ICANN84 | Réunion générale annuelle – Réunion conjointe : GAC et SSAC
Mardi 28 octobre 2025 – 15h00 à 16h00 IST

NICOLAS CABALLERO Mesdames et messieurs, veuillez prendre place. Nous allons commencer dans une minute.

GULTEN TEPE Bienvenue à cette séance du GAC avec le SSAC, ce mardi 28 octobre à 15 h UTC. Veuillez noter que cette session est enregistrée et qu'elle est régie par les normes de comportement attendues de l'ICANN, par le code de conduite, de participation de la communauté de l'ICANN et par la politique anti harcèlement de la communauté de l'ICANN. Les questions ou les commentaires pendant cette séance seront lus à haute voix, uniquement s'ils sont présentés suivant le format approprié et soumis dans le chat de Zoom.

L'interprétation de cette séance se fera dans les six langues de l'ONU plus portugais. Si vous souhaitez parler, levez la main sur Zoom. Souvenez vous d'indiquer votre nom pour les enregistrements et la langue dans laquelle vous allez parler si ce n'est pas l'anglais, parlez clairement et à un rythme raisonnable pour permettre une interprétation précise de vos propos. Je vais maintenant passer la parole au président du GAC, Nico Caballero.

NICOLAS CABALLERO

Merci Gulten. Bienvenue à tous. J'espère que vous avez profité du bon café irlandais. J'ai le plaisir de vous présenter un cher ami Ram Mohan et son équipe du SSAC. Nous avons Suzanne, Maarten et Tara. Bienvenue! Nous allons avoir une séance très intéressante à mes yeux divisée en quatre parties.

La première partie est la plus importante à mes yeux, toujours. C'est l'importance des FOSS, des logiciels à code source ouvert et libre dans l'industrie du DNS et ailleurs, mais c'est une autre discussion. Ensuite, les collisions de noms et leur incidence sur la stabilité du DNS, l'utilisation malveillante du DNS et la possibilité de coopération entre le SSAC et le GAC. Ensuite, je vais ouvrir la parole à… ouvrir le micro pour une discussion.

Encore une fois bienvenue. Je vais passer la parole à mon cher ami Ram Mohan.

RAM MOHAN

Merci Nico. C'est un plaisir d'être ici avec vous à Dublin, mais aussi ici dans cette salle du CAC. Nous nous sentons honorés d'être encore invités à parler avec vous. Nous savons que votre emploi du temps est toujours très chargé. Nous apprécions ces échanges avec vous et nous nous y préparons intensément, parce que nous savons que ces interactions que nous avons avec vous sont importantes au niveau de l'ICANN, mais aussi au niveau de leur

propre gouvernement, de ce que vous pouvez communiquer avec vos propres gouvernements.

Donc, sans plus attendre, j'aimerais attaquer la première partie de notre ordre du jour, l'importance du logiciel libre et à code ouvert dans l'industrie du DNS. Et, pour présenter ce sujet et partager des détails avec vous, je vais passer la parole à mon collègue Maarten Aertsen, qui est l'un des coprésidents du groupe de travail qui se penche sur cette question.

MAARTEN AERTSEN Merci Ram, merci Nico. Donc, aujourd'hui, je vais vous parler de logiciel. Le SSAC écrit habituellement des documents techniques. Ce document n'en fait pas partie. La communauté de l'ICANN n'est pas toujours le public primaire du SSAC. Ce document est adressé aux décideurs politiques, et je crois que je me trouve au bon endroit, vous et vos collègues qui s'occupent de la cybersécurité.

Alors, parlons logiciel. Si on résume notre rapport en une seule phrase, nous trouvons que le DNS est construit sur des logiciels libres et à code source ouvert. Ce n'est pas un plaidoyer. On n'est pas en train de dire que le logiciel libre et à code source ouvert est meilleur que les autres. On parle d'une réalité, C'est la manière dont fonctionne le DNS.

Alors, FOSS veut dire logiciel libre et à code source ouvert. Libre fait référence à liberté comme la liberté d'expression et non pas à la gratuité. Le fait que ce soit gratuit. FOSS est défini par quatre

libertés. Liberté d'utilisation. On peut utiliser les logiciels à toute fin. Étude, on peut étudier comment ce logiciel fonctionne, y compris son code source. Partage, On distribue des copies de ce logiciel et finalement changement, on peut modifier ce logiciel pour qu'il réponde à vos besoins.

Donc, ces libertés qui font partie d'une licence logicielle, créent un écosystème complètement différent pour les développeurs de logiciels, mais aussi pour la maintenance de ces logiciels comparé aux logiciels propriétaires. Il y a des différences philosophiques entre ce qu'est un logiciel libre et un logiciel à code source ouvert. Notre phrase concentre ces deux concepts. Diapo suivante s'il vous plaît.

Donc, le modèle FOSS a un profil de risque différent de celui des logiciels propriétaires. Comme pour la plupart des logiciels libres et à code source ouvert, ils sont maintenus par des bénévoles et donc la motivation joue un rôle fondamental. Si les personnes qui travaillent dans ces logiciels à titre bénévole sont démotivés, ils peuvent avoir des burn out et cela peut les amener à abandonner les projets.

Donc, ensuite, pour ce modèle FOSS, il n'y a pas une garantie par défaut. Si bien que les opérateurs doivent assumer la responsabilité et développer cette expertise en interne pour pouvoir réparer le logiciel, s'il a des défaillances, ou bien ils peuvent acquérir des garanties par rapport à ces logiciels.

Ensuite, en général, il y a bien sûr des organisations à but non lucratif qui s'occupent de cette maintenance et à ce moment là, on a la situation des passagers clandestins, des gens qui profitent de ce fait que ce logiciel soit gratuit. Donc, ces initiatives font partie d'organisations petites qui sont sensible à des réglementations trop exigeantes qui peuvent avoir des conséquences sur leur financement.

Ces risques sont réels et sont inhérents au modèle, FOSS. Ensuite, la réglementation, qui ne prend pas en considération ce type de risque peut rendre les choses pires.

Il y a également des avantages, bien entendu. Et, ici on voit le DNS en particulier, contrairement à la diapo précédente qui se penchait sur le FOSS en général. Pour ce qui est du DNS, on voit qu'il y a un avantage concernant donc la transparence et le travail collaboratif en matière de sécurité. Il y a une surveillance continue de la communauté universitaire par rapport à ces logiciels. Vous pouvez trouver des documents des années 90 qui se penchent sur des défaillances de certains logiciels et comment les résoudre. Donc tous ces problèmes sont discutés et résolus.

Ensuite, nous avons mené des recherches auprès de plus de 100 opérateurs qui utilisent les logiciels, et ils apprécient la possibilité de réparer rapidement tout type de défaillance. Il peut y avoir une proactivité accrue.

Dans le DNS en particulier, il y a un certain nombre de projets DNS populaires qui ne sont pas maintenus par des bénévoles, mais par

des organisations qui existent depuis longtemps. Et ces organisations font la maintenance et la mise en œuvre de ce type de logiciel depuis de longues années, et cette longévité leur permet de renforcer la confiance en ces logiciels.

Ensuite, un autre avantage, c'est qu'il y a une résilience opérationnelle grâce à la diversité, car il y a plusieurs mises en œuvre de ces logiciels FOSS. Cela réduit la possibilité qu'il y ait un point unique de défaillance, et cela réduit les barrières à l'accès et évite une dépendance vis à vis d'un seul constructeur. Et, donc, cette dépendance par rapport… ou par exemple, des dépendances par rapport à des entités étrangères. Diapo suivante.

Parlons sécurité. Le SSAC se focalise sur la sécurité. Il est très important de comprendre quelle est cette sécurité par rapport à FOSS. Et donc, la sécurité n'est pas déterminée par le fait que le code source soit ouvert ou pas. Ce qui détermine la sécurité, ce n'est pas non plus le fait de savoir si les développeurs sont payés ou pas, ou s'il s'agit d'un logiciel commercial ou non.

Ce qui détermine la sécurité d'un logiciel, c'est le processus de développement. Une maintenance à long terme. La qualité du processus de développement.

Et, comme le dit le rapport, la sécurité de tout projet de logiciel est déterminée par la qualité de son développement et de son processus de maintenance.

Donc, ici, on nous pose toujours la question est-ce que FOSS est plus sûr ou moins sûr que les logiciels propriétaires? Et, la réponse est ni l'un ni l'autre. Parce que la sécurité dépend de la qualité du processus de développement et non pas du modèle de licence.

Quelles sont les difficultés au niveau des politiques? Vous ne pouvez pas copier coller la réglementation du monde des logiciels propriétaires et s'attendre à ce qu'elle fonctionne dans la réalité d'un modèle FOSS.

J'ai dit au départ, j'ai fait des affirmations assez fortes au départ. Voyons les données. Voyons le système des serveurs racine. Sur les douze opérateurs de serveurs racine. Nous avons donc mené des enquêtes et voir quel était le type de logiciel qu'ils utilisaient. On a vu une prédominance de logiciels FOSS, ou au moins neuf sur douze de ces opérateurs utilisent exclusivement des logiciels FOSS. Il y en a qui utilisent des logiciels propriétaires, mais qui utilisent également des logiciels FOSS. Et donc, vous voyez que ce n'est pas un pour centage faible, FOSS est utilisé majoritairement dans le monde des serveurs racine.

Nous avons examiné également les fournisseurs de TLD. Ces entités fournissent des services qui font autorité et la principale conclusion est que si nous voyons quels sont les opérateurs qui servent le plus grand nombre de TLD, neuf sur dix de ces opérateurs utilisent FOSS.

Pour ce public, cela est d'autant plus pertinent que l'on peut appliquer cela également aux opérateurs ccTLD. Dans ce domaine

des ccTLD, on a constaté que 20 sur 25 opérateurs utilisent FOSS. De manière collective, les ccTLD servent 224 ccTLD uniques qui utilisent ces logiciels FOSS.

Donc, vous voyez que ce ne sont pas des ccTLD petits ou expérimentaux. Ce sont des ccTLD qui ont énormément d'utilisateurs par exemple, en Chine ou au Royaume-Uni, les ccTLD utilise FOSS.

Voyons maintenant les modèles qui utilisent FOSS. Nous avons vu donc deux modèles. Premier modèle. C'est un modèle basé complètement sur des systèmes FOSS. Cela existe, ce n'est pas la majorité, mais on a prouvé que c'est viable. C'est faisable. C'est un point important.

Le modèle le plus populaire, c'est celui où le logiciel est propriétaire. Mais, on a constaté que ces logiciels propriétaires ne sont pas développés de zéro. En général, ils se basent sur des logiciels FOSS. Dans la plupart des plateformes que nous avons, sur lesquelles nous avons enquêté. Toutes sont basées sur des fondements qui s'appuient sur FOSS.

Pour ce qui est des résolveurs. Ici, les mesures sont plus difficiles, mais nous avons constaté une utilisation significative de logiciels libres et à code source ouvert. 80 % des utilisateurs à l'échelle internationale utilisent des résolveurs locaux et par rapport à ces résolveurs locaux, la plupart sont basés sur FOSS. Il en va de même

avec les résolveurs publics. La plupart d'entre eux sont basés sur FOSS.

Il y a un cas d'étude de CloudFlare dans l'étude, où on a un noyau propriétaire entouré de logiciels FOSS. Pour ce qui est des hyperscalers, ils utilisent FOSS pour la résolution DNS. D'autres l'utilisent pour des librairies.

Et donc, pour citer notre rapport, dans les parties les plus critiques de l'infrastructure DNS, FOSS et la norme et le logiciel propriétaire est l'exception. Ce n'est pas une exagération, ce n'est pas un plaidoyer, c'est juste la réalité de ce que nous avons constaté. Les systèmes de nommage en général fonctionnent sur FOSS. Ils sont développés de manière collaborative et distribués de manière libre.

L'approche basée sur la chaîne de valeur traditionnelle requiert des normes de sécurité, en particulier pour des infrastructures critiques. On leur demande de prendre des responsabilités en cas d'échec, en cas de situation problématique et nous avons donc un contrat à chaque étape. Et, on a des règles d'achats publics par exemple.

Donc, qu'en est-il pour FOSS? Et bien en réalité, FOSS est téléchargeable à un coût nul. Il n'y a pas forcément de relation avec le fournisseur de manière traditionnelle, il n'y a pas d'opérateur, il n'y a même pas de vendeur qui peut réguler la vente. Ce sont des volontaires qui sont à la base de FOSS.

Donc, de mettre des coûts de conformité pourrait déstabiliser les petites organisations qui maintiennent ces logiciels. Ou, si ce sont des volontaires, et bien, ils pourraient perdre leur intérêt de manière totale et les projets pourraient être abandonnés. Donc, de passer sur des… d'éviter la juridiction et cela signifie donc que les logiciels deviennent de moins en moins accessibles et de moins en moins sécurisés. Prochaine diapositive.

Donc, nous avons fait une étude de cas parce que dans la plupart des juridictions comme les États-Unis, l'Union européenne ou le Royaume-Uni utilisent FOSS dans leur politique. Et, je ne vais pas rentrer dans les détails, sauf si vous êtes vraiment intéressé par ce sujet, mais cela peut être fait. Prochaine diapositive.

Alors, voici les lignes directrices que nous vous proposons, que nous avons créé. Donc, le SSAC n'a pas d'intérêt, n'est pas intéressé par la réglementation de FOSS. Mais, si dans vos juridictions, vous envisagez la réglementation de FOSS, et bien reconnaissez le rôle fondamental que FOSS joue, reconnaissez que l'infrastructure repose sur FOSS et qu'elle est importante à être préservée.

Deuxième ligne directrice, consultez la communauté FOSS Incluez-les dans l'élaboration des politiques pour éviter des conséquences dramatiques. Utilisez les études de cas qui existent et qui sont actuelles. Encouragez la durabilité de FOSS. Encouragez des contributions à des logiciels FOSS en tant qu'investissement dans les infrastructures publiques, par exemple, et lorsque vous envisagez…

Lorsque vous évaluez les risques, envisagez la réponse à ces risques de manière collective. Financez des solutions partagées avec des dépendances partagées, plutôt que de placer la responsabilité sur les mainteneurs, sur les responsables de la maintenance individuelle. J'en arrive à la fin de ma présentation et j'ai hâte d'entendre vos questions. Merci.

MARCO HOGEWONING Merci beaucoup Maarten pour votre présentation. Je vous encourage tous à lire cet ce rapport parce qu'il est très intéressant. Nous avons le temps pour quelques questions et je crois que la première personne sur la liste est à côté de moi.

NICOLAS CABALLERO Non, pardon, Nous allons donner la parole à la Commission européenne.

GEMMA CAROLILLO Merci beaucoup, monsieur le président et monsieur le vice-président. Nico, si vous voulez prendre la parole avant moi, je n'ai pas de problème. Nous faisons partie de ceux à qui vous vous adressez quand vous parlez des études de cas, des trois quarts, des études de cas d'ailleurs.

Donc, c'est un sujet qui est très important pour nous. Et, je voulais vraiment souligner le fait qu'en tant que régulateurs, nous avons également appris beaucoup de ce processus, en particulier sur la manière d'incorporer les différentes caractéristiques des logiciels

à code source ouverte dans les réglementations numériques. Ça a été très difficile, mais très utile également. Et, nous apprenons de manière collective et je crois que nous arrivons à des très bons résultats.

Ma question porte sur la sécurité de la chaîne d'approvisionnement, parce que ça reste une vraie question, parce que même si on veut se poser différentes questions, cela reste notre enjeu principal. Qu'en est il des réglementations sur les logiciels matériels et comment cela pourrait avoir un impact sur la sécurité des logiciels FOSS?

MAARTEN AERTSEN

Merci Gemma. Donc, vous demander demandez si le SSAC a une opinion sur les matériaux de construction des logiciels. Et, bien, nous n'avons pas d'opinion formée. Je peux vous donner mon opinion à moi, mais je ne parlerai pas au nom du SSAC.

Donc, oui, la sécurité est un problème pour les espaces de logiciels et les logiciels propriétaires ont également ces questions. La question des matériaux de construction peut être répondue par le fait que lorsque les personnes achètent des logiciels qui sont des logiciels propriétaires, il n'en reste que la majorité de ces logiciels sont FOSS. Et, dans ce cas-là, s'il y a un risque, il y a un risque pour tout le monde sur le marché. Et si on ne sait pas ce qui existe dans un produit que l'on achète ou même que l'on vend, et bien comment pouvons nous résoudre les problèmes qui pourraient

arriver avec ce type de produit. Nous en sommes au début de ces expérimentations.

Et, j'apprécie votre commentaire sur l'apprentissage collectif. Je sais que je parle en mon nom propre lorsque je dis que je trouve cela fascinant de voir les processus d'élaboration des politiques, et je suis absolument ravie de voir que nous avons une étude de cas que nous avons pu intégrer dans ce rapport.

MARCO HOGEWONING Merci beaucoup. J'ai le Bangladesh qui a levé la main, puis le président à côté de moi qui voulait prendre la parole, et nous devrons passer au prochain point de l'ordre du jour, le Bangladesh, vous avez la parole.

DR. SHAMSUZZOHA Merci beaucoup. Merci pour cette présentation très exhaustive, en particulier… Moi, je viens du Bangladesh. Nous travaillons avec différents logiciels avec différents systèmes d'harmonisation, de sécurité. Et, merci pour vos recommandations qui sont très utiles. J'ai un commentaire tout d'abord sur le fait que nous travaillons au niveau du ccTLD du Bangladesh, sur les normes de sécurité des procédures et cela couvre ces questions de logiciels. Et, nous sommes également responsables de travailler avec les infrastructures nationales, en particulier pour des questions de sécurité.

Donc, ce que nous essayons de promouvoir au niveau du gouvernement, c'est de faire cette promotion de ces logiciels FOSS. L'un des arguments qu'on nous oppose, c'est les questions d'exigences de capacité d'exigence urgente lorsqu'il n'y a pas de suffisamment de capacité dans l'infrastructure. Donc, cela peut poser des risques importants ainsi que des coûts très importants également. Donc, j'aimerais avoir votre point de vue sur la manière dont nous pouvons gérer des infrastructures sensibles et difficiles.

MAARTEN AERTSEN

Alors, sur ce sujet, je pense qu'il y a moins de différences entre les logiciels propriétaires et FOSS que l'on pourrait l'imaginer. Parce que si l'on travaille sur une infrastructure critique, et bien l'opérateur a une responsabilité de garantir son utilisation fluide. Et, si on décide d'utiliser FOSS qui est le choix majoritaire, dans ce cas là, vous avez soit des experts qui sont présents et c'est un coût effectivement d'avoir des experts ou il faut trouver ces experts ailleurs. Et, lorsque vous regardez les logiciels les plus réussis, et bien ils sont financés par des organisations de soutien. Ils utilisent des organisations de soutien.

Alors, si la situation était différente et si c'était un logiciel que l'on achetait, il fallait acheter des coûts de licence et dans ce cas là, il y aurait un soutien qui viendrait avec ces coûts. Mais, ici, je pense qu'il n'y a pas vraiment de différence par rapport à toutes ces forces, tous ces avantages que nous avons listés. Mais, oui, c'est une infrastructure critique qui parfois nécessite des exigences

d'expertise et chaque opérateur peut faire ce choix en fonction du travail qu'ils effectuent avec leur gouvernement.

MARCO HOGEWONING Merci beaucoup Maarten, et je vais laisser la parole à Nico qui est un grand soutien des FOSS.

NICOLAS CABALLERO Merci beaucoup Maarten pour cette présentation. Est-ce que vous pourriez commenter de manière très rapide sur la manière dont les logiciels libres évitent les situations de dépendance vis à vis des constructeurs, en particulier pour les pays en développement et peut-être surtout en coûts de cybersécurité?

MAARTEN AERTSEN Et, bien, la dépendance vis à vis d'un constructeur, c'est quand on décide d'investir dans un produit et que dans ce cas-là, on ne peut pas changer de produit parce que l'investissement qui a été effectué est bien trop important et les coûts de changement de logiciel sont trop importants également. L'avantage de FOSS et dans la question de dépendance vis à vis d'un constructeur et la question de cybersécurité, c'est que vous n'êtes pas obligé de garder cette relation exclusive avec le fournisseur originel. Parfois, il y a même des organisations qui peuvent vous aider à faire ce changement.

Alors, vous serez toujours dépendant du développeur originel, mais ce n'est pas le cas, comme dans les logiciels propriétaires où

vous n'avez qu'un seul interlocuteur en face. Donc, je vois ici, par exemple, qu'il peut y avoir un pays avec un plus petit budget qui voit une opportunité d'innovation, de lancer une expertise de manière locale plutôt que de payer d'autres entités externes. Mais ça, je pense que c'est un choix qu'ils peuvent faire. Et, c'est ce que je peux vous dire sur cette dépendance. C'est une opinion personnelle encore une fois, puisque nous n'en avons pas parlé dans le rapport. Donc ici, je parlais en mon nom propre.

MARCO HOGEWONING Merci à Nico pour la question et merci à Maarten pour la réponse. Pour des questions d'agenda, nous allons passer à notre prochain point à l'ordre du jour. Nous avons demandé au SSAC de venir nous aider au renforcement des capacités, et nous savons que nous avons beaucoup de nouveaux membres du GAC, pour qui le prochain sujet est un sujet assez nouveau, mais qui est très important et qui devient de plus en plus important, en particulier pour la prochaine série de nouveaux gTLD. Donc, je vais demander à Suzanne de prendre la parole.

SUZANNE WOOLF Merci Marco. Merci Maarten, tu as été excellent, comme d'habitude. Comme Marco l'a dit, je vais parler de NCAP, c'est à dire un projet d'analyse de la collision de noms qui a été proposé par SSAC à l'origine, mais mis en œuvre par un groupe de discussions intercommunautaire.

Et, comme Marco l'a dit, il y en a pas beaucoup d'entre vous qui s'en souviennent, mais ce n'est pas un sujet nouveau. Tout d'abord, nous avons connu des problèmes de collision de noms avec la série précédente, de nouveaux gTLD. Nous avons dû revisiter ces questions parce qu'il y a eu des changements au niveau des attentes et au niveau de la technologie, et au niveau de l'écosystème de réseau dans lequel nous vivons. Diapo suivante s'il vous plaît. Encore une.

Qu'est-ce que c'est qu'une collision de noms? Il est difficile à définir. Une façon de le faire serait de penser à des noms de domaine comme des adresses d'une maison. Si deux maisons ont la même adresse, il est difficile de savoir à laquelle il faut, par exemple, amener une lettre. Et, c'est la même chose avec les noms de domaine.

Les collisions de noms de domaine ont lieu lorsqu'il y a un chevauchement entre l'espace des noms de domaine DNS et un réseau privé. Par exemple, opéré par un fournisseur de VPN où les mêmes noms sont valides, mais où les mêmes noms veulent dire différentes choses. Et, à ce moment-là. Il peut y avoir des mauvaises interprétations et il peut y avoir des confusions très vite. Diapo suivante s'il vous plaît.

Nous allons passer en revue tout cela de manière assez générale. Nous n'allons pas rentrer dans le détail, mais vous aurez toute cette présentation à votre disposition, bien sûr.

Qu'est-ce qui n'est pas une collision de noms? Et certains de ces termes, vous les connaissez probablement si vous avez étudié un petit peu le guide de candidature ou si vous avez étudié la question des nouveaux gTLD. Les collisions du nom sont… Ce n'est pas la même chose qu'une similarité de chaîne ou des chaînes dont la ressemblance peut porter à confusion.

La collision de noms est un problème technique important qui peut affecter la stabilité et la résilience du système, et cela vient de l'utilisation d'un nom de domaine dans un réseau privé. Par exemple, si le nom est le même que celui qui est utilisé dans le DNS public, mais qu'il a une signification différente, cela pose des problèmes. Et le problème est que ces problèmes, ces noms de domaine dans l'espace privé peuvent être utilisés parfois dans le DNS public et cela pose un problème.

La similarité de chaîne pose problème également, mais cela est basé sur la perception de l'utilisateur et cela peut soulever des problèmes au niveau des internautes et des utilisateurs. Lorsque les noms de domaine se ressemblent par exemple, .exemple avec un a minuscule ou avec un A majuscule. Et à ce moment-là, la confusion des utilisateurs peut favoriser une utilisation malveillante de ces noms de domaine.

Donc, il y a donc des cas de collisions de noms qui peuvent avoir lieu, et donc la façon dont on s'en occupe peut avoir des conséquences dangereuses. Donc, il faut comprendre que la collision de noms est importante pour la sécurité du DNS, et cela

relève de la responsabilité de l'ICANN par rapport à un Internet qui soit résilient et qui soit sûr et stable.

Donc, ces noms de réseaux internes peuvent fuir au DNS globale. Cela peut augmenter le problème parce qu'il y a davantage de noms qui sont utilisés dans un contexte privé, mais qui peuvent être délégués dans l'espace DNS public lorsqu'il y aura un élargissement des noms de domaine. Donc, étant donné l'évolution de la technologie, ce problème peut également se traduire par des améliorations qu'il faut apporter. Il y a également une amélioration des noms dans l'espace privé qui ont rendu plus difficile ce travail dans l'espace du DNS. Je vous ai dit que ce problème n'était pas nouveau. Diapo précédente s'il vous plaît.

En 2012, donc, la série de 2012 a augmenté le nombre de noms de domaine dans le DNS, ce qui a posé la question de ce qui pourrait se passer avec ces nouvelles chaînes qui entraient dans le système. En 2013, SSAC a élaboré un document ou ont signalé que des problèmes pouvaient survenir s'il y avait des collisions de noms, et donc les collisions les plus importantes ont été .home, .corp et .mail qui étaient utilisées dans des réseaux privés. Il y a beaucoup de données par rapport à cela, et il y a eu donc un risque identifié de collisions de noms.

En 2017, le conseil d'administration et le SSAC ont mené des études détaillées pour permettre donc aux délégations futures de gTLD de se faire de manière sûre, stable et prévisible. Et, deux projets s'en sont suivis dont l'étude NCAP 2, qui a été communiqué en 2024, car

nous voulions aboutir à des recommandations fondées sur les données que nous avions pour que cela puisse être utile pour la série de 2026.

Nous avons donc... Nous nous sommes basés sur les travaux qui avaient été menés auparavant pour mener cette étude NCAP 2. Donc, le projet NCAP 2 a analysé la situation actuelle par rapport à l'atténuation des collisions de noms. Il y a eu des recommandations pour mieux gérer la collision de noms dans la prochaine série. Cela est présenté comme une évaluation de risque nouvelle afin d'évaluer quels types de dommages peuvent survenir et quels types de mesures d'atténuation il faut mettre en place.

Nous devons dire que l'évaluation devient de plus en plus difficile pour différentes raisons. Et, l'une de ces raisons, c'est qu'il y a beaucoup d'informations à laquelle on ne peut pas accéder, et cela ne nous permet pas de bien comprendre les raisons. Donc, on a eu des difficultés pour notre travail et nous avons donc fait de notre mieux pour répondre à nos objectifs afin de nous assurer de pouvoir évaluer la collision de noms. Nous avons un cadre pour évaluer les différents niveaux de détails en fonction des risques présents, avec un ensemble de collisions de noms.

Et, ensuite, objectif 2, pouvoir évaluer des plans d'atténuation et d'identification de collisions de noms. Nous avons découvert plus que par le passé. Tous ces cas seront un peu différents les uns des autres. Il n'y aura pas un questionnaire par rapport à cela, mais voici le diagramme du cadre auquel on a abouti à partir de NCAP 2.

Donc, l'un des principaux points, c'est la formation d'une équipe technique pour vérifier le processus et évaluer à quoi était rattaché les risques.

Nous avons pu faire l'hypothèse que, dans certains cas, il y avait des risques permanents et dans ces cas-là, l'atténuation était possible. Mais, lorsqu'il y a deux cas pareils, nous avons donc conclu qu'il fallait vraiment se pencher en détail pour savoir si ce type de collision pouvait survenir ou non. Donc, certains cas pouvaient être évalués de manière presque automatique et pour d'autres cas, il fallait l'intervention d'experts. Lorsque le cas était plus compliqué. Diapo suivante.

Alors, quels sont les bénéfices de ce cadre d'évaluation de la collision de risque? Les caractéristiques, une gestion de risque proactive qui permet d'évaluer et de revoir les stratégies d'atténuation des risques risque avant qu'il y ait des dommages. Ensuite, le cadre, nous avons essayé de le rendre cohérent et efficace. L'approche centralisée de cette analyse s'assure que cette atténuation se fasse pour tous les gTLD, parce que nous avons la responsabilité au niveau de la zone racine pour que ce soit stable. Et donc ce cadre est basé sur des données et vise à permettre une amélioration, une expansion sur des noms.

Nous avons également pris en considération les considérations concernant la confidentialité des données, et nous avons vu qu'il y avait un risque de ne pas évaluer de manière appropriée la collision de noms parce qu'on avait les mauvaises données. Et, donc, à notre

avis, ce risque était important. Tous les cas sont différents, je le répète, mais être capable de comparer le risque d'agir versus le risque de ne pas agir était également important pour nous afin de pouvoir analyser ce type de cas. Nous avons conclu sur le fait que l'identification précoce de ce type de risque est un élément crucial pour éviter le dommage. Voilà, un petit peu la présentation. Je serai ravi de répondre à vos questions.

MARCO HOGEWONING Merci Suzanne. Nous apprécions votre présentation. Donc, c'est bien de faire la part des choses entre ce que c'est que la collision de noms et la similarité de chaîne. C'est intéressant de bien insister sur cette différence. Je vois que Nico nous dit qu'on a le temps de quelques questions.

NICOLAS CABALLERO J'ai un commentaire rapide. Si on retourne à la page 23, nous avons quatre étapes là-bas. Ma question concerne le temps, en moyenne, parlons-nous de jours semaines? Et, je voudrais comparer cela avec les 32 étapes. Vous vous souvenez hier la présentation avec la GNSO pour ce qui est de l'efficacité et de la rapidité. Alors, en moyenne, combien de temps cela prend?

SUZANNE WOOLF C'est une question que nous nous sommes posés. Nous ne sommes pas tombés d'accord par rapport à quel délai recommandé. Parce qu'il y avait des pressions pour que ce soit aussi rapide que

possible, mais en même temps, on ne veut pas louper des risques importants. Donc, on parle de semaines plutôt que de mois ou des années, mais c'est quelque chose sur laquelle nous devons… Nous ne nous sommes pas prononcés. Ce serait à la communauté ou à l'organisation ICANN de le décider.

MARCO HOGEWONING Merci. Je pense qu'on a le temps pour d'autres questions, je n'en vois pas dans la salle, donc je vais remercier Suzanne pour ses explications. Cette présentation sera en ligne pour ceux qui sont intéressés. Et maintenant, nous allons passer au point suivant qui a été suggéré par les responsables de la thématique Utilisation malveillante du DNS. Je ne sais pas si Ram ou vos collègues pouvaient partager quelques recommandations techniques concernant le rapport thématique.

RAM MOHAN Merci Marco. Pour répondre vite à votre question, je voulais informer le GAC par rapport à la diapo précédente. Il y a un travail qui a commencé qui est lié à l'espace de noms. Nous avons commencé un groupe de travail qui s'occupe de l'intégration responsable dans l'espace du DNS, et ce groupe se focalise sur le fait de savoir ce qui se passe lorsque des identificateurs dans d'autres espaces de noms, et plus précisément dans l'espace des blockchains, qu'est-ce qui se passe lorsque ces identificateurs veulent interagir avec des identificateurs du système, des noms de domaine ou d'autres identificateurs du DNS? Donc, nous avons

commencé le travail. Nous espérons pouvoir fournir des conclusions.

Notamment, nous nous focalisons et nous nous inquiétons des problèmes concernant le cycle de vie des noms de domaine, la fraude, ainsi que sur des risques de stabilité et de sécurité qui pourraient être introduits dans le DNS. Lorsque vous avez des systèmes dans d'autres espaces de noms qui utilisent des thèmes ou des mots qui sont similaires à ceux que nous utilisons dans le DNS, mais qui n'ont pas la même signification, mais qui sont liés. Voilà. Diapo suivante.

Pour votre question, nous sommes ravis de savoir qu'il y a un travail en matière de politique qui a commencé par rapport à un éventuel PDP sur l'utilisation malveillante du DNS. Par le passé… on peut passer à la diapo suivante.

Le SSAC a fourni des commentaires et des avis une fois que les recommandations de politiques étaient formulées. Nous avons changé un petit peu le modèle. Avec nos collègues de la GNSO, nous avons été invités à être présents dans la préparation du PDP et ce que nous faisons.

Nous ne participons pas aux discussions sur une piste de travail, deux pistes de travail ou trois pistes de travail. Ce type de question concerne les gens qui s'occupent d'élaboration de politiques. Nous intervenons plus spécifiquement lorsque l'on a trait à des questions concernant l'utilisation malveillante du DNS, et nous

passons pas mal de temps à analyser l'évolution de ce type d'utilisation malveillante.

Nous nous concentrons donc sur cette question, et nous pensons que c'est un sujet très important pour nos discussions avec le conseil d'administration pour les priorités de 2026. Nous avons soutenu ce que la GNSO a dit, en particulier pour les parties contractantes, et sur le fait que l'utilisation malveillante du DNS doit être au top des priorités en haut des priorités de toute la communauté. Parce que si nous n'arrivons pas à lutter contre cette utilisation malveillante du DNS, ce ne sont pas seulement les utilisateurs malveillants qui en pâtiront, mais tout ce système, toute cette communauté multipartite et ce modèle multipartite qui que nous présentons comme un formidable exemple. Donc, il faut absolument se concentrer sur l'utilisation malveillante du DNS. Il faut être impliqué là-dessus, en particulier dans la phase de conception.

MARCO HOGEWONING Merci beaucoup Ram. C'est formidable de vous entendre dire cela. Est-ce qu'il y a des membres qui travaillent sur l'utilisation malveillante du DNS, qui veulent répondre ou qui ont d'autres questions pour le SSAC? Ou, bien sûr, si quelqu'un d'autre a une question sur ce sujet. La Commission européenne, vous avez la parole.

JANOS DRIENYOVSZKI

Merci beaucoup d'être ici aujourd'hui avec nous. Merci pour votre présentation. Nous nous demandions si… Pour les PDP, bien sûr, il est important de comprendre le champ d'application. Et, nous nous demandions quels sont vos points de vue sur les enregistrements groupés sur cette piste de travail, cet enjeu? Parce que, bien sûr, nous voulons lancer un processus d'élaboration des politiques qui soit pertinent et qui ait un impact et qui cible qui… qui est la bonne cible.

Et, lorsqu'il concerne les API, vous avez parlé de cela et nous nous demandons si cela comprend tous les enjeux liés aux enregistrements groupés, aux enregistrements de masse. Donc, nous aimerions avoir votre point de vue. Est-ce que c'est une bonne approche de se concentrer sur les API, ou est ce que nous devrions formuler le champ d'application d'une manière qui soit plus durable et qui nous permette de prendre cela en compte? Alors, ça, c'était mon ma propre question. Je ne sais pas si quelqu'un spécialiste de la technique pourrait y répondre.

RAM MOHAN

Merci beaucoup. Alors, il y a une réponse assez nuancée à vous offrir, puisqu'il y a des exemples où il y a des raisons justifiables, des raisons légitime d'avoir des enregistrements groupés pour pouvoir protéger le nouveau produit des registres. Et parfois, au sein d'un TLD, il y a des enjeux spécifiques qui justifient un enregistrement groupé.

Donc, je voudrais savoir si les accès API ne sont pas seulement la seule manière pour avoir des enregistrements groupé. Il y a énormément de situations où des acteurs malveillants ont enregistré des TLD avec des noms de domaine malveillants, sans utiliser les API, parce qu'il y a des manières de contourner cette barrière.

Ceci étant dit, c'est un bon point de départ pour cette investigation. Les enregistrements en masse, Les enregistrements groupés doivent être définis. Une préoccupation que nous partageons avec certains acteurs de la communauté, c'est que si on définit un seuil, si on dit que tout ce qui est en dessous de et on choisit n'importe quel chiffre, on ne l'évaluera pas avec la même intensité. Et bien, dans ce cas là, on peut s'attendre à ce que ce soit utilisé de toute manière.

Donc, mon objectif, mon espoir, c'est qu'une politique soit créée pour offrir un cadre large pour le type de comportement que l'on veut éviter, plutôt que des méthodes spécifiques par lesquelles ce comportement est mis en œuvre. Donc, ça, c'est la distinction qui est importante à garder en tête lors de ce processus d'élaboration des politiques.

MARCO HOGEWONING Merci beaucoup Ram. Je vois qu'il n'y a plus de questions. Donc, cela me permet de vous remercier… de vous remercier, de vous dire que vous ferez partie du PDP. Et, nous avons pour objectif de renforcer les liens entre le GAC et le SSAC, et cela nous permettra

d'avoir des questions plus larges sur la manière dont nous voyons des opportunités de collaboration, que ce soit Le GAC et le SSAC. Nous ferons partie de ce PDP. Cela ne sera peut-être pas la seule manière dont nous pourrons travailler main dans la main, mais c'est l'une de celles-ci. Prochaine diapositive s'il vous plaît. Alors, est-ce qu'on reste sur l'utilisation du DNS ou sur la question précédente?

INDE

Alors, j'ai une question peut-être sur l'utilisation malveillante du DNS. Mais, tout d'abord, qu'en est-il de la réduction de la fenêtre de quinze jours pour l'utilisation du DNS? Nous pensons que c'est la première étape qui nous permettrait d'avancer et de réduire les utilisations malveillantes du DNS. Dans deux jours, nous aurons la validation de ces défis qui sont présents depuis des décennies désormais.

Mais, ces questions d'authentification, c'est quelque chose que l'on fait constamment dès qu'on rentre dans une chambre d'hôtel, dès qu'on va dans un aéroport et qu'on utilise le wifi ouvert, on a ces questions d'authentification. Et, si on apporte ces questions d'authentification au niveau du nom de domaine, je pense que ce n'est même pas une question d'identifiant ici qui devrait être soulevée. J'aimerais savoir ce que vous pensez de cela, parce que je ne comprends pas la la raison pour laquelle on garde cette fenêtre de quinze jours.

MARCO HOGEWONING Merci pour cette question. Alors, oui, nous parlons de ces deux semaines de vérification. Ram, est-ce que vous pensez à cela? Qu'est-ce que vous pensez de cela?

RAM MOHAN Et, bien, nous avons une… Nous avons déjà formé notre opinion sur cette question. Et, bien, si on parle d'une situation urgente, il faut que cela se traduise quelque part. Et, si c'est quelque chose qui nécessite une réponse rapide. C'est l'équivalent d'appeler un service d'urgence dans la vie réelle, on n'attend pas une réponse sous quinze jours ou sous deux jours, même lorsqu'on appelle un service d'urgence. Notre approche ici, c'est de dire que cette question d'urgence est très importante.

Pour la question de la validation et de la vérification. Nous, du point de vue du SSAC, nous n'avons pas encore développé un point de vue défini du point de vue du SSAC ou du RSSAC, mais nous avons fait des recherches de sécurité sur ces questions, et des membres des agences responsables de l'application de la loi qui se sentent empêchés par cette mise en œuvre de cette validation et de cette authentification. Donc, nous avons encouragé le développement d'un système d'accès tiers qui permettent l'accès à des parties qui ont un intérêt légitime à ces questions.

Donc, voici où nous nous trouvons. Donc, les requêtes urgentes, en particulier lorsqu'il s'agit du GAC ou du conseil d'administration, il faut les garder. Il faut garder en tête que la définition dans le

dictionnaire de l'urgence, n'est pas… ne devrait pas être la base de cela.

INDE Alors, ma question portait vraiment sur l'utilisation malveillante du DNS lors de cette fenêtre de quinze jours et où l'on demande une authentification, une validation pour l'enregistrement du domaine. Je pense que c'est quelque chose que je ne comprends pas et qui mérite réponse.

RAM MOHAN Merci d'avoir clarifié votre question. Alors, encore une fois, je ne peux pas parler au nom du SSAC dans son entièreté. Je pense que c'est une question qui doit être étudiée de manière plus précise, et nous devrions évaluer les dommages qui sont faits aux utilisateurs finaux, les mesurer par rapport à d'autres exigences contractuelles et de développement des politiques. Mais, nous devrions garder les dommages faits aux utilisateurs finaux comme première priorité.

MARCO HOGEWONING Merci à l'Inde. Merci à Ram. Y a-t-il d'autres questions? Il nous reste deux minutes. On peut évidemment conclure ici s'il n'y a pas d'autres questions et je peux vous les donner une pause un peu plus longue si vous le souhaitez. Encore une fois, nous avons hâte de mener cette collaboration.

NICOLAS CABALLERO J'ai encore une question en ce qui concerne la collaboration sur les FOSS. Est-ce que cela fait partie de cette collaboration que l'on peut envisager? Parce que lors du dernier forum sur la gouvernance de l'Internet en Norvège, le gouvernement de Norvège a partagé des solutions et il y a plus de 45 pays qui bénéficient de ces solutions. Alors, quelle serait la manière de fonctionner? Est-ce que nous avons des membres du GAC qui sont intéressés par cette coopération sur les FOSS? Comment pourrions nous faire cela?

RAM MOHAN Alors, je suggérerais de rentrer en contact directement avec moi en tant que président ou tous les membres du personnel qui travaillent pour le SSAC, qui sont excellents, et nous pourrions lancer un dialogue et voir quelle est la meilleure manière pour fournir du contenu ou pour vous aider et collaborer avec vous. Si vous êtes intéressés dans ce domaine, c'est l'un des rapports du SSAC qui s'adresse directement à vous. Donc, vous travaillez avec nous. Nous voulons collaborer et nous voulons que cela fonctionne. Si vous venez travailler avec nous, cela valide le fait que ce type de travaux est très utile et cela nous encourage grandement.

MARCO HOGEWONING Très bien. Sur cette note, encore une fois, merci très chaleureusement à Ram, Suzanne, Maarten et Tara d'être venu avec nous. Tara, d'être venu parler de cette collaboration future entre le GAC et le SSAC. Ceci étant dit, sauf s'il y a des commentaires...

NICOLAS CABALLERO Oui, un détail d'organisation. Vous avez une pause café désormais? Nous nous retrouvons à 4 h 30. La séance est levée. Merci.

[FIN DE LA TRANSCRIPTION]