ICANN83 | Forum de politiques – Séance du GAC sur la sécurité et la stabilité
Mercredi 11 juin 2025 – 09h00 à 10h15 CEST

PERSONNE NON-IDENTIFIÉE Au personnel audiovisuel, il y a encore un élément qui n'est pas allumé.

DAN GLUCK Bonjour et bienvenue à la session du GAC sur la sécurité et la stabilité de l'ICANN 83, le mercredi 11 juin à 9 h, heure locale. Cette session est enregistrée et régie par les normes attendues de comportement de l'ICANN et la politique anti-harcèlement de la communauté de l'ICANN. Pendant cette session, les questions et les commentaires seront lus à voix haute s'ils sont soumis dans le bon format dans le chat Zoom. L'interprétation se fera dans les six langues de l'ONU et le portugais.

Si vous souhaitez prendre la parole, levez la main dans le logiciel Zoom. Lorsqu'on donnera votre nom, vous pourrez allumer votre micro. Donner votre nom et dites la langue que vous parlez si c'est une autre langue que l'anglais, et parlez à un rythme raisonnable et clairement pour permettre une interprétation précise. Je donne la parole à Marco Hogewoning, Vice-Président du GAC. Merci, à toi Marco.

MARCO HOGEWONING

Bonjour! C'est moi qui vais présider cette session. J'espère que Nico est quelque part dans la salle en train de profiter d'une bonne tasse de café. Nous avons divisé cette session en deux segments. Dans un premier temps, le SSAC va nous parler de certains de ces projets. J'ai demandé également à un représentant de SIDNLabs de nous parler de la façon dont l'informatique quantique peut interagir avec la sécurité du système de nom de domaine. On en avait déjà parlé à l'ICANN 82 à Seattle.

Donc, je vais donner la parole à mes collègues à la table. Donc, je me suis déjà présenté. Marco Hogewoning, représentant des Pays-Bas. Je donne la parole à mes autres collègues.

MAARTEN AERTSEN

Bonjour, je suis Maarten Aertsen, je suis membre de SSAC.

WARREN KUMARI

Bonjour, Je suis Warren Kumari, également membre de la SSAC.

GREG AARON

Je suis Greg Aaron, également membre du SSAC.

RAMMOHAN

Et, moi je suis Ram Mohan. Je suis également du SSAC, que je préside le SSAC.

CRISTIAN HESSELMAN Christian Hesselman. Je suis l'opérateur de registre pour .nl, le domaine de premier niveau des Pays-Bas et je suis avec SIDNLabs.

MARCO HOGEWONING Je donne la parole à Ram.

RAM MOHAN Nous voulions partager quelques informations relatives à l'accès aux données d'enregistrement de domaine. Que voulons-nous faire? Nous voulions diffuser auprès du GAC ce que sont nos objectifs. Nous voulons faire en sorte que les politiques prises relatives à l'accès aux données d'enregistrement des gTLD soient robustes, bien élaborées et qu'elles servent les besoins de la communauté de l'Internet et qu'elle nous protège des menaces sécuritaires. C'est ce qui doit être fait.

Alors, comment le faire? Il faut créer un système d'accès à ces données qui épouse un mécanisme structuré et accéléré afin que les requêtes légitimes, urgentes tout particulièrement, soient traitées de façon prioritaire et accélérée. Il faut que les politiques en matière de délai de réponse, en matière de méthodologie de réponse, soient clairement élaborée et acceptée par toute la communauté. Nous estimons également que l'organisation ICANN doit partager des indicateurs liés aux requêtes de données, d'enregistrement, de nom de domaine.

Il faut que l'accès aux données d'enregistrement demeure une clé de voûte de l'architecture de sécurité et de stabilité. Nous avons

fourni des retours à l'EPDP sur ce point, le processus accéléré de l'élaboration de politiques, mais ceci n'est pas un champ qui entre en conflit avec la confidentialité. Les besoins de confidentialité doivent être traités de façon adéquate. Mais, il y a également une préoccupation très claire en matière de sécurité et de stabilité. Dès lors, nous voulons que le processus qui débouchera sur ces changements au sein de la communauté prenne en compte les principes que nous avons énumérés à l'écran. C'est ce que nous voulions dans un premier temps partager avec vous et je suis disposée à répondre à vos questions.

MARCO HOGEWONING Merci RAM. Bien sûr, je pense que le GAC est d'accord avec votre point de vue en la matière. Y a-t-il des questions? Bien que nous venions de commencer la réunion. Je n'en vois pas dans Zoom. Peut-être qu'à la fin de la session, on pourra revenir vers toi RAM. Alors, le prochain sujet, ce sont les logiciels libres et à code source ouvert. Maarten.

MAARTEN AERTSEN C'est un sujet familier les logiciels libres et à code source ouvert. Ils peuvent être utilisés, librement, partagés, modifiés, étudiés. Nous nous penchons tout particulièrement sur le rôle que joue ce type de logiciel dans le système de nom de domaine global. Ils sont au cœur de ce système, mais il n'y avait pas d'études exhaustives qui ont été menées sur ces logiciels particuliers.

Ces logiciels sont uniques en matière de développement et de gouvernance de par le monde. Les parties prenantes parlent d'infrastructure, de fiabilité, de logiciels, etc. Et nous, nous voulions rendre plus visible ce type de logiciel, ces caractéristiques, afin que les discussions politiques l'évoquant prennent ces caractéristiques en compte. Donc, ce sont nos deux objectifs. Nous voulons faire en sorte que cette dépendance critique soit visible et nous voulons également rendre évidentes les caractéristiques de ces logiciels pour peut-être bien informer certaines des hypothèses qui pourraient être élaborées à propos de logiciels en général, mais de ces logiciels libres et à code source ouvert en particulier.

Alors, voici les champs qui nous intéressent. Il y en a quatre. Donc, il y a une enquête pour laquelle nous décrivons l'état des lieux. Nous nous penchons sur le volet enregistrement de domaine. Nous nous penchons également sur la sécurité, sur le système de noms de domaine où l'on publie et on extrait des cartes. On analyse les caractéristiques de ce logiciel et son modèle de développement. C'est différent que la fabrication d'une marchandise physique ou d'autres logiciels avec d'autres caractéristiques. On compare ensuite les caractéristiques avec celles des logiciels qui importent pour le DNS.

Puis, on clarifie certaines des hypothèses qui ont déjà été formulées et qui ne tiennent pas la route, et on clarifie certains des malentendus. Puis l'on se penche sur les facteurs de risque pertinents qui devraient être pris en compte par les décideurs

politiques ou les régulateurs. Cela a trait au développement, mais également aux opérations. Voici les champs que nous couvrons.

À Muscat, nous espérons pouvoir vous en dire davantage. En effet, nous souhaitons publier ce rapport d'ici l'ICANN 84. Nous estimons que l'utilisation des logiciels libres et à code source ouvert dans le DNS et dans l'enregistrement de nom de domaine est une force, mais qu'il y a des risques à prendre en compte et nous pensons pouvoir vous fournir quelques orientations en matière d'utilisation de ces logiciels libres et à code source ouvert. C'est tout pour moi. Je suis disposée à répondre à vos questions.

MARCO HOGEWONING C'est vraiment très bref comme présentation. Y a-t-il des questions pour Maarten? l'Inde.

SAJID RAHMAN J'ai une question pour Ram Mohan. Nous partageons un objectif. Un délai de réponse de 24 h pour les données d'enregistrement. Mais, cela fait plus de deux ans que l'on tente de pousser l'ICANN à trouver un accord, donc pour l'instant, on n'a toujours pas de calendrier.

Le niveau d'urgence a été formulé à plusieurs reprises de la part du GAC et du SSAC, mais le processus se prolonge. Il y a deux axes. Il y a un axe politique et un axe authentification. Selon vous, en tant que président du SSAC et je parle également au Vice-Président du GAC, peut-être qu'une déclaration conjointe du SSAC et du GAC

serait utile afin d'encourager le CA de l'ICANN à prendre une décision aussi rapidement que possible.

MARCO HOGEWONING RAM, je te donne la parole.

RAM MOHAN Merci. Alors, nous sommes convenus que pour les requêtes urgentes, le processus doit être clarifié. Je pense que l'on en discute déjà, notamment avec les parties qui doivent mettre en œuvre ces changements. Je ne peux pas m'exprimer au nom du SSAC. Je devrais consulter les membres, mais nous l'avons déjà dit très clairement, si l'on estime qu'un volet est urgent, il doit être traité dans l'urgence et les réponses apportées doivent être apportées de façon très prompte. Cela ne devrait pas prendre trop de temps. Si une déclaration commune avec le GAC aurait du poids. Nous sommes évidemment ouverts. Nous sommes prêts à mettre l'accent sur l'importance de ce sujet et nous pensons que c'est un sujet important. Il faut être très clair, urgent. C'est urgent. Ça ne veut pas dire que l'on procède comme à l'accoutumée.

MARCO HOGEWONING Oui, merci, je suis d'accord. Vous le savez, le GAC a évoqué les requêtes urgentes dans les cinq derniers communiqués du GAC. Du moins si je n'en oublie pas. Donc, nous sommes actifs en la matière. Nos collègues sont présents dans ce champ. Selon moi, on progresse. C'est vrai que pour les requêtes urgentes, on n'avance

pas de façon aussi rapide que l'on devrait. Donc, je suis tout à fait d'accord avec Ram. Si une déclaration commune nous permet de faire avancer les choses, et bien on peut le faire, on pourra y revenir en tout cas. Y a-t-il d'autres questions? Russell.

RUSSELL WORUBA Merci aux collègues du SSAC. Vous faites un super boulot! Je suis un grand fan du SSAC. Merci de tous ces travaux sur les logiciels libres et à code source ouvert. Les FOSS, F.O.S.S. Nombre de pays dans les régions mal desservies dépendent des logiciels en source ouverts pour opérer le système de nom de domaine, notamment au niveau des ccTLD. Le paysage change et nous nous réjouissons de consulter les résultats de ces études. Auriez-vous peut-être quelques références à nous donner? Notamment pour l'état actuel des lieux dans les régions?

MAARTEN AERTSEN Merci de cette question. Je peux vous donner un petit avant-goût. Pour ce qui est de l'enquête sur l'environnement, on tente d'avoir des données robustes sur qui utilise quoi. Pour l'instant, on n'a qu'un projet de texte qui n'a pas encore été publié. Et, là, on dit que le DNS global opère grâce au logiciel libre et à code source ouvert. Ce n'est pas simplement vous. On a des données pour étayer cela. Dans l'espace ccTLD, 20 sur 25 opérateurs principaux utilisent ce logiciel. Si vous ajoutez l'espace gTLD, c'est 9 sur 10 et si vous vous

penchez sur le système de serveur racine, c'est 9 sur 12 qui utilisent ces logiciels libres et à code source ouvert.

C'est la valeur ajoutée qu'a ce rapport. Il s'agit de diffuser auprès d'un plus vaste public ces informations. Et, nous voulons vraiment diffuser cet état de fait, car nous constatons que dans certaines régions, on réglemente l'utilisation du logiciel mais qu'on ne pense pas vraiment aux logiciels libres et à code source ouvert. Et c'est un problème car les caractéristiques sont différentes, notamment en matière de développement et de financement, en matière d'utilisation et cette réglementation n'est peut-être pas la bonne stratégie, en tout cas pour ces logiciels FOSS.

MARCO HOGEWONING Je vois l'Allemagne.

RUDY NOLDE Je voulais vous demander ce que vous vouliez dire aux décideurs politiques. Puis, j'ai vu votre dernière planche où vous proposez des orientations. C'est un avant-goût, mais moi je suis peut-être un peu impatient et j'aimerais que vous nous disiez de façon très, très préliminaire quelles orientations sont les vôtres pour les décideurs politiques en tout cas.

MAARTEN AERTSEN Alors, je ne veux pas empiéter trop sur le temps de mes collègues, mais je serai bref. Alors, nous voulons mettre le doigt sur quelques points qui sont sujets à des malentendus. Alors, par exemple, dans

le champ politique, on parle souvent de relation contractuelle. Vous dites on va réglementer les infrastructures critiques des opérateurs et donc dans ce cas-là, il y a des obligations qui sont appliquées à leurs sous-traitants et leurs sous-traitants vont appliquer des obligations à leurs sous-traitants. Donc cela peut fonctionner pour du matériel, parfois pour des logiciels.

Mais, cela ne marche pas si l'on télécharge directement les logiciels sur l'internet, car là il n'y a pas de chaîne d'approvisionnement. Donc, ce type d'obligation contractuelle ne fonctionne pas pour les logiciels libres et à code source ouvert. Parfois, il y a des logiciels qui sont développés et entretenus par un groupe qui s'y consacre et les liens vont bien au-delà de ce que sont des liens contractuels ou des instruments de ce genre. Ce ne sont pas les mêmes liens.

Donc, quels sont nos conseils? Et, bien, il faut réfléchir à comment l'on interagit avec les développeurs. Mais, il faut savoir que si vous forcez des opérateurs à respecter des exigences. Il ne faut pas les entraver dans leur choix des meilleurs logiciels qui pourraient être ces logiciels libres et à code source ouvert. Et, si vous faites cela, vous n'allez pas atteindre vos objectifs politiques. Voilà, c'est un peu. Ce que nous pensons, mais je pense qu'il faut que nous publiions le rapport dans un premier temps, puis on pourra en parler.

MARCO HOGEWONING On serait ravis que vous reveniez nous parler après la publication du rapport. Je vois qu'il n'y a plus de demande de prise de parole.

Dès lors, je propose que l'on passe au dernier segment la refonte du blocage DNS. Greg.

GREG AARON

C'est un document qui est en réalité une actualisation de deux documents rédigés par le SSAC il y a onze ans. Le blocage DNS, ce n'est pas nouveau, mais nous pensions qu'il était venu le temps de le mettre à jour, car il y a eu de nombreux nouveaux exemples de par le monde de blocage DNS. On a constaté ce qui s'est produit dans le sillage de ces actions de blocage. Il y a également de nouvelles technologies qui ont été élaborées entre temps, des technologies qui ont une incidence sur le blocage DNS et sur la façon dont les individus peuvent extraire des ressources de l'Internet. Donc, il y a 20 membres du SSAC qui se sont penchés sur ce dossier. Warren et moi-même avons coprésidé ce groupe.

Qu'est-ce que le blocage DNS? Alors, vous êtes derrière votre ordinateur. Vous voulez vous rendre sur un site web? Vous tapez l'adresse, le nom de domaine et là, votre requête est envoyée à un résolveur DNS. On les appelle des résolveur récursif DNS. C'est souvent votre FAI qui gère cela. Donc votre résolveur récursif transforme votre nom de domaine en adresse IP et ensuite le système de nom de domaine identifie votre destination et vous permet d'interagir avec le site web sur lequel vous souhaitez aller.

Normalement, ce processus se produit de façon instantanée. Vous arrivez directement là où vous souhaitez aller, mais le résolveur récursif peut bloquer un nom de domaine. Cela signifie que le

résolveur va vous donner une autre réponse qu'attendu. Et pour cela, il y a deux approches. Dans le premier exemple, le résolveur récursif peut vous dire que le nom de domaine n'existe pas alors qu'il existe. Par exemple, si vous allez sur Wikipédia, vous tapez l'adresse, mais vous n'êtes pas connecté à Wikipédia, mais l'autre exemple c'est plutôt que d'aller sur le site web désiré, vous êtes emmené sur un autre site web. Autrement dit, le résolveur récursif vous donne une réponse inattendue. Peut-être même que l'on pourrait dire qu'il vous ment, qu'il ne vous donne pas la réponse qui existe dans le système de nom de domaine.

Le blocage DNS est une technique, c'est un outil et comme tout outil, il peut être utilisé à plusieurs fins. Il peut être utilisé de manière experte, ou bien elle peut être utilisée de manière non professionnelle. C'est comme un marteau. Vous pouvez l'utiliser pour construire une maison ou bien vous pouvez l'utiliser pour frapper quelqu'un sur la tête. Et donc, il est conçu pour empêcher que l'on puisse accéder à certains contenus ou accéder à certains services. Cela affecte non seulement l'accès à certains sites Web, mais l'utilisation générale du DNS. Cela peut affecter les services de messagerie, la gestion de réseau et d'autres services qui s'appuient sur le DNS.

Diapo suivante s'il vous plaît! Alors, si le résolveur DNS était Gandalf. Gandalf, c'est ce qu'il dirait. Vous ne passerez pas. Le blocage DNS est utilisé à différentes fins. Une façon de l'utiliser, c'est pour garantir la sécurité. Un résolveur pourrait… C'était dramatique ça. La lumière s'est éteinte. Un résolveur DNS peut être

configuré de manière à ne pas diriger les gens vers des sites qui sont malveillants ou des sites d'hameçonnage. Cela est configuré de manière à être un service bénéfique pour les utilisateurs et nous sommes tous de quelque manière que ce soit, protégé par des bloqueurs DNS. Bien souvent, quand vous voulez accéder à une page web, vous recevez un message comme quoi vous ne pouvez pas le faire ou il vaut mieux que vous ne le fassiez pas.

Et, donc, ce type d'utilisation du blocage DNS est assez fréquente, car ce système est conçu pour aider les gens et pour cela, le système est utilisé au niveau local. Donc, vous l'utilisez dans votre compagnie pour sécuriser votre réseau.

D'autres personnes l'utilisent pour contrôler le contenu. Par exemple, dans une librairie publique, on peut vous empêcher l'accès à certains types de contenus que la communauté considère qu'ils ne devraient pas être accessibles, par exemple des sites de pornographie ou d'autres types de sites qui peuvent être dangereux. Certaines sociétés peuvent par exemple bloquer l'accès à des réseaux sociaux à leurs employés. C'est une configuration locale qui répond à la politique mise en place par une société, une compagnie.

Une utilisation plus controversée, l'utilisation du blocage DNS pour empêcher les personnes d'accéder à certains contenus et que ce blocage est fait au niveau national, c'est à dire le fait d'empêcher que les citoyens d'un pays en particulier ne puissent pas accéder à un certain type de contenu. Et, c'est pour cela que nous voulions

présenter ces informations à des décideurs politiques, à des membres de GAC, parce que ce type de décision affecte un grand nombre d'utilisateurs.

Parfois, cette décision est prise en fonction de La loi locale. Par exemple, il y a des pays qui décident de bloquer tout contenu pouvant contenir des informations pédopornographiques par exemple. Et donc certains pays ont la liste de ces domaines qui est distribuée pour être bloquée. D'autres pays préfèrent bloquer l'accès à des contenus qui expriment des opinions politiques. Et donc ce type d'utilisation vise des utilisations en vue de censurer certains contenus.

On veut faire une distinction entre le blocage DNS et la saisie d'un nom de domaine. Le blocage ne permet pas de retirer des contenus sur Internet. La suspension d'un domaine empêche l'accès au contenu en supprimant le nom de domaine. Il y a des centaines de noms de domaine qui sont suspendus tous les jours pour des problèmes d'utilisation malveillante d'hameçonnage par exemple.

Mais, de temps en temps ces saisies répondent à des décisions de justice. Par exemple, les forces de l'ordre dans cette diapo, vous voyez qu'il y a les forces de l'ordre qui décident de supprimer ce nom de domaine et de le suspendre. Cette décision peut impliquer la suspension de nom de domaine ou bien la redirection des utilisateurs vers un autre site ou il y aura un message communiquant ce qui s'est passé.

Donc, le SSAC dans son document explique les techniques qui sont utilisées pour le blocage DNS. Quelles sont les motivations derrière l'utilisation de cet outil? Et bien sûr, il peut exister des raisons concrètes qui peuvent être légitimes dans certains pays et pas dans d'autres pays pour mettre en place ce type d'outil. Nous n'émettons pas de jugement de valeur par rapport à ces cas particuliers.

WARREN KUMARI

Diapo suivante, s'il vous plaît. Le blocage DNS est un outil et comme tout outil, il y a des avantages et des inconvénients. Il est important de comprendre comment fonctionne cet outil pour savoir comment l'utiliser et ne pas avoir des conséquences inattendues.

Donc le blocage DNS, comment fonctionne-t-il? Il s'agit de mettre dans le résolveur des informations par rapport à ce qui doit être bloqué, ce qui ne doit pas être bloqué. Mais cela s'applique à des utilisateurs qui utilisent ce résolveur-là. Cela veut dire que si un utilisateur décide d'utiliser un autre résolveur, il pourra contourner ce blocage.

Dans ce diagramme que vous voyez en bas, vous voyez que les requêtes sont envoyées à l'un des résolveurs ordinaires de FAI. Mais si le nom qu'il cherche est correct, la résolution va se faire normalement. Mais si ce nom figure dans une liste de blocage, quelque chose va se passer. Soit vous recevez une réponse comme quoi le nom n'existe pas, ou bien le résolveur va essayer de vous

rediriger pour que vous accédiez à un autre site. Mais si la requête va vers un autre résolveur et qu'il n'y a pas la liste de blocage, l'utilisateur pourra accéder normalement à Internet. Diapo suivante.

Alors, comment ça se fait que les utilisateurs puissent utiliser différents résolveurs? Il y a un certain nombre de ce qu'on appelle des résolveurs publics qui sont utilisés par beaucoup de personnes : 21 % des utilisateurs d'après les recherches d'APNIC utilisent des résolveurs publics. Par exemple, Google PublicDNS utilise le résolveur public, Cloudflare, Quad9, mais il y a également d'autres versions. Un autre exemple, c'est DNS4EU. C'est un résolveur public de l'Union européenne et donc c'est assez facile, y compris pour des utilisateurs non experts, de mettre à jour leur résolveur pour utiliser ce type de résolveur public. Diapo suivante.

Si vous avez utilisé des services de streaming ces derniers jours, vous avez vu qu'il y a des publicités par rapport à ce type de résolveur. Parfois, ils passent par des VPN, parfois pas, et ils fournissent un certain nombre de services. Ils donnent plus de protection et d'anonymisation, mais ils sont conçus pour contourner des restrictions géographiques. Par exemple, si vous voyagez et que vous souhaitez regarder une série qui passe dans votre pays, vous pouvez donc mettre en route votre VPN et cela va contourner les restrictions géographiques liées au pays où vous êtes. Si vous êtes dans un pays et que vous voulez accéder à des contenus qui ne sont pas accessibles dans ce pays-là, vous pouvez

utiliser le VPN pour accéder aux contenus dans le pays où ces contenus sont disponibles. J'ai cinq minutes. D'accord.

Alors, qu'est-ce que cela veut dire? Donc, le fait d'utiliser différents résolveur dans les différents pays, cela vous permet de contourner un blocage DNS s'il y en a un. Vous pouvez juste changer, mettre en route un VPN pour le faire. Diapo suivante, s'il vous plaît.

MAARTEN AERTSEN

Qu'est-ce qui peut se passer mal? Le sur-blocage intervient lorsque ce blocage est trop vaste. Par exemple, vous pouvez bloquer un nom de domaine de troisième niveau qui est beaucoup plus précis que de bloquer un deuxième nom de domaine de second niveau ou de premier niveau. Si ce blocage est trop vaste, il peut couper l'accès à plus d'une destination, à plus d'un site web, et cela va créer des désagréments pour les visiteurs qui se rendent sur ces sites Web.

Cela a lieu souvent lorsque l'on bloque le mauvais site. On a beaucoup d'exemples. Si vous voulez des exemples, des détails, je vous suggère de lire les études de cas. Par exemple, l'Italie a un système qui distribue certains noms de domaine à leur réseau de diffusion de contenu et à leur FAI. Et par accident, ils ont bloqué un domaine qui est utilisé au niveau de l'infrastructure et donc ce sur-blocage a bloqué Google Docs par exemple pour les utilisateurs en Italie pendant un court moment jusqu'à ce qu'ils se soient rendu compte de cette erreur. Cette erreur a créé des désagréments pour

les utilisateurs qui ont souhaité utiliser ce service. Donc voilà des dommages collatéraux qui peuvent être associés à ce sur-blocage.

Comme Warren l'a bien dit, les gens peuvent contourner le blocage. Lorsqu'il se produit un blocage, on doit faire l'hypothèse qu'il y aura des utilisateurs qui vont contourner ce blocage, notamment s'ils veulent vraiment le faire, car ils peuvent changer de résolveur. Et il y a des technologies qui aident les personnes à accéder toujours à des contenus ou à rendre des contenus toujours disponibles. Le blocage DNS est toujours une question d'échelle. On peut faire l'hypothèse que si l'on bloque un domaine et que l'on envoie un ordre aux FAI du pays, le problème sera réglé pour un certain nombre d'utilisateurs, mais pas pour tous.

WARREN KUMARI

Diapo suivante. Quand un domaine est bloqué, le résolveur peut donner deux réponses. Une réponse, c'est que le domaine n'existe pas. Mais ce que l'on voit également, c'est que le résolveur vous redirige vers un autre site et on voit une augmentation de ce type de réponse et c'est assez dangereux. Pourquoi?

Si l'utilisateur veut accéder à un site, par exemple food.com, et qu'il est redirigé ailleurs, le navigateur va vous dire : Vous êtes en train d'accéder à ce site web, mais le résolveur n'est pas celui qui vous permet d'accéder et vous devez cliquer sur ces messages. Et cela a des implications au niveau de la sécurité, parce qu'on vous apprend à ignorer ce type d'alerte et donc la prochaine fois que cela va se produire, il se pourrait qu'il ne faille pas ignorer cette

alerte. Et donc ce n'est pas recommandable de rediriger et de faire de la redirection si vous utilisez le blocage DNS.

Comme nous l'avons dit à plusieurs reprises, le blocage DNS est un outil. Et comme tout outil, notamment des outils puissants, ils peuvent être utilisés pour le bien. Mais si vous ne comprenez pas vraiment comment cela fonctionne et que vous ne voyez pas les instructions, vous pouvez vous faire mal vous-même. Donc, si vous souhaitez mettre en place le blocage DNS, assurez-vous que vous comprenez bien comment cela fonctionne et quels peuvent être les dommages collatéraux associés. Diapo suivante, s'il vous plaît!

MAARTEN AERTSEN

Deuxième recommandation du SSAC. Si on va ordonner un blocage, cela peut être au sein d'une société. Cela peut être un FAI individuel. Cela peut être au niveau national. Ces directives doivent être suivies. Ces directives sont basées sur la recommandation de ne pas faire mal.

Il faut comprendre si le blocage DNS répond vraiment à vos objectifs, il peut y avoir d'autres moyens de résoudre votre problème. Par exemple, si vous bloquez, il y aura des utilisateurs qui vont pouvoir contourner le blocage. Est-ce que cela va vous aider? Ou bien ce ne sera pas suffisant? Deuxième recommandation. Il faut avoir une politique claire par rapport à ce que vous allez bloquer et comment vous allez le faire. Il faut avoir des procédures claires et précises pour voir ce qui figure dans une liste de blocage afin de minimiser les risques. Il faut comprendre

comment corriger une erreur. Nous ne recommandons pas des politiques spécifiques ou des procédures spécifiques, parce que tout cela dépend de vos objectifs, mais c'est un principe très important.

Troisième. La mise en œuvre doit minimiser le sur-blocage ou des dommages collatéraux qui pourraient porter préjudice aux utilisateurs ou aux personnes par rapport auxquelles vous avez certaines responsabilités, par exemple vos employés. Et finalement, il ne faut pas affecter les personnes qui se trouvent en dehors de vos responsabilités administratives. Ici en Europe par exemple, il y a beaucoup de pays. Certains FAI servent des personnes dans plusieurs pays. Si vous vous trouvez dans un pays A et le FAI fournit des services pour des utilisateurs dans un pays B et C, si par exemple il y a un ordre pour un blocage dans le pays A, ce blocage ne va pas affecter peut-être les gens du pays B qui ne se trouvent pas dans la même juridiction. Donc quand on voit le monde, on voit qu'il y a des frontières nationales, mais l'Internet ne fonctionne pas comme ça.

Et donc on dit ici, il faut faire attention à ne pas affecter les gens que vous n'avez pas le droit d'affecter. Dernière diapo.

WARREN KUMARI

Dernière recommandation au niveau des serveurs récursifs. Nous recommandons d'utiliser donc ce type de code d'erreur pour éviter

des problèmes. Et bien sûr, nous arrivons à la fin de la présentation et nous sommes prêts à répondre à vos questions.

MARCO HOGEWONING

Merci beaucoup! Il ne nous reste pas beaucoup de temps. C'est excellent ce travail que vous faites et nous apprécions énormément ces présentations. Nous n'avons pas beaucoup de temps, mais je pense que nous pourrions prendre une dernière question. Est-ce qu'il y a une personne qui souhaite faire des commentaires? La Papouasie-Nouvelle-Guinée.

RUSSEL WORUBA

En tant que pays, nous avons été invités à participer à des essais relatifs au DNS protecteur et je me demandais si c'était celui-ci.

MAARTEN AERTSEN

Alors oui, on peut protéger par le biais du blocage. Par exemple, les résolveurs publics fournissent des services de noms de domaine protecteurs. Ils bloquent les logiciels malveillants et l'hameçonnage pour protéger leurs utilisateurs. Donc c'est une technique qui peut être utilisée pour protéger les internautes. Ce document a déjà été utilisé pour éclairer des décisions politiques qui font actuellement l'objet de discussions au Japon, où l'on envisage de bloquer un type de contenu très spécifique dans le pays.

WARREN KUMARI

Brève mise à jour. Cloudflare est une organisation qui fournit des résolveurs publics et il y a au moins trois adresses différentes. Donc il y a notre adresse IP 1.1.1.1 où il n'y a pas du tout de blocage. Puis il y a 1.1.1.2 qui bloque les logiciels malveillants. Puis ils ont 1.1.1.3 qui est un DNS plus protecteur, qui bloque les logiciels malveillants et les contenus adultes.

Le SSAC peut-être. C'est simplement ma perspective. Mais s'il y a un service DNS protecteur offert à un grand groupe, il faut pouvoir choisir le niveau de protection. Donc si vous êtes un parent, vous voulez peut-être utiliser un service DNS protecteur qui bloque le contenu adulte. Mais si vous êtes un adulte, vous voulez peut-être consulter un tel contenu. Donc il faut pouvoir choisir quel niveau de protection l'on veut avoir. Il y a différents types de blocage. Il y a différents sous-groupes de population qui sont touchés. Peut-être que vous avez choisi vous-même d'avoir la protection. Et dans ce cas-là, c'est un peu plus durable, du moins plus durable que si c'est une protection qu'on vous a imposée.

MARCO HOGEWONING

J'ai trois personnes qui souhaitent prendre la parole. Ce sont les trois dernières questions. Une minute pour chaque question. DRC.

BLAISE AZITEMINA FUNDJI

Alors, je suis Blaise de la République démocratique du Congo. J'ai une préoccupation relative au VPN. Alors je suis très reconnaissant de la sécurité que peuvent fournir des outils DNS de ce genre tels

que les VPN. Mais d'un point de vue de politique publique, je suis préoccupé pour ce qui est de la délocalisation dans des pays en voie de développement. Les internautes utilisent les VPN, pas pour la sécurité et la stabilité, mais simplement pour naviguer dans une autre région géographique. Et ça, ça peut être parfois une violation des politiques nationales.

Il y a des plateformes de streaming qui ont trouvé des solutions particulières. Elles interdisent toute connexion par le biais de VPN, tout simplement. Donc voilà quel peut être l'équilibre aménagé entre la sécurité et la fiabilité, mais également votre implantation géographique?

MAARTEN AERTSEN Je ne pense pas que le SSAC a pris en compte toutes les répercussions de cela. Bon. La réalité est que les VPN sont utilisés de par le monde à de bonnes fins et à de mauvaises fins. Les criminels utilisent les VPN pour se dissimuler. Les VPN tirent parti de la façon dont fonctionne l'Internet, donc ils ne vont pas nous quitter. Certaines entreprises ont des listes d'adresses IP de VPN connus et ces entreprises utilisent ces listes pour évaluer le risque résultant du trafic provenant de ces adresses. Donc, il y a des outils pour détecter et comprendre le trafic venant des VPN.

WARREN KUMARI Les VPN sont conçus pour prendre la forme habituelle du trafic Internet. Donc pour certains sites, pour certains pays, il y a un

blocage des VPN. Donc ces pays où ces sites sont en mesure de bloquer les grands services VPN. Mais dans ce cas-là, les utilisateurs pourraient utiliser un VPN qui est de plus faible envergure, mais qui est peut-être plus risqué pour eux. Donc parfois, il y a des conséquences au blocage de techniques qui permettent aux utilisateurs d'accéder au contenu qu'ils souhaitent consulter, car ces utilisateurs pourraient utiliser des outils qui sont plus risqués pour eux.

MARCO HOGEWONING Alors il y a l'Inde désormais.

SUSHIL PAL Pensez-vous que le DNS, soutenu par le gouvernement, offre des avantages par rapport au DNS public? J'ai une autre question. Je pense que les VPN jouent un rôle important, en tout cas s'ils sont des VPN reconnus. Je sais qu'il y a des agences chargées de la sécurité qui se penchent sur la façon dont on peut suivre des VPN inconnus. Le font-elles, ces agences?

MAARTEN AERTSEN DNS4EU, sur leur site Web, fait valoir que c'est un effort de défense de la souveraineté plutôt que d'envoyer du trafic vers des grands résolveurs publics. Eh bien, l'Europe veut garder le trafic Internet en Europe. Je pense que l'intention est clairement stipulée. Pour ce qui est des agences responsables et des questions de sécurité,

prennent-elles des mesures pour suivre les VPN inconnus? Je ne sais pas.

MARCO HOGEWONING L'Indonésie. Dernière question.

ASHWIN SASONGKO SASTROSUBROTO Alors je voudrais que vous me parliez d'un point lié au blocage. Si nous choisissons de restreindre notre cyberespace à certains DNS, peut-être que l'on peut autoriser certaines adresses IP, point ou certains domaines de premier niveau, .org ou .com, etc. Peut-être que l'on pourrait tout bloquer et seulement autoriser des connexions avec une préapprobation.

WARREN KUMARI Je ne sais pas si c'est faisable. On a des millions de sites sur internet et avoir une liste de ce qui est visible, ce serait compliqué. Mais même si vous voulez faire cela, c'est difficilement faisable d'un point de vue technique de bloquer tout accès au DNS. Il y a beaucoup de nouvelles technologies, il y a DNS Over Quick, DNS TLS, et parfois on ne sait même pas si ces requêtes sont des requêtes DNS. C'est tout simplement du trafic internet qui prend une forme habituelle. Donc la seule chose que vous pourrez faire, c'est simplement bloquer tout l'accès à l'Internet dans votre pays. Donc en fait, ce serait déconnecter l'Internet de votre pays et interdire Starlink ou d'autres fournisseurs satellites. Si vous vous connectez sur l'Internet, il y aura du trafic DNS.

MAARTEN AERTSEN Les technologies mentionnées par Warren sont des technologies relatives au chiffrement qui sont conçues pour protéger l'identité de l'individu qui formule une requête. Ces technologies visent à garantir un plus haut niveau de confidentialité sur l'Internet.

MARCO HOGEWONING Merci, merci! C'est un sujet très intéressant. Je vois qu'il y a beaucoup de questions. Donc il y aura sans doute une réunion de suivi. À l'écran, le code QR pour le rapport, vous pouvez lire ce rapport. Il est publié depuis un moment. Cela dit, merci Greg, Ram, Warren, Maarten pour rester parmi nous. Mais sans plus attendre, je voudrais donner la parole à notre invité Cristian Hesselman pour que l'on parle d'informatique quantique et des risques que cela pose. Donc Cristian Hesselman de SIDNLabs va nous parler de l'incidence du chiffrement post-quantique sur le DNSSEC et nous parler de ce que nous, gouvernements, nous pouvons faire.

RAM MOHAN Alors avant, je voulais que nous remercions le GAC au nom du SSAC. Nous accordons beaucoup de valeur à notre collaboration et nous espérons pouvoir poursuivre cela. Merci.

MARCO HOGEWONING Christian.

CRISTIAN HESSELMAN

Merci Marco. Alors comme Marco l'a dit, nous allons parler d'informatique quantique et du DNS et de l'incidence potentielle de ces ordinateurs quantiques. Alors j'ai inclus quelques mesures que le GAC pourrait prendre, du moins d'un point de vue gouvernemental. Alors je vais continuer à parler, tout simplement. Alors ce que vous avez vu, c'est une image que j'ai récupéré du centre de l'informatique de Leibnitz où ils travaillent sur ces ordinateurs quantiques. Bon. Ils sont toujours en phase expérimentale, mais ce n'est pas non plus de la science-fiction. Donc voilà, on parle de recherche à long terme.

Alors, qu'attend-t-on des ordinateurs quantiques? Alors je veux le dire tout de suite, je ne suis pas un expert en ordinateurs quantiques. Je suis un expert en systèmes distribués. Les ordinateurs quantiques sont une question qui relève de la physique et je ne suis pas un physicien. En tout cas, c'est ce que je vous dis. Ça vient de la littérature que j'ai pu lire. Donc il y a des nouvelles applications pour l'informatique quantique telles que l'identification de nouvelles méthodes de création de médicaments. Il y a de l'apprentissage automatique.

Et comme Greg l'a dit, on peut utiliser la technologie de façon différente. Donc c'est comme le marteau dont parlait Greg. On peut l'utiliser de façon positive, mais également négative. Donc il y a des risques résultant de l'informatique quantique. Alors quel est le désavantage de l'informatique quantique?

L'informatique quantique pourrait saper nos systèmes de chiffrement algorithmique actuels, notamment pour le DNSSEC, système que l'on utilise pour authentifier les messages DNS et pour contrôler l'intégrité de ces messages. Un instant.

Alors, quels sont les risques de l'informatique quantique pour le DNSSEC? Il pourrait saper les algorithmes de chiffrement que le DNS utilise pour vérifier l'authenticité et l'intégrité des réponses DNS. Potentiellement, un adversaire pourrait attribuer une signature compromise à un message DNS et envoyer des internautes sur un mauvais site ou des composantes logicielles pourraient se retrouver sur le mauvais site.

Moi, je pars du principe que l'on vit déjà dans une ère post-quantique. Et il ne faut pas se dire que l'on va stocker maintenant des données, les déchiffrer plus tard, non. Maintenant, on peut les déchiffrer en temps réel grâce à l'informatique quantique. Les experts pensent que cela ne va pas se produire d'ici 10 à 15 ans. Donc vous vous demanderez peut-être pourquoi l'on doit plancher sur ce sujet maintenant.

Remplacer les algorithmes de chiffrement dans le DNSSEC, cela prend beaucoup de temps. Voici un graphique tiré d'un article scientifique où l'on voit le développement d'un algorithme de chiffrement dans le DNSSEC. Donc du premier projet d'algorithmes jusqu'à son déploiement, on voit que ça prend environ 10 ans. C'est une caractéristique classique de la mise à jour des infrastructures et il en va de même pour ces algorithmes DNS. Donc, si les

ordinateurs quantiques se matérialisent dans 10 à 15 ans, il faut que l'on réfléchisse aujourd'hui à ce que l'on peut faire pour le DNS.

Outre le calendrier, on déploie actuellement beaucoup de mesures pour le DNSSEC. On voit ici à gauche les pays qui ont signé leur ccTLD avec du DNSSEC. En vert et en bleu, on voit les pays qui l'ont fait – 48 % du monde. À droite, c'est la validation. C'est un peu plus rouge ici, car la validation de ces signatures est moins répandue. Il y a toujours des éléments à améliorer, mais vous pouvez le constater, il y a un déploiement conséquent du DNSSEC actuellement. C'est quelque chose que l'on fait de pair avec l'informatique quantique notamment, car la validation devrait augmenter à l'avenir et la signature également.

Si vous souhaitez protéger le système de nom de domaine de l'utilisation malveillante de l'informatique quantique, il y a trois stratégies selon nous. Remplacer, repenser et retirer. Donc on remplace l'algorithme de chiffrement existant avec un nouvel algorithme, des algorithmes prêts à l'ère post-quantique. Repenser, cela veut dire complètement repenser le système de la sécurité du nom de domaine. Et la troisième option, c'est se débarrasser tout simplement de la sécurité du système de nom de domaine, le DNSSEC.

Ces trois approches ont des avantages et des inconvénients. Par exemple, la stratégie de remplacement est plutôt simple à mettre en œuvre, mais il y a des risques opérationnels et je vais en parler un peu plus un peu plus tard. Repenser l'approche, c'est partir de

zéro. Peut-être utiliser de nouvelles technologies telles que des arbres dits Merkle. Cela réduirait le risque opérationnel, mais il faut repenser tout le système DNSSEC et le protocole. Donc cela prendrait du temps.

Puis le retrait total. Cela peut sembler facile, mais cela peut avoir une incidence, car si vous retirez le système DNSSEC, vous ouvrez le DNSSEC à toute une série de nouvelles attaques qui, habituellement, sont entravées par le DNSSEC, et donc vous pourriez avoir une incidence également sur les protocoles. Donc le SIDNLab, mon organisation a opté pour la première option, le remplacement envers. Donc je vais vous parler de cette approche.

Ne vous inquiétez pas, je ne vais pas vous expliquer ce graphique. Vous voyez ici les interactions qui prennent place entre un résolveur et un serveur de noms faisant autorité avec des messages DNSSEC qui sont diffusés à l'écran. Ici donc, on a les badges jaunes et rouges. Ce sont des messages qui ont des éléments clés, des signatures ou des clés publiques, et donc ce sont ceux-ci qui doivent être remplacés.

Je vais vous donner un avant-goût de ces signatures. Voici deux exemples. En haut à gauche, une clé publique. Donc c'est une clé que nous utilisons actuellement dans le DNSSEC qui est à droite, c'est la signature générée par cette clé. Et en bleu, c'est une clé publique et une signature qui sont créées par un algorithme post-quantique. Donc c'est un algorithme qui est censé nous protéger de l'informatique quantique et donc vous voyez que cette clé est

considérablement plus longue. Donc vous voyez ce que peut prendre cette nouvelle approche d'un point de vue technique.

Prochaine planche. Donc il y a plusieurs algorithmes prêts pour l'ère post-quantique, notamment dans la zone NIST PQC. Donc, c'est l'Institut national des normes et de la technologie aux États-Unis. Donc, ils ont créé un concours pour les cryptographes pour qu'ils créent des algorithmes résistants à l'informatique quantique. Donc on a expérimenté avec quelques-uns de ces algorithmes. Donc il y a MAYO, Falcon et SQSign.

Donc les noms sont un peu étranges et il y en a encore d'autres. Donc on a mené quelques expériences avec ces algorithmes et on a pu valider le temps que cela prend pour signer un dossier zone, notamment le mail pour valider les archives DNS. Puis on s'est penché sur la taille des signatures et la taille des clés, car vous avez vu la différence de taille sur la planche précédente. Ici, vous pouvez voir comment il faut arriver à un compromis parce qu'il faut considérer les aspects, par exemple de taille si vous utilisez des tailles plus petites, vous aurez un résultat différent que si vous utilisez des clés d'une taille plus importante.

Diapo suivante, s'il vous plaît! Vous voyez le dernier test que nous avons mené pour la zone .nl. Nous avons essayé de signer. Nous avons signé la zone avec deux algorithmes post-quantique. Je ne vais pas rentrer dans le détail, mais comme vous le voyez ici, cela prend deux fois plus de temps de signer la zone avec les algorithmes SPQC. Habituellement, c'est 10 minutes. Et cette fois-

ci avec ces algorithmes post-quantiques, cela a pris 20 minutes. Voyez donc les résultats qui sont assez bons du point de vue opérationnel. Diapo suivante.

C'est ici notre situation actuelle. Voilà où nous en sommes. Nous avons identifié des éléments que nous voudrions examiner à l'avenir. La plupart de ces éléments concernent la taille des clés publiques que nous utilisons et nous aimerions également étudier les délais de validation dans les résolveurs de manière plus détaillée pour voir quel est le rôle que joue le cache.

Ma dernière diapo concerne des mesures suggérées pour le GAC. Vous pourriez peut-être travailler avec NIST. C'est une agence du gouvernement des États-Unis qui se penche sur l'alignement des algorithmes post-quantique. Par rapport à certaines exigences du DNS, on pourrait intensifier le développement des logiciels libres et à code source ouvert qui sont présents dans l'infrastructure du DNS. Cela pourrait être fait par exemple par le biais des fonds des organisations qui fournissent des fonds de financement.

Une autre mesure qui pourrait être prise, c'est la simulation de déploiement de ce type d'algorithmes, comme on a fait pour le .nl, pour vérifier donc les différents schémas, pour vérifier à quel point votre domaine est préparé à mettre en place ce type d'algorithmes. Et finalement, nous devons mener davantage de recherches par rapport à l'impact opérationnel de ces algorithmes post-quantiques et ce que cela représente pour les opérateurs du DNS et pour le DNS. Diapo suivante, s'il vous plaît.

Le logiciel que nous avons développé. Pardon. Les tests que nous avons menés utilisent un logiciel à code ouvert que nous avons développé et donc vous retrouverez ces informations si vous cliquez sur le QR Code. Si vous avez des questions, n'hésitez pas à me les poser.

MARCO HOGEWONING Merci beaucoup pour cette présentation. Ma conclusion, c'est que nous avons beaucoup à réfléchir du point de vue des gouvernements. Le DNS représente donc une opportunité également pour des gouvernements. Le gouvernement des Pays-Bas a mené certains tests, comme vous l'avez vu, et donc nous devons travailler là-dessus. J'ai deux questions. Je vois deux personnes qui souhaitent prendre la parole.

BARRY LEIBA Barry Leiba de SSAC. Je voulais préciser un élément, car à chaque fois que l'on parle de cryptographie post-quantique, je pense qu'il y a un élément qui doit être souligné. Il y a cette idée que la cryptographie post-quantique met en péril toutes les cryptographies. Il s'agit d'un chiffrement qui est utilisé. Le chiffrement que nous utilisons pour le trafic Internet n'est pas en péril. On parle ici du chiffrement post-quantique pour un type de chiffrement qui est utilisé pour le DNSSEC, qui est très particulier.

CRISTIAN HESSELMAN Le DNS a des exigences très précises et dans nos cas d'utilisateurs, nous nous nous penchons sur ces critères qui sont très spécifiques.

MARCO HOGEWONING Merci beaucoup.

PETER THOMASSEN Je fais partie du SSAC. Je voulais parler des chiffres du DNSSEC qui sont assez faibles. Mais si on considère le DNSSEC dans des chiffres absolus, c'est plus de 10 millions de domaines, ce qui est assez important. On ne sait pas encore quelle sera la méthode future de signature si l'on utilise les méthodes post-quantiques, mais il y aura une utilisation post-quantique. Peut-être qu'à l'époque où l'on fera la transition, ce nombre de domaines augmentera et il faudra peut-être avoir recours à l'automatisation.

Dans les pays qui étaient en bleu, les ccTLD Unités sont en mesure de soutenir ce type de changement. Donc il faut voir si les différents pays souhaitent soutenir cette transition qui pourrait être automatisée. Et donc, si cela vous intéresse, n'hésitez pas à me contacter ou à contacter d'autres membres du SSAC.

CRISTIAN HESSELMAN C'est un point important.

MARCO HOGEWONING Nous avons un peu de temps encore s'il y a des questions. Nico, le président du GAC.

NICOLAS CABALLERO Merci beaucoup et merci pour cette présentation, excellente présentation. Ram et ton équipe, c'est toujours un plaisir de vous avoir ici. Deux éléments très rapides. Ram, Cristian, j'aimerais bien profiter du fait que Jim Galvin est présent pour préparer une présentation pour le conseil d'administration à Muscat. C'est pour le mois d'octobre. Car il est probable que nous devions présenter une version allégée peut-être de ces informations à certains membres du conseil d'administration qui sont plus intéressés dans les aspects techniques.

Et puis, je profite du fait que je suis à côté de mon collègue du Brésil pour vous dire que nous organisons un atelier de renforcement des capacités dans notre région. Les détails sont encore à définir. Donc, avant ou après Oman, est-ce que vous pourriez nous aider avec cela? Nous voudrions parler de la mise en œuvre DNSSEC, un aperçu très court de la cryptographie, chiffrement symétrique/asymétrique, RSA. Il y a deux ou trois semaines apparemment – je ne sais pas si c'est sûr ou pas, mais apparemment le RSA a eu des difficultés. Je ne sais pas, c'est à valider ou à confirmer.

Mais on sait qu'il y a beaucoup d'avantages pour les gouvernements à utiliser les logiciels libres et à code source ouvert. Moi, j'utilise beaucoup ce type de logiciel, mais j'ai du mal à

	expliquer de manière simple à des personnes qui n'ont pas une formation technique quels sont les avantages du point de vue technique mais aussi du point de vue économique les bénéfices de GPL-3, etc.? Donc j'aimerais savoir si vous pouvez nous aider pour que nos efforts soient couronnés de succès. Donc voilà deux éléments : présentation pour le conseil d'administration et ensuite nous aider pour organiser notre atelier de renforcement des capacités régionales pour les pays de l'Amérique latine. Cet atelier pourrait avoir lieu à Sao Paulo ou Brasilia.
RAM MOHAN	Merci beaucoup. Nous serons ravis de vous aider. N'hésitez pas à revenir vers moi. Nous allons bien sûr vous aider.
MAARTEN AERTSEN	Oui, pareil pour moi.
NICOLAS CABALLERO	Par rapport au RSA et au problème qu'il y a eu au niveau du RSA?
WARREN KUMARI	Je pense que vous parlez d'un problème qui figure dans un document qui a été publié récemment où l'on dit que le RSA avait un problème, qu'on avait cassé le code du RSA. Mais cela n'est pas encore arrivé. Donc c'était une estimation de la puissance quantique dont vous auriez besoin pour construire un système qui soit fiable.

Et donc le document dit que vous n'avez pas besoin d'autant de puissance quantique que l'on pensait au tout départ. Mais ce n'est pas encore un problème par rapport auquel il faut s'inquiéter pour le moment. Ce n'est pas que le RSA a été cassé, mais dans un certain nombre d'années, on pourrait le casser. Mais l'estimation actuelle, il y a un document que je ne retrouve pas en ce moment où l'on dit qu'il faudrait donc une puissance X qui change en fonction des experts qui se penchent dessus. Mais pour le moment, c'est très difficile à prévoir. On pense que ça pourrait avoir lieu dans quelques années, mais c'est comme la fusion, à un moment donné, l'énergie par fusion va venir, mais on ne sait pas encore quand. Bien sûr qu'il vaut mieux être préparé parce que toute cryptographie peut être cassée. Il faut se préparer pour cela.

NICOLAS CABALLERO Vous réparez votre toit quand il ne pleut pas, n'est-ce pas?

MARCO HOGEWONING Merci beaucoup. Il nous reste que deux minutes. Je vois une main levée de l'Australie. On va donc donner la parole à Australie.

INGRAM NIBLOCK Je me demande… J'ai une question par rapport à la diapo où vous montrez les avantages et les inconvénients des différents chiffrements. Et je comprends bien le problème de taille de la clé. Je voulais savoir si cela a un effet sur le délai de signature par exemple si on passe de deux minutes à 10 minutes. Est-ce que cela

représente un problème? Est-ce que si cela doit être fait très souvent, cela peut devenir un problème au niveau du DNS?

CRISTIAN HESSELMAN Nous avons 6,2 millions de domaines dans notre zone et la fenêtre de publication pour la re-signature, c'est 30 minutes, c'est-à-dire que nous devons resigner toutes les 30 minutes. Si ce délai de signature était trop long, on n'aurait pas le temps de le faire. Il y a un impact.

MAARTEN AERTSEN Cela dépend du modèle de déploiement. Christian parlait d'un modèle de déploiement qui concerne toute la zone, mais il y a des modèles où il y a une signature progressive ou une signature légère par partie de la zone. Donc c'est difficile de répondre à cette question de manière générale, mais disons que la vitesse compte.

PETER THOMASSEN Plus ça prend de temps à signer, plus il faut modifier le modèle.

MARCO HOGEWONING J'espère que cela répond à votre question. Nous n'avons plus de temps. Je suis ravi qu'on ait déjà des dates pour poursuivre cette discussion. N'hésitez pas à contacter les intervenants pendant la pause-café si vous souhaitez obtenir des informations plus détaillées. Merci beaucoup, Ram, Warren, Greg, Maarten et Cristian pour ces informations précieuses que vous avez partagé avec nous

pour nous aider à mieux comprendre ce qui se passe. Avant de passer au café, je vous dis qu'après le café dans une demi-heure, nous allons parler DNS et exactitude des données d'enregistrement. J'espère vous revoir dans une demi-heure pour tout le reste. J'espère que cela a été intéressant et profitez de la pause-café.

[FIN DE LA TRANSCRIPTION]