du DNS qui vont simuler le nom de domaine du serveur et des serveurs faisant autorité. Donc je peux lister plusieurs noms de serveurs et à chaque fois qu'un serveur récursif cherche des informations et me demande quel est le serveur faisant autorité pour cela, je peux donner un nom, peut-être un seul registre ou bien une liste de noms et le serveur récursif va essayer

d'atteindre tous ces serveurs faisant autorité. Donc si le serveur récursif fait une requête et qu'il n'y a pas de réponse, il va passer au suivant sur la liste. Donc je peux avoir une liste de noms de serveurs et donc avoir des copies.

L'autre technique, c'est Anycast. C'est une technique qui est un petit peu différente. C'est défini comme avec des adresses IP, protocole internet. C'est un ensemble d'adresses internet et il y a la destination du paquet qui passe par un système de routage et de réseaux. Il n'y a pas besoin de configuration spéciale, mais ce qui est requis, c'est que la même adresse IP soit affectée, soit assignée à ces serveurs faisant autorité. Là, il n'y a plus de noms différents mais il y aura la même adresse IP. Vous pouvez vous demander comment l'accès va se faire. Ce sont des copies, donc ce sont les mêmes informations. Et cela n'importe pas quel serveur va être atteint, vous allez obtenir les mêmes réponses. Donc là, j'ai la même adresse IP pour différents services et là, j'ai les mêmes informations.

Dans ce cas de figure avec Anycast, il y a plusieurs serveurs faisant autorité, tous les serveurs faisant autorité utilisent la même adresse IP et lorsqu'il y a une requête, le routage va décider d'où envoyer le paquet et il y aura une réponse qui sera effectuée. Donc Anycast est un mécanisme similaire qui a beaucoup d'avantages pour les serveurs DNS. Il y a donc une redondance, il y a une résilience qui est apportée. Et comme on l'a vu, il y a une distribution des charges et des requêtes et cela réduit le temps de latence parce que vous avez la même adresse IP et vous pouvez aller au plus près du client. La requête va être envoyée au plus près et donc, moins de temps de latence, une résolution plus

rapide et plus de solidité dans le système et une atténuation des dénis de service, des attaques de distribution contre l'infrastructure du DNS.

Anycast peut être appliqué aux serveurs faisant autorité et aux serveurs récursifs. Vous pouvez avoir plusieurs serveurs récursifs. On va pas trop rentrer dans les détails de la mise en œuvre, ce sera pour un autre webinaire que nous ferons cela. Nous parlerons de routage plus précisément lors d'un autre webinaire. Mais cette technique de serveurs faisant autorité, c'est très important. C'est très important d'avoir les mêmes informations dans chaque serveur et il faut qu'il y ait un mécanisme dans la zone avec un nombre défini de serveurs.

Les opérateurs de serveurs racines, là, vous avez aussi la possibilité d'avoir plus de résilience au niveau du DNS, pas seulement tout le système du DNS, mais les serveurs racine. Vous savez que la racine du DNS, c'est là où commence cet arbre, cette racine. Cette racine du DNS, je simplifie un petit peu les choses, on peut dire que le propriétaire ou le gérant de cette racine de ces données, c'est l'ICANN et les fonctions IANA. C'est centralisé au niveau de l'ICANN et l'ICANN gère cette mise en œuvre de ces serveurs racine, elle opère ces serveurs racine et c'est une organisation de maintien et de maintenance de ces serveurs racine.

Nous avons d'autres organisations qui existent. Vous avez différents serveurs racine, vous en avez 13, mais A et J, c'est Verisign. En fait, vous n'en avez que 12. Vous avez 13 lettres, mais 12 opérateurs de serveurs racine qui chacun gère un serveur de la zone racine indiqué par des lettres. En fait, il y a des centaines de serveurs pour chacun d'entre eux, parce que chaque organisation comme l'ICANN met sur plusieurs

serveurs les mêmes adresses IP. Il y a plusieurs copies qui existent et il y a une maintenance de toutes ces copies des serveurs racine. Et voilà donc les sites où se trouvent... C'est le site serveurracine.org et vous avez une liste de tous les serveurs racine qui se trouvent dans le monde entier aujourd'hui. Vous voyez les informations, c'est aujourd'hui le 18 avril et c'est très précis comme site web. C'est remis à jour constamment, 1 533 instances opérées par ces 12 opérateurs de serveur racine, ces 12 opérateurs indépendants pour la zone racine gérée donc par une de ces 12 organisations dont nous avons vu la liste. Et vous voyez par exemple dans notre région, nous en avons 29 au nord près des Caraïbes et il y a 110 copies qui se trouvent en Amérique du Sud. Nous en avons 266 qui se trouvent aux États-Unis et il y en a quelques-uns qui se trouvent pour le nord des Caraïbes également sur ces serveurs, plusieurs que maintiennent ces organisations.

Pour la racine du DNS, pour cette racine, je maintiens beaucoup de copies pour que quelqu'un, un serveur récursif, lorsqu'on commence cette recherche, puisse accéder à ces copies et obtenir des informations. En ayant beaucoup de copies proches, ce que l'on va avoir, c'est davantage de résilience, moins de latence, plus de tolérance, plus de capacité pour atténuer et contenir ces attaques et en définitif, une meilleure qualité de service perçue par les utilisateurs lorsqu'ils vont faire la résolution de ces noms de domaine. Ces programmes qui existent à travers ICANN et d'autres organisations qui gèrent et maintiennent les serveurs pour la zone racine, on peut maintenir et installer une copie de ce serveur racine dans son pays, dans sa région, etc. C'est une manière aussi d'augmenter la résilience et la sécurité du système du DNS, donc la sécurité du DNS.

Je ne sais pas s'il y a des questions. Je vais peut-être un peu vite. Est-ce qu'on est bon au niveau du temps ?

SILVIA VIVANCO : Oui, c'est bon. Et il n'y a pas de question, juste un commentaire. Je vous l'enverrai pour que vous puissiez le lire.

NICOLAS ANTONIELLO : Parfait, donc on continue.

Le DNSSEC, la sécurité, c'est une caractéristique des extensions de sécurité du DNS conçue pour augmenter la sécurité du système. On appelle cela un système de sécurité et c'est le DNSSEC. Vous vous souvenez de cet aperçu que je vous ai montré concernant l'écosystème mondial du DNS où agit le DNSSEC dans ce système et qu'est-ce qu'il apporte. Il agit entre le serveur récursif et le serveur faisant autorité. Donc ici, on a le client, il va envoyer la question au serveur récursif qui va la chercher entre différents serveurs faisant autorité en commençant toujours par la racine. Une fois qu'il obtient la réponse, il l'envoie aux clients. Et ce dialogue entre le serveur récursif et le serveur faisant autorité, c'est ce qui peut être assuré en utilisant le protocole DNSSEC.

Qui doit déployer ce protocole DNSSEC ? Quels sont les participants qui doivent déployer ce protocole DNSSEC ? Ce sont ceux qui administrent des serveurs récursifs et ceux qui administrent des serveurs faisant autorité. Le client ne peut pas le faire, c'est quelque chose qui se passe entre ces serveurs. Le DNSSEC va être pour les administrations de serveurs récursifs et faisant autorité.

Que fait le DNSSEC ? Le DNSSEC utilise la cryptographie de clé publique. On verra plus tard de quoi il s'agit. C'est un type de cryptographie qui permet de chiffrer des données et des signatures numériques afin de fournir une authentification d'origine. Lorsque je fais une requête, j'obtiens une réponse de ce serveur faisant autorité. L'authentification d'origine me permet d'être sûr que la réponse obtenue qui est venue par internet est réellement venue du serveur qui a l'autorité de me donner cette réponse et non pas d'un site d'un serveur DNS d'un attaquant et qu'il ne s'agit pas d'une fraude. Donc cela me permet de savoir de qui provient cette information et que cette personne a vraiment l'autorité pour m'envoyer cette information.

Et l'autre chose, c'est l'intégrité des données. Cela assure que ces données, quand elles ont voyagé du serveur faisant autorité au serveur récursif, n'ont pas été modifiées. Si les données ont été modifiées et si j'ai le DNSSEC, je vais le savoir. Je vais recevoir ces données, je vais savoir si ces données ont été altérées ou pas. Donc authentification d'origine, intégrité des données. Si ces données ont été altérées, je vais le savoir, sinon je vais être sûr que les données sont les données correctes. Par exemple, si je rentre dans ma banque, je mets www.mabanque.com, si la banque n'a pas le DNSSEC, je ne sais pas si j'accède correctement à ma banque ou à un site malhonnête. C'est comme cela qu'on va être sur que l'on accède correctement aux sites que l'on souhaite accéder. Je peux avoir accès à une page identique à celle de ma banque et je vais mettre mon mot de passe et j'ai perdu. Si la banque a déployé le DNSSEC, quand ce serveur récursif va recevoir la réponse du serveur faisant autorité, si ces données, si cette réponse a été falsifiée, le serveur récursif va s'en rendre compte et il ne va pas

donner la direction IP aux clients. Il va envoyer un message d'erreur et votre client va dire : « Je ne peux pas rentrer dans ma banque, c'est bizarre. Qu'est-ce qui se passe ? » En réalité, ce qui se passe, c'est que le serveur récursif s'est rendu compte qu'il y a eu une manipulation des informations et va m'empêcher d'accéder à ceci. Donc le protocole DNSSEC évite ce type d'attaque. Il offre une protection contre la falsification de données du DNS et il évite des attaques d'empoisonnement du cache dont nous parlerons plus tard.

Qu'est-ce que le DNSSEC ne fait pas maintenant ? Il fournit une confidentialité dans l'échange de données du DNS ? Non, il ne fournit pas de confidentialité et il n'évite pas non plus des attaques de déni de service. Ce qu'il fournit, c'est une protection contre la falsification des données, c'est tout, pouvoir être sûr que ces données n'ont pas été manipulées, mais il ne fournit pas de défense contre une attaque de déni de service et il ne fournit pas de confidentialité dans les échanges de données du DNS.

Quels sont les avantages techniques ? Il fournit une authentification, une validation d'origine, il offre l'intégrité et la non-manipulation des données du DNS. Il permet de dire aussi à un client... Parce que, que se passe-t-il si je veux rentrer dans une page qui n'existe pas ? Je vais recevoir une réponse. Est-ce que je sais si cette réponse est authentique ? Est-ce que quelqu'un a falsifié l'information en me mentant ou est-ce que vraiment ce site n'existe pas ? Le DNSSEC dispose d'un mécanisme qui permet aux sites faisant autorité de ce nom de domaine de me dire : « Ce domaine que vous consultez n'existe pas, je vous l'affirme, il n'existe pas. » Le client peut être sûr que ce qu'on lui

dit, c'est vrai, qu'il ne s'agit pas d'un mensonge. Cela me permet d'être sûr que ce site n'existe pas. Donc ce sont les bénéfices techniques.

Au niveau de l'impact sur les différents membres de l'écosystème, cela donne une certaine confiance à l'utilisateur final, il est sûr d'être arrivé là où il voulait dans le cas de HTTPS par exemple. Pour le titulaire de nom de domaine, atténuation de la fraude, protection renforcée de la marque. Pour le bureau d'enregistrement, cela répond aux normes de l'industrie, cela satisfait les demandes des titulaires pour une plus grande sécurité, cela permet d'attirer et de retenir les clients, les titulaires de nom de domaine en se basant sur la sécurité et sur la réputation. C'est très important dans ce domaine. Et puis, pour ce qui est des opérateurs de registre, ils se conforment aux meilleures pratiques du secteur et aux demandes des bureaux d'enregistrement pour une sécurité accrue des domaines.

SILVIA VIVANCO : Nicolas, excusez-nous, maintenant, c'est l'heure et je voudrais vous lire quelques questions que vous avez reçues, par exemple des questions d'Alejandro Pisanty, pour conclure parce qu'il ne nous reste juste une demi-heure pour cet appel et nous avons encore d'autres choses à aborder dans notre ordre du jour.

NICOLA ANTONIELLO : Parfait, vous avez déjà un certain nombre d'informations. Nous verrons le reste dans la deuxième partie de notre séminaire web.

SILVIA VIVANCO : Très bien, Nicolas. Nous aurons donc une autre présentation et c'est passionnant. Je vais vous poser des questions, vous lire les questions.

« Le DNSSEC avait un effet secondaire non désirable, faciliter la publication de zones entières. Comment est-ce qu'on atténue ce problème dans l'actualité ? » Deuxième question : « Dans quelle mesure est-il possible de déployer le DNSSEC vu le coût et la complexité pour un entreprise ? »

NICOLAS ANTONIELLO : Merci Alejandro pour ces questions.

En ce qui concerne la première question, je vais voir un petit peu, question concernant les effets secondaires non indésirables du DNSSEC qui faciliteraient la publication ou ce que l'on appelle le parcours de la zone. Si j'ai bien compris ta question, Alejandro, pour expliquer aux autres en quoi cela consiste, il est vrai qu'avec ce mécanisme de DNSSEC à travers lequel je vais pouvoir être sûr qu'un site n'existe pas, je peux être sûr que ce n'est pas un mensonge de quelqu'un d'autre.

Les premières mises en œuvre de ce protocole s'appellent NSEC. Et ce protocole, son implémentation ou cette partie du protocole, ses premières implémentations permettaient qu'un attaquant, qu'un agresseur avec un certain degré de technologie puisse faire des requêtes et parcourir une zone de cette manière et savoir quelles étaient les zones qui existaient et quelles étaient celles qui n'existaient pas. Par exemple pour le dictionnaire, je vais envoyer des mots d'un dictionnaire qui ont un sens pour les êtres humains de manière pseudo aléatoire. Je vais faire des requêtes avec ces mots pour savoir s'il y a des

domaines associés avec ces mots. Donc je vais demander à un serveur un domaine, un autre, un autre, un autre. Quand il existe, je vais avoir une réponse positive, quand il n'existe pas, je vais aussi avoir une réponse mais négative. Et je vais pouvoir comme cela avoir une copie de la zone sans avoir besoin d'accéder au serveur pour copier tout cela.

Il existe une autre version de ce protocole qui s'appelle DNSSEC 3, qui modifie la façon dont le DNS répond lorsqu'il n'y a pas de zone et qui réduit énormément et rend presque impossible de faire ce parcours de zones et d'obtenir ces informations. Mais cela dépend de celui qui déploie ou qui implémente le DNSSEC, s'il a les autres programmes dont j'ai parlé, NSEC, etc. Cela s'applique seulement pour obtenir toutes les informations d'une zone, parce que ces zones, par définition, son publiques.

Des fois, on est très soigneux ou très prudents, les bureaux d'enregistrement ou les opérateurs de registre qui gèrent tout cela font attention de ne pas révéler ces fichiers de zones qui sont publics, sinon ils ne répondent pas à leurs objectifs. Ils doivent être capables de répondre à quiconque fait une requête. Par conséquent, le fait d'obtenir toute une zone n'implique pas non plus nécessairement que cela soit un problème de sécurité. Cela peut être un problème parce qu'on obtient la liste de clients d'un opérateur de registre en particulier, ce qui peut être un problème de sécurité pour cet opérateur de registre, mais ce n'est pas un problème de sécurité pour les utilisateurs et ce n'est pas non plus un problème de sécurité pour le système de noms de domaine. Mais c'est une préoccupation dont on peut tenir compte pour les opérateurs. Il y a des fichiers de zones qui sont publics. Par exemple la zone racine est publique et quiconque peut la charger, la télécharger

dans sa totalité. Il y a d'autres fichiers de zones qui sont publics. Mais si on descend un peu plus dans la hiérarchie, ce n'est pas nécessairement le cas. Ces zones ne sont pas nécessairement publiques. Cela dépend d'un business du bureau d'enregistrement, c'est sous sa responsabilité et il va devoir atténuer ce risque.

Le deuxième point également, la taille pour un responsable qui va être mis en œuvre le DNSSEC. On a parlé des saveurs faisant autorité et des serveurs récursifs. Pour les saveurs récursifs, cela ne sera pas utile. Si vous déployez un protocole pour des serveurs faisant autorité, ce ne sera pas utile. Il faut déployer sur les deux, sur les serveurs récursifs et faisant autorité et il ne va pas y avoir trop de charges à ce niveau. Si vous indiquez à un serveur récursif mis à part les communs, ils ont déjà par défaut le DNSSEC, si vous avez une idée de la charge, il n'y aura pas de problème. Donc les personnes qui ont eu des serveurs depuis de nombreuses années et qui n'ont pas mis en œuvre le DNSSEC, cela peut poser problème. Mais le DNSSEC ne surcharge pas, c'est tout à fait négligeable au niveau de la charge ce qu'apporte le DNSSEC, cela ne pose pas de problème. Mais il faut surveiller les protocoles, il faut résoudre tous ces protocoles.

Pour les serveurs faisant autorité, c'est plus complexe. Là, vous avez la signature, vous devez activer les clés, vous devez avoir des mécanismes de maintenance et cela peut être plus ou moins coûteux, cela dépend si votre serveur joue un rôle critique ou pas. Chaque jour, je peux avoir des centaines de nouveaux noms de domaine, c'est possible, mais le DNSSEC doit être intégré pour ces noms de domaine. Donc c'est tout à fait possible maintenant, il y a beaucoup d'expériences concernant le

DNSSEC depuis plusieurs années et il y a beaucoup de formations également qui sont disponibles pour le DNSSEC.

Et Alejandro, ce que je voulais dire, c'est qu'à l'ICANN, nous invitons les opérateurs et les contractants à se former et à déployer le DNSSEC sur leurs serveurs récursifs et sur les serveurs faisant autorité. On est là pour les soutenir au niveau technique, mais nous assurons des formations pour que cela se fasse pour les opérateurs et pour qu'il y ait plus d'efficience. Pour les serveurs faisant autorité, là, cela peut coûter plus cher et ce n'est pas seulement une question de formation.

Mais ce que je peux dire du DNSSEC rapidement, c'est que le DNSSEC doit être mis en œuvre par tous et toutes. C'est extrêmement important et ce protocole DNSSEC permet beaucoup d'assurer la sécurité.

SILVIA VIVANCO : Je vois qu'il y a encore des mains de levées, mais on n'a plus beaucoup de temps, Nicolas. Donc Nicolas, si vous êtes d'accord, nous allons vous remercier et vous allez revenir nous parler. Et désolée pour Sergio et Carlos, mais nous n'avons plus beaucoup de temps et nous avons encore beaucoup à l'ordre du jour. Carlos, vous pouvez envoyer les questions directement à Nicolas ou nous allons les lui envoyer. Vous pouvez les envoyer par l'intermédiaire du personnel.

NICOLA ANTONIELLE : Oui, je serais très heureux que d'y répondre et je couvrirai ces questions lors du prochain webinaire.

SILVIA VIVANCO : Oui. Merci beaucoup.

Augusto, vous pouvez poursuivre maintenant.

AUGUSTO HO : Merci Silvia.

J'aimerais beaucoup remercier Nicolas de sa participation et de sa présentation et de son engagement pour vraiment nous informer beaucoup sur ces thèmes.

Nous allons avancer dans notre ordre du jour maintenant. Nous allons donner la parole à León Sanchez qui va effectuer un rapport sur le Conseil d'Administration de l'ICANN. León, vous avez la parole.

LEÓN SANCHEZ : Merci beaucoup.

Bonjour à toutes et à tous. Le Conseil d'Administration a été très actif ces derniers mois et nous avons eu notre atelier du Conseil d'Administration avant l'ICANN73 et nous avons eu de nombreuses interactions avec la communauté pendant l'ICANN73.

Nous avons commencé notre atelier le 1er mars et nous avons ouvert plusieurs points stratégiques, une analyse des tendances stratégiques qui se dessinent, et cela nous permet de voir tout l'écosystème et d'anticiper les problèmes qui peuvent survenir qui vraiment nécessitent notre attention et l'attention de l'organisation ICANN et du Conseil d'Administration. Le niveau de participation que nous devons avoir dans

ces domaines a été pris en compte, on a analysé les tendances les plus pertinentes dans les domaines qui peuvent poser problème à l'ICANN.

Par exemple, je pourrais mentionner le système de résolution des noms de domaine alternatif avec le blockchain notamment. Il y a des systèmes alternatifs qui peuvent avoir un impact fort sur l'internet et c'est un débat que nous devons avoir. On a besoin d'interaction avec ces systèmes alternatifs. C'est juste un exemple des différentes tendances dont on a parlé au niveau stratégique pendant notre atelier du Conseil d'Administration.

Nous avons également eu une séance durant laquelle nous avons analysé les différentes activités des gouvernements et également dans l'écosystème de l'ICANN, des initiatives qui se déroulent dans différents pays, différentes réglementations qui peuvent avoir un impact sur l'ICANN.

Lors du second jour de notre atelier, nous avons parlé d'utilisation malveillante du DNS et des recommandations provenant du SSR et du SSR2. Nous avons également parlé d'une proposition d'avoir une révision du SSR3 qui se déroule plus tard. Le Conseil d'Administration à une résolution pour remettre à plus tard la troisième révision de SSR pour s'aligner avec les recommandations spécifiques de l'équipe de révision de l'ATRT3, qui ont indiqué que les prochaines révisions du SSR devraient être remises à plus tard, une fois que toutes les recommandations de l'ATRT3 seront mises en œuvre. Nous avons accepté cela et nous devons attendre la prochaine version de l'ATRT.

Nous avons travaillé avec Göran Marby également. Nous avons parlé du système d'atténuation des attaques contre le DNS. Et il a également

effectué un rapport sur l'utilisation malveillante du DNS. Nous avons passé du temps également à analyser comment nous pouvons prioriser ces différentes activités du Conseil d'Administration pour s'aligner avec la communauté.

Et bien entendu, le Conseil d'Administration doit s'engager dans de nombreuses activités. Et il faut voir l'urgence de certaines, la pertinence de certaines activités. Donc, nous faisons ce type d'analyse.

C'est un exercice tout à fait intéressant pour qu'on ne travaille pas d'une manière unilatérale. Nous voulons nous assurer que nous ayons également la communauté qui nous informe et qui ait voix au chapitre et que nous puissions travailler de cette manière. On regarde tous les éléments qui rentrent en ligne de compte dans l'ICANN en tant qu'organisation. Le Conseil d'Administration, c'est un élément simplement de l'ICANN et l'exercice de priorisation, c'est pour tout l'ICANN.

Le dernier jour de notre atelier, nous avons observé les résultats pour la prochaine série et l'opérationnalisation de la prochaine série, on a regardé l'évolution de l'ODP. Nous avons pris en compte les nouvelles séries de nouveaux gTLD. Et nous avons eu également notre réunion du Conseil d'Administration où nous avons accepté des résolutions. La première, j'en ai déjà parlé, la révision de l'ATRT3. Nous avons également adopté une résolution pour la phase 2A du EPDP à partir du travail du conseil de la GNSO.

Et nous avons soumis pour considération auprès du Conseil d'Administration des points concernant le processus de révision indépendante avec .web. Il y avait une controverse au niveau de .web et

il y avait un litige entre différentes parties prenantes qui ont participé à l'enchère pour obtenir ce nouveau gTLD de délégué. Il y avait un conflit d'intérêt qui existait et nous avons analysé la situation. Il y avait un processus de règlement de litiges, cela n'a pas été en justice. Ensuite, ce processus a été lancé. On a évité la résolution de ce processus en faisant quelques recommandations. Et on a soumis à la considération du conseil de direction cette résolution et le comité de mécanisme de révision des comptes va réviser cette résolution en détail et faire des recommandations au Conseil. Cela n'est pas terminé, cela va suivre son cours et va être analysé par ce comité. Il y aura d'autres commentaires à faire.

Une autre résolution dont vous avez probablement entendu parler est ce qui concerne la constitution d'un fonds d'urgence pour soutenir un accès continu à internet. Cela provient de la crise vécue actuellement en Ukraine suite au conflit entre l'Ukraine et la Russie dans la région. Et on a décidé de faire un apport d'un million de dollars pour que l'on puisse commencer à travailler avec des personnes dans la région pour garantir un accès continu à internet dans cette zone de conflit dans la mission de l'ICANN bien sûr en s'assurant qu'il y ait en permanence une transparence complète de la gestion des fonds. Voilà.

Donc je dirais que c'est ce qui a été fait par le Conseil. La semaine prochaine, nous serons à Los Angeles pour la première fois depuis longtemps. Une réunion présidentielle va avoir lieu avec des leaders des différentes organisations de soutien et des comités consultatifs et avec le Conseil. Ce sera notre première réunion en présentiel depuis longtemps. Je vous donnerai des détails par la suite concernant cet

atelier qui va avoir lieu à Los Angeles. Je continuerai à assumer mon poste de vice-président.

Je vous remercie Augusto, je reste à votre disposition s'il y a des questions. Merci.

AUGUSTO HO : Merci beaucoup Léon.

Rapidement, nous allons donner la parole à Carlos.

CARLOS AGUIRRE : Merci beaucoup Augusto.

J'avais levé la main pour poser une question à León, mais vu que nous avons peu de temps, je ferai parvenir ma question à León d'une autre manière.

Mon intervention ici dans cette réunion est liée à beaucoup de choses que León a mentionnées. Il s'agit de ce que l'on fait au niveau du groupe de travail des politiques consolidées de l'ALAC qui se réunit tous les mercredis. Je voudrais demander au personnel de l'ICANN de mettre à la disposition de tous les participants ici le lien de cette réunion, qui est une réunion ouverte à laquelle vous pouvez tous participer de façon à être au courant de ce qui se fait dans ce groupe de travail. Je vous le dit rapidement vu qu'il y a très peu de temps.

Les thèmes traités dans ce groupe de travail des politiques consolidées sont liés à l'utilisation malveillante du DNS. Lors de notre dernière réunion, on a parlé d'enregistrements malicieux, quelque chose qui a eu

lieu pendant la pandémie, on le sait, et des différentes manières d'atténuer ces attaques, ce type d'attaques ou ce type de situations qui sont très compliquées pour les utilisateurs.

Un autre thème traité a été le processus de la révision de la politique de transfert de domaines et on a abordé un point important ici en parlant de la complexité du RGPD et du fait que le RGPD a donné davantage de complexité à l'ensemble du système. On a parlé de délai pour faire ce type de transfert en tenant compte très souvent de l'intérêt des opérateurs de registre. Et il me semble que dans la région, on devrait davantage travailler, on devrait approfondir cette question pour mettre en première ligne l'intérêt des utilisateurs finaux de l'internet parce que très souvent, il s'agit d'une question personnelle. Je vois très souvent donc qu'il y a des gens qui sont des membres du comité ALAC qui, de par leur ancienneté ou par leurs relations, ont une influence sur différentes prises de position de la GNSO ou de l'unité constitutive commerciale. Et je pense qu'il y a beaucoup d'intérêts ici, que l'on veut contrôler les intérêts économiques, les intérêts de la part des opérateurs de registre et on ne tient pas vraiment compte des utilisateurs finaux. Donc c'est quelque chose qui devrait être pris en compte dans la région quand on parle de l'utilisation malveillante du DNS, pour voir comment faciliter un système de plaintes pour les utilisateurs de l'internet de façon à faciliter, en tout cas à offrir une solution aux utilisateurs qui ont vécu des violations de leur droit.

Une autre question abordée dans ce groupe de politiques consolidées, il s'agit du EPDP sur les domaines internationalisés qui est lié à la question de l'acceptation universelle. Ici, il y a plusieurs questions par rapport à

différents pays de notre planète avec des traits particuliers, par exemple le Myanmar.

Et une autre question, je m'excuse, je passe un peu rapidement, le système d'accès SSAD qui a aussi été traité dans le cadre de ce groupe de l'ALAC. Et ce que l'on traite maintenant, et c'est important parce qu'il y a des délais ici et dates butoirs qui arrivent à leur fin, c'est l'ordre du jour de la prochaine réunion de l'ICANN, l'ICANN74, et quels sont les thèmes que l'on va aborder au cours de cette réunion avec d'autres questions, parce qu'il s'agit d'une réunion hybride, peu de gens vont pouvoir s'y rendre et participer de manière présidentielle. Beaucoup vont participer à distance et comment est-ce qu'on va réunir ces deux types de participation. C'est une espèce de défi parce que c'est quelque chose de nouveau pour nous et pour eux, pour les organisateurs et pour les participants, donc on va voir ce que cela va donner pour les prochaines réunions de l'ICANN.

Une autre question importante, pour l'ICANN74, ce sera le premier jour à la première heure pour la communauté At-Large et c'est quelque chose qui découle de l'intérêt de la GNSO, je l'assume en tant que tel, c'est quelque chose que je dis en mon nom, pour gérer les questions des procédures ultérieures. Ce que la GNSO veut, c'est de voir ce qui se passe avec la nouvelle série de nouveaux gTLD. Je ne sais pas si cela intéresse les utilisateurs finaux, cela intéresse le secteur, l'industrie, les unités constitutives commerciales et ils font une promotion de cela. Et c'est là que nous sommes concernés, parce que les membres de l'ALAC doivent fournir des conseils sur ces questions. Voilà, c'est ce que je pouvais dire.

J'en ai terminé. Je vous remercie pour votre temps. J'étais un petit peu rapide et je m'en excuse. Je voulais essayer d'être le plus rapide possible.

AUGUSTO HO : Merci Carlos.

Nous allons donner la parole à Sergio Salinas Porto qui va nous mettre au courant du programme LAC digital.

SERGIO SALINAS PORTO : Bonjour, bonsoir. Merci Augusto. Je vais être bref de façon à ce que cette réunion finisse à l'heure.

Nous avons avancé, nous avons reçu l'acceptation des trois thèmes. On est en train de voir s'il peut y avoir quatre participants, mais pour le moment, nous avons trois participants garantis, ce qui nous mettrait dans une situation positive parce que les deux autres objectifs que nous avons au niveau du service public essentiel et au niveau de l'infrastructure en zone rurale, on avance et on va continuer à avancer. Je pense qu'à la fin de cette semaine, on va avoir les 12 pays et les 24 orateurs qui vont intervenir de façon à ce qu'on puisse avoir notre site web qui est presque terminé. Il nous manque les photos et les CV des personnes qui vont intervenir au niveau des gouvernements et de la société civile.

Je pense qu'on va presque pouvoir présenter un événement qui arrivera au 17 mai et qui permettra d'avoir une salle pleine. Dans quelques jours, nous aurons d'avantage d'information et on pourra avancer dans

ce domaine. De toutes façons, je m'engage, comme je l'ai dit la semaine dernière, à vous envoyer un rapport par écrit à toute la région. Je vais le faire.

Et je profite de l'occasion que j'ai aujourd'hui pour dire à mon ami Alejandro Pisanty que demain, par mail ou par téléphone, je vais le joindre, je voudrais qu'on en parle un petit peu plus.

Merci beaucoup. Voilà, c'est tout ce que je voulais dire.

AUGUSTO HO : Merci beaucoup Sergio de cette mise à jour sur LAC digital.

Nous allons maintenant donner la parole à Claire Craig qui va nous dire quelques mots sur les élections pour 2022. Claire, vous avez la parole.

CLAIRE CRAIG : En ce qui concerne les deux postes disponibles, pour le moment, je crois que vous devez le voir à l'écran, ces postes sont pour un représentant pour l'ALAC, c'est pour la région Antigua, Brésil, Paraguay et Uruguay et la position de NomCom pour la région, [inaudible], Amérique centrale, Mexique, Bélize, Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua, Mexique et Panama.

En ce qui concerne ces élections, aujourd'hui nous avons... Je vais parler un petit peu plus lentement. Le 18 avril, aujourd'hui, il y a eu l'annonce de cet appel à la nomination. Entre le 18 et le 29, nous allons avoir la période de nomination, 10 jours ouvrables. La date limite pour l'acceptation, c'est le 6 mai. Ensuite, jusqu'au 12 mai, il y a la possibilité d'avoir des appels avec les candidats. Du 13 au 14 mai, il y a les

élections qui vont se dérouler pas plus tard qu'une semaine après la date limite pour l'acceptation de nomination et elle va se terminer pas plus tard que deux semaines à la suite de cette date limite. Lors de l'AGM 2022 de l'ICANN75, les membres de l'ALAC nouvellement élus et les leaders des RALO prendrons place à la fin de l'AGM 2022 à la suite de la fin du Conseil d'Administration le 22 septembre 2022.

Toutes les informations sont disponibles sur le wiki. Je sais que je devais aller très vite aujourd'hui, mais effectuez vos nominations s'il vous plaît. Vous avez les différents territoires que vous avez vus, ces régions. [inaudible] et D, donc d'Amérique centrale, Mexique pour le NomCom.

Merci beaucoup.

AUGUSTO HO : Merci beaucoup Claire.

Nous sommes un petit peu en retard. Nous allons devoir clore cet appel, cette réunion. Nous pourrons aborder d'autres points lors de la prochaine réunion.

J'aimerais vous demandez donc de remplir le questionnaire. Nous avons quelques minutes néanmoins pour Vanda. Vanda, en deux minutes, vous avez la parole.

VANDA SCARTEZINI : Merci beaucoup.

Oui, c'était simplement une demande pour effectuer un court rapport sur le fait que tout s'est très bien passé avec la réunion présidentielle à

Washington aux États-Unis pour le NomCom qui s'est retrouvé avec 14 personnes. Tout s'est très bien passé. Nous avons été testés chaque jour à 7 h du matin avant d'entrer dans la salle. Nous étions tous en forme, sans problème. Et je voulais donc partager avec vous que tout a été très bien organisé. Évidemment, les transports étaient complexes, mais néanmoins aucun problème sérieux. Tout s'est très bien passé avec le personnel à Los Angeles et dans le reste du monde. Le soutien a été prodigué à distance. Il y avait d'autres membres du NomCom qui n'ont pas été en mesure d'obtenir leur visa en temps requis pour venir à la réunion, donc ils ont participé à distance, au téléphone. Très bien organisé.

Nous avons eu d'excellentes conversations. Nous avons pris des photos également et à l'extérieur, tout s'est très bien passé véritablement. Je voulais simplement vous l'indiquer. Cela a été une expérience utile et positive. Nous sommes satisfaits, nous sommes contents et contentes. Merci beaucoup de votre attention.

AUGUSTO HO : Merci Vanda.

Et maintenant, Silvia, à moins qu'il y ait quelque chose d'urgent, nous pouvons clore la séance.

SILVIA VIVANCO : Oui. Merci de remplir le questionnaire qui va apparaître sur l'écran.

AUGUSTO HO : Merci beaucoup. Je vous souhaite une excellente soirée.

[FIN DE LA TRANSCRIPTION]