
SAN JUAN – Réunion conjointe : conseil d’administration de l’ICANN et le RSSAC
Jeudi 15 mars 2018 – 10h30 à 11h30 AST
ICANN61 – San Juan, Porto Rico

KAVEH RANJBAR : Nous allons commencer dans deux minutes.

David, est-ce que vous pourriez venir ici à la table s’il vous plaît ?

Bien, nous allons commencer notre réunion. Si on peut afficher à l’écran s’il vous plaît ? Jonne, s’il vous plaît, venez au panel.

Nous allons commencer cette séance. Est-ce que quelqu’un du RSSAC ou du Conseil d'Administration n’est pas encore assis ici au panel ? Si ce n’est pas le cas, venez vous asseoir, s’il vous plaît.

Bonjour à tous. Bienvenue à la séance publique conjointe Conseil d'Administration de l’ICANN-RSSAC. Je vais commencer cette réunion en commençant par une présentation de tous les membres assis ici à la table. On va commencer par George. George s’il vous plaît, pouvez-vous vous présenter ?

GEORGE SADOWSKIY : George Sadowsky.

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

DAVID CONRAD : David Conrad, CTO ICANN.

AVRI DORIA : Avri Doria, Conseil d'Administration de l'ICANN.

RYAN STEPHENSON : Ryan Stephenson, RSSAC, DOD.

JONNE SOININEN : Jonne Soininen, liaison IETF au Conseil d'Administration de l'ICANN.

LITO IBARRA : Lito Ibarra, Conseil d'Administration de l'ICANN.

KAVEH RANJBAR : Kaveh Ranjbar, liaison RSSAC au Conseil d'Administration de l'ICANN.

BRAD VERD : Brad Verd, co-président RSSAC.

TRIPTI SINHA : Tripti Sinha, co-présidente RSSAC.

CHERINE CHALABY : Cherine Chalaby, Conseil d'Administration de l'ICANN.

CHRIS DISSPAIN : Chris Disspain, Conseil d'Administration de l'ICANN.

BECKY BURR : Becky Burr, Conseil d'Administration de l'ICANN.

RAM MOHAM : Ram Mohan, liaison SSAC au Conseil d'Administration de l'ICANN.

[ININTELLIGIBLE] : [Inintelligible], membre RSSAC.

JEFF OSBORN : Jeff Osborn, membre RSSAC.

DANIEL MIGAULT : Daniel Migault, liaison IETF au RSSAC.

GÖRAN MARBY : Göran Marby, ICANN org.

KAVEH RANJBAR : Merci beaucoup.

RUSS MUNDY : Russ Mundy, liaison du SSAC au RSSAC. Excusez-moi, j’arrive rapidement.

BRAD VERD : Plusieurs excuses également de plusieurs membres du RSSAC qui ne sont pas là qui ont dû prendre des vols pour Londres pour la réunion de l’IETF.

KAVEH RANJBAR : Alors laissez-moi vous dire qu’il s’agit d’une réunion informelle, réunion formelle entre le Conseil d'Administration et le RSSAC, mais on préfère que ce soit une discussion informelle. On a une série de questions mais on veut que ces questions nous permettent d’orienter nos discussions. Mais ce qui nous intéresse réellement, c’est d’avoir un dialogue. Alors peut-être que les opinions déclarées seront des opinions personnelles des membres RSSAC. Il ne s’agira pas évidemment de décisions. Les décisions sont toujours envoyées par le RSSAC dans son ensemble au Conseil d'Administration. Mais en tout cas, on veut saisir cette opportunité s’il y a des questions, des commentaires à poser pour utiliser cette séance pour le faire.

Pouvons-nous passer à la diapositive suivante, s'il vous plaît ?

Voici les questions du Conseil d'Administration au RSSAC. Donc il y avait deux questions. On va commencer par la première question.

Quels sont les principaux objectifs du RSSAC pour 2018 ? Je vais laisser le soin au président de répondre.

TRIPTI SINHA :

Merci Kaveh, merci de cette question.

Par rapport à nos principaux objectifs pour 2018, ils sont au nombre de trois. Je vais commencer par le premier.

Comme certains d'entre vous le savez, on travaille depuis près de trois ans maintenant sur certains avis clés au Conseil d'Administration concernant la prochaine phase ou plutôt l'évolution du système du serveur racine. Cela a été mis en œuvre il y a quelques années et depuis, le modèle a été relativement statique. Il n'a pas du tout évolué.

Donc on a consacré beaucoup de temps à approfondir ce modèle et à répondre à des questions qui étaient en suspend depuis de nombreuses années, par exemple mesures de comptabilité, envers qui nous sommes redevables, comment

est-ce que ce système est soutenu, comment continuer à évoluer dans un internet chaque fois croissant.

Donc on a essayé de résumer nos avis en termes de calendrier. On a une version préliminaire. On veut avoir une version proche d'une version finale d'ici mai, lors de l'atelier de travail du RSSAC. Et notre idée, c'est d'harmoniser cette version avec celle du Conseil d'Administration afin de présenter une version finale en juin. Donc à moins d'un problème imprévu, nous allons présenter cet avis lors de la réunion ICANN62.

Deuxième objectif, il y a une révision en cours qui va probablement arriver en avril. À la suite de cette révision, il y aura des recommandations et nous allons présenter ces recommandations au comité pertinent.

Nous avons également un caucus qui se concentre sur les aspects techniques. Et on a trois domaines d'activités en cours.

Donc voilà nos trois principaux objectifs pour l'année 2018.

CHERINE CHALABY :

Merci beaucoup Tripti. Par rapport à l'avis, par rapport au calendrier que vous avez mentionné, vous allez le présenter lors de la conférence 62 de l'ICANN. Est-ce que vous avez dit que vous vouliez le montrer au Conseil d'Administration avant, c'est cela ?

TRIPTI SINHA : Oui. Lors de votre retraite à vous, celle du Conseil, à Vancouver.

KAVEH RANJBAR : Oui, c'est ce qu'on nous avait demandé.

CHERINE CHALABY : Oui. Par rapport à la révision RSSAC, y a-t-il des commentaires sur l'efficacité de la révision jusqu'à présent ? Quel est votre sentiment ?

TRIPTI SINHA : Pour nous, il s'agissait d'une révision organisationnelle qui consistait à voir la dynamique du comité du RSSAC et voir la dynamique générale de ce comité dans l'écosystème en général. Donc il s'agissait, je le répète, d'une révision organisationnelle du RSSAC. Et cela s'inscrit dans la discussion en cours actuellement au sein de l'ICANN entre le rôle du RSSAC et pour répondre aux questions des membres de la communauté qui demandaient à ce qu'un rôle du RSSAC soit mieux défini.

CHERINE CHALABY : La raison pour laquelle je pose cette question, c'est parce qu'on entend beaucoup de groupes de la communauté, unités constitutives de la communauté, s'interroger par rapport à

l'efficacité de ces révisions. Et il y a un dénominateur commun entre toutes ces préoccupations.

D'abord, il faut essayer de faire en sorte qu'il y ait moins de révisions et que ces révisions soient plus efficaces. Par exemple, pour l'année prochaine, il y a neuf révisions prévues. Est-ce que le RSSAC serait en faveur puisque presque tout le monde semble dire la même chose ? Essayons d'avoir une image, un panorama plus général et essayons et faire moins de révisions mais plus efficaces.

TRIPTI SINHA :

Oui, tout à fait d'accord. On aimerait apporter notre contribution, effectivement, et prendre un petit peu de recul pour voir l'efficacité des révisions, quel est l'objectif et le résultat escompté de chaque révision. Et pour ce faire, il faut fournir plus de sauvegardes ou de lignes directrices par rapport à la manière dont ces révisions sont entreprises, par rapport à la portée - qui doit être clairement définie - des révisions, également les rapports doivent être instructifs et constructifs.

CHERINE CHALABY :

Oui. Par rapport aux révision, votre idée, c'est d'envoyer un rapport de documentation ou de consultation, plutôt ? Quelle est votre idée ?

GÖRAN MARBY :

Il y a deux choses en fait qu'il faut aborder ici. D'abord, ce qui est prévu dans les statuts constitutifs ; donc cela, c'est une discussion. Et ce genre de révisions, je le disais, sont prévues dans les statuts constitutifs. Sinon, il faut modifier les statuts constitutifs.

Et autre aspect qui me paraît très important et qui a été soulevé non seulement par vous mais par les autres aussi, à savoir définir les objectifs clairement des révisions. Qu'attend-on de ces révisions ? Et je sais que ces discussions commencent à poindre aussi.

Moi, personnellement, je n'ai pas de plan à ce niveau-là, encore. Or, je devrais l'avoir parce que cela a été soulevé à maintes reprises cette semaine. Et on investit beaucoup d'argent et de temps dans les révisions elles-mêmes et certaines révisions se sont prolongées pendant de nombreuses années. Je crois qu'à l'At-Large, il y a une révision qui a pris quatre ans. Et cela, c'est une autre discussion.

Donc sur ce point en particulier, je dois dire cela et me tourner vers l'OEC et parler avec le président et avoir une discussion.

BRAD VERD : J'allais dire que le RSSAC est en train de préparer deux réponses: une réponse à l'examineur indépendant dans l'espoir de pouvoir partager notre sentiment sur le retour d'informations et par rapport au fait que nous espérons que les recommandations soient instructives et constructives comme vous le disiez et ensuite, préparer des commentaires et notre opinion sur l'ensemble du processus qu'on aimerait partager avec l'OEC.

KHALED KOUBAA : J'aimerais partager avec vous le fait que l'OEC a eu une discussion informelle ce matin à 7:30 avec tous les membres de notre groupe. Et nous remercions le volume très significatif de commentaires que nous avons reçus de la part de la communauté. Nous apprécions également les commentaires qui ont été faits. On va s'assurer que différentes actions sont mises en œuvre. Comme Göran l'a dit, il y aura des mesures, des actions à court terme, moyen terme et long terme.

En tant qu'OEC, nous ne sommes pas appelés à prendre quelque décision que ce soit pour l'heure puisque pour l'instant, il faut digérer tous les commentaires et les contributions qu'on a eus de la part de la communauté. Il faut classer et analyser tous ces commentaires afin de voir s'ils sont étayés et afin qu'ils puissent éventuellement découler sur des décisions informées. Mais

étant donné le fait que c'est une question très sensible, il faut absolument procéder de cette manière. Et effectivement, il est impératif de se poser la question « Quel est l'impact de cette révision sur l'organisation ? » Mais cela, c'est une question à long terme.

KAVEH RANJBAR : Merci beaucoup.

Cherine ?

CHERINE CHALABY : Alors si nous avons un moment, j'aimerais parler de l'avis sur l'évolution du système de serveurs racine. Est-ce que je peux le faire maintenant ?

KAVEH RANJBAR : Oui.

CHERINE CHALABY : Moi, la question qui me vient à l'esprit, c'est celle des coûts. Je ne sais pas si vous serez en position de fournir des indications quant au coûts pour accompagner votre avis ou est-ce qu'on peut le travailler ensemble. Parce que ce qui se passe à l'heure actuelle - et on l'a vu dans pratiquement toutes les unités constitutives - par exemple ce matin, nous avons une réunion

avec le SSAC qui nous a dit que le volume de travail auquel ils sont confrontés a des implications en termes de coûts. Et il en va de même dans l'autre sens. Tout ce qu'on nous demande de mettre en œuvre, cela a des implications en termes de coûts. Et cela, c'est une question cruciale. Est-ce que vous, vous allez pouvoir nous donner une indication sur les coûts ou est-ce qu'il faut qu'on le travaille ensemble ?

TRIPTI SINHA :

Je pense qu'il y a trois questions là-dessus. D'abord le coût qui consiste à réunir les avis ensemble avec le comité consultatif. Et quand je vois le volume de temps et d'engagement que cela a représenté pendant trois ans d'investir là-dedans et cela n'a pas été associé avec un coût, donc si on veut l'appliquer, il va y avoir un coût de mise en œuvre, simplement de mise en œuvre.

Ensuite, il y a un autre coût. C'est le coût du modèle une fois qu'on a un modèle opérationnel en place, pour qu'il puisse fonctionner dans l'infrastructure et le service actuel, quelque soit ce modèle ou le modèle que nous allons adopter. Cela aussi va représenter un coût pour les parties prenantes. Donc il s'agit de trois coûts différents.

Maintenant, est-ce qu'on va inclure des chiffres dans notre avis ? Pas dans la version actuelle, ce n'était pas notre objectif parce que nous pensions que nous allons procéder de la manière

suivante : nous allons présenter l'avis, le présenter au Conseil d'Administration pour qu'ils l'examinent puis voir qu'elles étaient les implications financières ; donc procéder par étapes, examiner en profondeur cet avis et voir ensuite si c'était viable ou pas. Bien entendu, il y a le coût de mise en œuvre et le coût du modèle en soi.

BRAD VED :

Oui, je pense que le processus de feedback dont Tripti vient de parler concerne la communauté mais aussi le Conseil d'Administration.

CHERINE CHALABY :

Oui, donc cela affecte le système de serveurs racine et par défaut, les opérateurs de serveur racine. Est-ce qu'il y a un avis consensuel par rapport à l'accord qu'on a avec les opérateurs de serveur racine ?

TRIPTI SINHA :

Non, il y aura consensus au RSSAC et on a dit très clairement que tous les RSO ont des obligations qui sont contenues vis-à-vis de leur entreprise ou de leur filiale. Donc il y aura très certainement un consensus là-dessus, à savoir lorsque cela sera mis en place, nous pensons qu'il y aura quelque chose de bien plus vaste et ce sera un processus qui devra être mis en place par la

communauté parce qu'ensuite, il y a beaucoup de choses qui échappent, finalement, à notre domaine d'activités et de compétences.

KAVEH RANJBAR :

Y a-t-il d'autres questions, demandes d'intervention sur ce point ? Si ce n'est pas le cas, je voudrais dire que Maarten, Lousewies, Lito, Ron, Sarah, Matthew. Khaled et León sont ici dans la salle.

Deuxième question du Conseil d'Administration au RSSAC. Quels sont les principaux objectifs à long terme du RSSAC ? Parce que le Conseil d'Administration travaille sur le prochain plan stratégique quinquennal. Et donc pourquoi est-ce que le Conseil d'Administration pose cette question ? C'est pour connaître l'opinion du RSSAC comme contribution à ce plan stratégique. Donc c'est une question très importante, je sais que cette discussion va se poursuivre au Panama. Mais pour l'heure, est-ce que les membres du RSSAC ont des commentaires à faire là-dessus ?

BRAD VERD :

Oui, je pense que notre principal objectif à long terme sera la mise en œuvre de l'avis que nous allons fournir lors de la réunion ICANN62. Là, on va attendre la réaction du Conseil

d'Administration et ensuite, l'effort que cela avait impliqué pour la communauté.

KAVEH RANJBAR : Oui, c'était justement l'un des principaux commentaires d'ouverture de Cherine.

Pouvons-nous passer à la diapositive suivante s'il vous plaît ?

Donc vous voyez les questions à l'écran du RSSAC au Conseil d'Administration. D'abord, quelles sont les principales préoccupations du Conseil d'Administration par rapport au service de la racine ? Quelles sont les pressions que le Conseil d'Administration perçoit par rapport au service racine ?

RAM MOHAM : La principale préoccupation du Conseil d'Administration par rapport au système du serveur racine, c'est les menaces d'attaques DDoS qui menacent l'ensemble du système. Et d'ailleurs, ce n'est pas une menace qui concerne uniquement le système de serveur racine ; tous les services sur internet sont menacés.

Le Conseil d'Administration a parlé des différentes options à disposition de la communauté pour atténuer cette menace. Malheureusement, il y a très peu d'actions que la communauté

peut entreprendre, que l'organisation ICANN peut entreprendre afin d'avoir un effet immédiat sur ces menaces.

La principale mesure d'atténuation à court terme semble être une capacité du serveur racine supplémentaire. Est-ce que les opérateurs de serveur racine ont l'intention d'étendre les capacités? Et est-ce qu'ils ont les ressources en termes de finances, de ressource humaines, etc. pour le faire? Voilà un petit peu la question que le Conseil d'Administration a évoquée en interne.

Également, le Conseil d'Administration s'intéresse à la responsabilité générale des opérateurs de serveur racine qui doit être améliorée. Le Conseil d'Administration voit qu'il y a une demande non-technique pour des opérateurs de serveur racine supplémentaires. Le Conseil d'Administration sait que l'ICANN doit prendre toutes les actions raisonnables afin d'atténuer les menaces DDoS et reconnaît également la volonté de la communauté de mettre en place une responsabilité plus grande de la part de opérateurs.

KAVEH RANJBAR :

Merci beaucoup. Lors de la séance publique avec le bureau de la technologie, nous avons présenté ce qui avait été proposé par OCTO sur l'atténuation, ce qui ressortait de l'organisation ICANN

pour l'atténuation de ces problèmes. Donc nous avons discuté de tout ceci.

L'étape suivante, c'est donc cette proposition du bureau technologie qui a été soumise à la communauté technique. Et donc la prochaine fois que nous nous réunirons, donc la semaine prochaine, au sein de la communauté technique dans le cadre d'une liste de diffusion, nous allons donc aller de l'avant, nous allons contacter le RSSAC – le RSSAC fait partie de la discussion – donc la discussion se poursuit.

Entre temps, je crois que le RSSAC a déjà exprimé son intérêt par rapport à cela. Nous en avons déjà parlé, il y a différentes possibilités. Certains ont exprimé des préoccupations, d'autres ont appuyé la décision.

BRAD VERD :

Alors il y a plusieurs questions là-dessus. Donc le DDoS, c'est la dernière chose à mon avis, ce sera là-dessus que le dialogue sera le plus fourni

En ce qui concerne la responsabilité, la question sur la responsabilité du Conseil et de la communauté, comme nous l'avons dit, nous y travaillons. Nous pensons que cette question recevra une réponse dans l'avis qui sera fourni au Conseil. Donc la seule chose que j'ai à vous répondre là-dessus, c'est attendez

de voir. Désolé de vous répondre comme cela, mais nous en sommes conscients. Nous avons passé pas mal de temps là-dessus mais nous devons nous assurer de bien considérer tous les obstacles possibles de manière à ce que le modèle que nous proposons traitera de tous ces problèmes. Donc cela prend un petit peu de temps

Du point de vue des demandes non-techniques, ce n'est pas quelque chose qui fera partie du travail d'évolution mais nous vous fournirons les outils pour que le Conseil puisse mettre ceci en œuvre. Donc c'est aussi un enjeu politique et donc il y a un comité technique. Donc les choses ne sont pas forcément très claires.

En termes de capacités pour les serveurs racine, ce que je dois mentionner, c'est la croissance de la plateforme actuelle, qui est au service de la racine. Il n'y a pas longtemps, je crois que c'était il y a un an ou un peu plus, on se disait six instances et maintenant, on en a 950 dans le monde, donc on est passé de 600 à 950. Donc la croissance se poursuit, elle est continue. Et comme vous l'avez dit, la première ligne de défense pour le risque DDoS, c'est justement de s'occuper du risque DDoS.

En ce qui concerne la racine L, c'est une discussion qui existe entre le RSSAC et le Conseil d'Administration. C'est exactement ce qui se passe au niveau des opérateurs de serveur racine. Donc

on peut appliquer cela aux lettres aujourd’hui. Tout est fait au niveau des opérateurs.

En ce qui concerne le DDoS, encore une fois, les menaces existent, ce n’est pas une menace nouvelle au système de serveur racine, c’est une menace qui existe depuis longtemps. Le RSSAC s’en inquiète, les opérateurs de serveur s’en inquiètent, ce qui est évident étant donné les investissements pour élargir la plateforme. Comme vous l’avez dit, ce n’est pas une menace spécifique. N’importe quelle personne qui est sur internet, en fait, court un risque.

Dans notre discussion avec le bureau technologie, nous avons parlé justement de l’argument comme quoi la racine est en danger, est menacée comme n’importe quelle autre plateforme. Il y a certainement des TLD qui courent le même risque et qui pourraient avoir un impact supérieur dans un délai plus court, donc nous avons énormément discuté de cette question. Voilà.

Ceci étant, je crois que j’ai répondu à toutes les questions que vous avez soulevées, sinon, dites-le moi.

CHERINE CHALABY :

Alors la question qui a été posée entraîne une autre question. Pourquoi maintenant ? Alors je vais vous demander de m’aider à y répondre.

Notre mission a toujours été la sécurité, la stabilité de l'internet, du système d'identificateur. Le système de serveurs racine, depuis toujours, a été très stable, depuis l'existence, depuis la création de l'ICANN. Donc nous nous devons d'expliquer pourquoi tout d'un coup, nous soulevons cette question au RSSAC puisque le système est stable.

Donc c'est vrai, notre mission nous demande de nous assurer – nous n'avons pas d'autorité directe sur les opérateurs de serveur racine - mais notre mission nous demande.

Alors pourquoi est-ce que cette question est devenue importante ? Alors je vais vous expliquer un petit peu, si vous me le permettez, les changements que nous voyons du point de vue de la technologie qui font que cette question est pertinente.

RAM MOHAN :

Merci Cherine. La discussion au Conseil est déjà de reconnaître que le DDoS n'est pas une menace nouvelle. Mais ce qui a accru l'attention du Conseil portée sur cette question, c'est le fait que les attaques prennent une ampleur supérieure de nos jours. Et en grande partie, le nombre de ces attaques est de plus en plus important. Et donc il faut reconnaître que ce n'est pas uniquement au niveau du système de serveurs racine.

Il y a un autre élément à prendre en considération, c'est donc la prolifération de dispositifs qui, constamment, sont connectés à l'internet. Et donc à leur état natif, ils ont des vulnérabilités, ils peuvent être entraînés dans un réseau zombie de manière beaucoup plus directe ou plus facilement. Et donc tous les systèmes source ouverte font que tout est connecté, tout est sur un système de chaîne et cela veut dire que les attaques sont beaucoup plus efficaces. Donc ce n'est pas la question du DDoS mais c'est la question du nombre d'attaques et de l'ampleur de ces attaques et le fait que cette évolution est plus rapide que l'évolution des réponses, des réactions. Et donc il nous faut absolument avoir un système plus solide pour répondre à toutes ces préoccupations.

KAVEH RANJBAR :

Je vois que nous avons six opérateurs qui sont représentés ici sur les 12. Donc la question que je pose à nous tous, opérateurs, est-ce que cela nous empêche de dormir ? Du point de vue technique, nous comprenons tous l'ampleur, la possibilité, ces menaces au système de serveurs racine. Mais est-ce que vraiment vous vous préoccupez très souvent de cette question ? Est-ce qu'elle vous empêche de dormir ?

JEFF OSBORN :

Jeff Osborn avec ISC. Nous opérons la racine F. Un des atouts du système de serveurs, c'est la diversité des méthodes et donc nos différentes organisations qui ont différentes approches, et donc en fait ces différentes approches représentent un atout.

Pour moi, c'est quelque chose qui existe depuis longtemps dans l'internet. Nous sommes là depuis vraiment longtemps, nos employés, si on ajoute toute notre expérience, on est à des centaines d'années d'expérience. Donc vraiment, notre organisation est solide.

Au cours de l'année et six mois passés, nous avons augmenté notre capacité de bande passante en mettant à niveau tout le matériel qui existait dans un partenariat avec Cloudflare qui permet vraiment d'augmenter la bande passante. J'étais à Katmandou la semaine dernière et ils sont vraiment partout.

Donc le volume de données qui nous fait peur, ce n'est pas vraiment un problème pour Cloudflare, cela ne leur fait pas peur. Donc toutes ces préoccupations, en fait, on est partie de cela mais maintenant, ce n'est pas vraiment un problème.

Dans le rapport du bureau technologie, apparemment, l'ICANN ne choisit pas en tant qu'opérateur de racine de procéder de la même manière et c'est très bien ; c'est bien qu'il y ait une divergence d'opinion. C'est positif.

Maintenant, je vous propose une idée un peu folle. Nous avons eu l'idée d'avoir 10 000 petits dispositifs Cloudflare dans le monde entier pour avoir des [catchments] tellement petites que les DDoS ne peut jamais en fait prendre de l'ampleur, vraiment créer une immense tempête dans tout le système pour éviter en fait que la menace se répande dans le monde entier. Parce que l'idée du DDoS, c'est justement cela, que tout soit rassemblé à partir d'une attaque et se dissémine partout.

Donc personnellement, je dors très bien, je pense que les choses avancent de manière positive. Et également, je crois que par définition, il faut être humble et reconnaître que les attaques peuvent se produire. Il ne faut pas non plus prendre trop de fierté par rapport à cela.

LARS-JOHAN LIMAN :

Lars Liman de Netnod.

J'aimerais ajouter un point là-dessus. Il y a d'autres mécanismes de défense qui sont en phase de déploiement du point de vue des filtres, du point de vue des liens entre les opérateurs de serveur racine et les différents fournisseurs de services qui, en fait, amènent les attaques, qui sont les porteurs de ces attaques.

Il y a tout un réseau de personnes dans notre organisation qui ont vraiment l'intention que tout continue de fonctionner de

manière adéquate. Et cela, c'est une réelle ressource. Nous ne sommes pas seuls. Il y a tout un internet qui est là pour nous aider et qui souhaite nous aider.

KAVEH RANJBAR : Merci beaucoup.

Ram.

RAM MOHAN : Merci. J'aimerais revenir à une chose qui a été dite par rapport au rapport du bureau technologie et qui parlait de l'expansion de la racine L avec des groupements et des instances uniques. Donc ce type d'expansion, cela peut s'appliquer à toutes les autres lettres à mon avis.

Au sein du Conseil, les choses ne sont pas nécessairement claires. Il n'est pas très clair de savoir s'il y a autant d'investissements en matière de développement des capacités. Cela ne veut pas dire qu'on n'est pas conscients ou sensibilisés.

Mais l'autre préoccupation que nous avons, c'est qu'on peut passer de 1,7 téraoctet à 5,7 téraoctets pour les attaques. C'est le souci. Mais est-ce qu'il y a une planification appropriée ? Est-ce qu'il y a une gestion des risques appropriée ? Quels sont les mécanismes d'atténuation qui existent ? J'ai ceux à qui on fait

confiance pour l'opération des systèmes de serveurs racine. Donc c'est justement ce type de dialogue, ce type d'informations dont le Conseil a besoin. Cela permettrait en fait de minimiser notre niveau de préoccupation.

Alors autre chose qui pourrait être utile en matière de responsabilité, c'est d'avoir à haut niveau un rapport, un rapport sur le niveau d'investissement sur l'élargissement des capacités. Je pense qu'un niveau peut-être uniforme, c'est quelque chose qui pourrait être mis à disposition de la communauté, parce que ce n'est pas uniquement le Conseil qui se pose cette question, c'est aussi la communauté.

KAVEH RANJBAR :

David, vous voulez prendre la parole par rapport à cela ou est-ce que c'est autre chose ?

Donc on va simplement vous demander de continuer sur cette question.

BRAD VERD :

Quelques petits points là-dessus. Donc je comprends bien que nous sommes en train de nous poser des questions opérationnelles. Nous avons déjà mentionné le fait qu'il n'y a pas de responsabilité opérationnelle en dehors de la racine L. Donc le travail sur l'évolution que nous effectuons a pour

objectif de parler de la gouvernance et de la responsabilité opérationnelle.

Alors je sais qu'on parle de l'avenir. Il y a un risque qui force ces questions opérationnelles. Donc nous comprenons qu'il y a un besoin immédiat et qu'il y a également l'avenir, ce que l'on peut faire ou délivrer à l'avenir. Donc voilà, je voulais clarifier un petit peu.

Pour être très honnête, en tant qu'opérateur mais en tant que non membre du RSSAC, je ne sais pas quel est mon point de vue par rapport à cela ; je ne sais pas ce que dirait mon organisation par rapport à un grand rapport qui explique les capacités, les investissements parce que ce qui n'est pas souhaitable, c'est de fournir une feuille de route pour les mauvais acteurs. Donc il faut bien garder ceci présent à l'esprit parce que ce n'est pas une bonne idée de publier certaines informations.

Du point de vue opérationnel, pas du point de vue des politiques, cela représenterait un risque et il faut le prendre en compte. Le Conseil doit y penser, la communauté doit y penser lorsque ces questions sont posées. C'est cela le problème, en fait.

RAM MOHAN :

Oui. Il faut savoir que le Conseil d'Administration est d'accord là-dessus. Nous sommes tous d'accord. De toute évidence, on ne va pas fournir de feuille de route aux acteurs malveillants pour leur expliquer comment effectuer leurs attaques.

Mais notre collaboration, à mon avis, doit inclure une des discussions que nous avons eues lors d'un atelier du Conseil. Imaginons qu'il y a une attaque, une grosse attaque, la racine ne fonctionne plus correctement. Qui va être présent au comité pour répondre aux questions et quelle sera la question ? La question, ce sera « Est-ce que vous étiez au courant qu'il pouvait y avoir une menace ? Est-ce que vous saviez que cette menace avait le potentiel d'être énorme ? Et est-ce que vous saviez qu'une partie de la racine pourrait être défaillante ? »

Donc ce que nous essayons de faire, c'est de collaborer pour en arriver à décrire la situation, tout en gardant à l'esprit que de l'autre côté, il faut faire attention pour ne pas exposer tout votre travail. Votre travail est excellent, c'est un travail important ; on ne va pas le publier. Mais en même temps, du point de vue du Conseil, nous avons besoin d'une certaine visibilité, d'un certain niveau de confiance. Nous devons savoir qu'effectivement, vous faites le travail. Ce n'est pas simplement de vous entendre dire : « Oui, oui, ne vous inquiétez pas, nous nous en occupons. » C'est cela.

Je suis très honnête, là, avec vous. C'est en fait cela, la nature de la question du Conseil d'Administration.

KAVEH RANJBAR : Merci. Y a-t-il une réponse par rapport à cela ?

TRIPTI SINHA : Ram, j'aimerais vous répondre sur deux points.

Nous comprenons tout à fait que vous avez besoin d'une petite explication. Nous respectons votre point de vue, nous le comprenons. Alors que ce soit une attaque nucléaire, que ce soit une attaque dans le cyberspace, etc., tout ceci, nous en sommes conscients, ne l'oublions pas, et nous améliorons nos opérations dans la mesure du possible.

Alors je comprends bien que nous devons vous fournir un rapport qui rassemble tout ce que nous faisons, voilà ce que nous faisons au niveau des opérateurs de serveur. Bien sûr que nous ne souhaitons pas nécessairement exposer tout le travail, tout le détail mais au moins, vous fournir quelque chose qui vous rassure. Et cela, c'est quelque chose dont nous sommes conscients et ce n'est pas uniquement le système de serveurs racine mais c'est aussi pour n'importe quelle menace.

C'est justement la raison pour laquelle nous travaillons sur cet avis. Parce que nous comprenons bien que nous avons besoin d'être responsables. Qui sont nos parties prenantes ? Nous sommes là depuis le début et un moment viendra où nous ne serons plus là. Donc il nous faut absolument créer ce nouveau modèle. Nous le comprenons.

Mais en parallèle, nous continuons de renforcer nos services. Nous le faisons différemment. Nous sommes un groupe très diversifié. Voilà.

Je ne sais pas si cela répond à votre question.

KAVEH RANJBAR :

J'avais demandé la permission à David de continuer cette discussion avant de passer à son commentaire. Alors on va peut-être passer quelques minutes de plus sur ce sujet.

RAM MOHAN :

Je crois qu'on ne peut pas nécessairement résoudre la question maintenant mais au moins, le dialogue est lancé. Et je parle en mon propre nom, je ne parle pas au nom du Conseil mais ce dont nous avons besoin, c'est un mécanisme qui nous permette de poursuivre le dialogue de manière continue, de manière à ce que le dialogue ne soit pas limité aux sessions mais vraiment, il faudrait pouvoir le poursuivre parce que vous l'avez dit, ces

menaces, nous en sommes conscients et il y a en d'autres types de menaces. Mais nous avons besoin d'un mécanisme qui nous permette de poursuivre cette boucle, ce dialogue. Nous n'en sommes pas encore là, mais c'est vraiment quelque chose qui m'intéresse. J'aimerais trouver un moyen de dialoguer à l'avenir parce que pouvoir prendre le temps avec nous de vous poser des questions, écouter ce qui vous inquiète. C'est savoir à la fois le problème opérationnel mais aussi de savoir quelle est votre réponse ; êtes-vous crédible et est-ce que vous pouvez nous le prouver ? Cela, c'est quelque chose que nous pouvons faire si nous avons un dialogue continu.

BRAD VERD :

Pour répondre brièvement à votre commentaire sur le fait qu'on en est à 1,7 pour l'instant. On pourrait en arriver à 5,7 téraoctet plus tard. Et bon, on n'en est pas à une attaque de 1,1 pour l'instant. Donc cela, c'est un petit peu ce qui se passe entre les bons et les méchants. Il y en a un qui avance, l'autre recule, prend une mesure, etc. Donc les vecteurs d'attaque changent sans arrêt et il faut essayer d'être de plus en plus créatifs pour affronter les méchants.

KAVEH RANJBAR :

Y a-t-il d'autres demandes d'intervention ?

RAM MOHAN : Oui, je vois que Lito est là. Lito et moi-même sommes co-présidents du comité de risques au Conseil d'Administration.

Là, ce qu'il faut adopter, c'est une approche d'évaluation de risques. Il ne s'agit pas de connaître toutes les solutions qui existent mais il s'agit de comprendre que les risques ainsi que l'atténuation des risques ont été analysés. Et il est réconfortant de savoir que ces mesures d'atténuation ont des chances assez raisonnables de réussite.

DAVID CONRAD : Oui, je voulais préciser un point. Le rapport fourni par le bureau technologie au Conseil d'Administration avait pour but de montrer les différentes options qui s'offraient à l'organisation par rapport au contexte des opérations sur la racine L et aux options liées à la protection du serveur racine. L'objectif, ce n'était pas d'indiquer une décision déjà prise ou de privilégier telle ou telle approche, plutôt de faire des suggestions par rapport à l'opinion de notre bureau technologie par rapport à une approche rationnelle qui pourrait être adoptée. Ce document, donc, n'implique pas un volume conséquent de dépenses en termes de ressources.

KAVEH RANJBAR : Merci beaucoup.

Passons-nous au point suivant, sauf s'il y a des questions ou commentaires ? Non ?

Donc deuxième question du RSSAC au Conseil d'Administration. Quelle est la perspective du Conseil d'Administration sur le plan prévu de roulement de la KSK ? Alors peut-être que je vais me tourner vers David pour répondre à cette question. David ?

DAVID CONRAD :

La situation actuelle est la suivante. Nous avons des données qui semblent indiquer que lorsque nous appliquons le roulement de la KSK, il y a un certain pourcentage de résolveurs qui vont être mal configurés et qui ne vont pas réussir à faire la résolution s'il y a validation du DNSSEC. Mais ces données ne sont pas très utiles en fait parce que la conception originale du roulement de la KSK se concentrait sur les utilisateurs qui étaient affectés, ce qui implique que seuls 0,5 % des utilisateurs seraient affectés de manière négative par le roulement de la KSK.

Donc à l'heure actuelle, on en est à une période où on essaie d'obtenir des commentaires supplémentaires sur un plan proposé pour avancer vers le roulement de la KSK pour le 11 octobre 2018, quelque soit les données que nous recevions de la

part de ce qu'on connaît comme le rapport 8145 de la part des résolveurs.

Le problème, c'est de savoir quel est le point de vue du RSSAC sur ce plan proposé et ce que proposerait le RSSAC pour atténuer tout risque ou préoccupation associé au roulement de la KSK.

KAVEH RANJBAR :

Oui, je vais répéter ce qui a été dit aussi lors de la réunion avec le bureau technologie. Lorsque ce calendrier a été présenté, il est fort probable qu'on ait une résolution de la part du Conseil d'Administration qui va demander un avis au RSSAC. Mais c'est parce qu'il y a un certain nombre de mesures ou d'étapes qui doivent être franchies avant que le Conseil d'Administration prenne cette mesure. Donc veuillez garder présent cela à l'esprit. Merci beaucoup.

Dernière question. La question était posée et entre temps, il y a eu une évolution. Je vais demander à Brad de développer.

BRAD VERD :

Oui. Je crois que cette question, finalement, n'est plus vraiment d'actualité. Elle est liée à la question de la GNSO, qui attendait une réponse des différentes AC par rapport à l'ajout de 25 000 noms à l'espace de noms.

Et le RSSAC a répondu et cette réponse a été posée au Conseil d'Administration bien avant que ces transactions aient lieu. Donc je ne suis pas sûr quel est le sentiment du Conseil d'Administration, mais je pense que cette question n'est plus d'actualité.

KAVEH RANJBAR :

Merci beaucoup, Brad. Y a-t-il d'autres commentaires sur ce sujet ?

Si ce n'est pas le cas, est-ce qu'il y a d'autres commentaires, observations que les membres du RSSAC ou du Conseil d'Administration souhaiteraient aborder ? D'ailleurs, puisque nous sommes un petit peu en avance, est-ce que dans la salle il y a des questions à l'attention des membres du RSSAC ou du Conseil d'Administration ?

Si ce n'est pas le cas, nous allons lever cette séance. Merci à tous de votre participation.

[FIN DE LA TRANSCRIPTION]