ICANN83 | Foro sobre políticas – Sesión del GAC sobre seguridad y estabilidad
Miércoles, 11 de junio de 2025 – 9:00 a 10:15 CEST

DANIEL GLUCK

Bienvenidos a la sesión del GAC sobre seguridad y estabilidad de la ICANN83 hoy miércoles 11 de junio a las 7:00 UTC. Tengan en cuenta que esta sesión se está grabando y se rige por los estándares de comportamiento esperados de la ICANN y la política antiacoso de la comunidad de la ICANN.

Durante esta sesión las preguntas o comentarios solamente se leerán en voz alta si se presentan de la manera adecuada en el chat de Zoom. Habrá interpretación en los seis idiomas de Naciones Unidas más portugués. Si desean hablar durante la sesión levanten la mano en la sala de Zoom. Cuando digan su nombre, los participantes podrán habilitar el micrófono en Zoom. Digan su nombre para los registros y el idioma en el que hablarán cuando no sea inglés. Por favor, hablen a un ritmo razonable para permitir una interpretación correcta. Ahora le doy la palabra al vicepresidente del GAC, Marco Hogewoning. Gracias. Le doy la palabra.

MARCO HOGEWONING

Gracias, Dan. Buenos días. Hoy voy a estar presidiendo esta sesión porque nuestro presidente, Nico, está disfrutando de un café, ocupado. Vamos a hablar de alguno de los proyectos que está haciendo el SSAC. Tenemos también a Cristian Hesselman, de

	SDNLabs para explicarnos cómo la computación cuántica interactúa con DNSSEC. Antes de comenzar quizá podamos hacer una breve ronda de presentaciones para que sepan quiénes están aquí en la mesa. Yo soy Marco Hogewoning, vicepresidente, de Países Bajos.
MAARTEN AERTSEN	Buenos días. Soy Maarten Aertsen. Soy miembro del SSAC.
WARREN KUMARI	Hola. Soy Warren Kumari, también miembro del SSAC.
GREG AARON	Soy Greg Aaron, del SSAC.
RAM MOHAN	Soy Ram Mohan, también del SSAC. Presidente del SSAC.
CRISTIAN HESSELMAN	Cristian Hesselman, de SIDNLabs, que es el registro para el dominio de primer nivel de Países Bajos, .NL.
MARCO HOGEWONING	Muy bien. Le damos la palabra a Ram, para los primeros comentarios.

RAM MOHAN

Muy bien. Vamos a empezar a hablar un poquito del acceso a los datos de registración de dominios. ¿Qué queremos hacer? Queremos asegurarnos de compartir con el GAC nuestro objetivo. Queremos asegurarnos de que toda política correspondiente al acceso a los datos de registración de los gTLD esté bien definida, sea robusta y que cubra las necesidades de la comunidad global de Internet y que la proteja de las amenazas a la seguridad. Esto lo podemos lograr con un sistema de acceso que siga una estructura con un mecanismo expeditivo que permita manejar los pedidos de información, sobre todo los urgentes, de manera expeditiva, que las políticas en cuanto a tiempos de respuestas, el cómo, el qué y el dónde estén claramente definidas y sean aceptadas dentro de la comunidad.

También creemos que en la organización de la ICANN debería seguir compartiendo indicadores sobre las solicitudes de datos que llegan para pedir datos de registración de dominios. Creemos que el acceso a los datos de registración es importante. Es algo fundamental dentro de la seguridad y la estabilidad. Nosotros le dimos nuestra opinión al EPDP, que se ocupa de esta materia pero queremos decir que esta no es un área que esté en conflicto con las necesidades en términos de privacidad.

Tenemos las necesidades de privacidad abordadas de la manera correcta pero hay también una inquietud que tiene que ver con la seguridad y la estabilidad que es clara y queremos asegurarnos de que el proceso a través del cual se realizan estas modificaciones en la comunidad tengan en cuenta los principios que ustedes ven aquí

enumerados en esta pantalla. Eso es realmente lo que queremos decir. Quedamos a disposición para preguntas o comentarios.

MARCO HOGEWONING Gracias, Ram. Creo que el GAC está alineado con lo que usted expresó sobre el acceso a los datos de registración. ¿Hay alguna pregunta? Todavía es temprano. No veo ninguna mano levantada aquí en la sala ni tampoco en Zoom. Tal vez podemos continuar con el próximo tema que creo que hace referencia al software de código abierto. Maarten.

MAARTEN AERTSEN Estamos trabajando en un tema que puede ser familiar para algunos de ustedes que es el software libre y de código abierto. El software que se puede utilizar de manera libre, se puede compartir modificar o incluso estudiar. Estamos tratando de determinar el rol de este tipo de software dentro del DNS global.

Hemos pensado que dependemos mucho de esto pero no hay un estudio exhaustivo disponible para esta comunidad. Este software libre y de código abierto tiene algunas características en cuanto a su desarrollo y a su gobernanza. Si bien en distintas partes del mundo las personas discuten sobre la infraestructura, el software y la confiabilidad, nosotros creemos que es importante hacer visible la función de este software, sus características, para asegurarnos de que cuando haya un debate en materia de políticas, se tenga en cuenta esto.

Este trabajo entonces tiene dos objetivos. Queremos dar visibilidad a esta dependencia crítica y también queremos que las características de este software sean visibles e informar alguna de las suposiciones que nosotros normalmente hacemos sobre el software en general pero que tal vez no se apliquen necesariamente a este tipo de software.

Esta es una presentación para adelantar lo que viene después. Básicamente nos concentramos en cuatro áreas con una encuesta para describir el estado de situación, ver qué pasa del lado de la registración de dominios y también del lado del DNS donde se publican y se recuperan mapeos para tener una idea de cómo está la situación ahora. También analizamos las características de este software, incluso el modelo de desarrollo que no es el mismo que se utilizaría para bienes físicos u otro tipo de software. Luego, contrastamos este análisis del software libre y de código abierto en cuanto a sus características con el software popular en DNS. Aquel que nos preocupa en este contexto.

La tercera parte tiene que ver con aclarar algunos supuestos que nosotros aplicamos en la práctica, que tal vez no son viables aquí y aclarar si hay algún concepto errado. Luego tratamos de enumerar los factores de riesgo que pueden ser pertinentes y que tienen que ser considerados al formular políticas o reglamentaciones. Tienen que ver con desarrollo pero también con las operaciones de este software. Básicamente estas son las áreas en las que nos estamos concentrando. En Muscat esperamos contarles más al respecto

porque esperamos publicar este informe en los meses posteriores a esta reunión de hoy.

A modo de adelanto, les quiero decir que creemos que el uso del software libre y de código abierto en el sistema de nombres de dominio y con los registros es una fortaleza pero también queremos ofrecer algunas pautas generales respecto del uso de este tipo de software para también considerar sus riesgos. Quedo a disposición para cualquier pregunta.

MARCO HOGEWONING Fue un adelanto breve, conciso. ¿Hay alguna pregunta para Maarten sobre este trabajo? India levantó la mano.

SAJID Gracias, señor Presidente. Esta es una pregunta para Ram Mohan. Compartió los objetivos de que los datos de registración deberían estar disponibles en un plazo de 24 horas pero ya hace dos años que estamos tratando de que se acuerde aquí este plazo. Por el momento no tenemos ninguno acordado. Si bien se establece la urgencia, se ha mencionado en reiteradas oportunidades, tanto en el GAC como en el SSAC. Este es un proceso muy extenso que va por el camino de la autenticación por un lado y de la política por el otro. ¿Qué piensa como presidente del SSAC? La pregunta también es pertinente al vicepresidente del GAC. ¿Podría haber una declaración conjunta de ambos comités respecto de acordar un plazo para este acceso a los datos tan pronto como sea posible?

MARCO HOGEWONING Le voy a dar la palabra a usted.

RAM MOHAN Gracias por su intervención. Estamos de acuerdo en que para los pedidos urgentes de información el proceso debería estar muy claro y creo que hay ciertas deliberaciones en curso entre las partes que son responsables de implementar estos cambios. No puedo hablar en nombre del SSAC en su conjunto. Tendría que consultar con sus miembros pero hemos sido muy claros en cuanto a que si hay algo que es considerado urgente tiene que ser tratado como tal y las respuestas deben proporcionarse de manera expeditiva. No puede insumir demasiado tiempo. Si ayuda que hagamos algo en forma conjunta con el GAC, por supuesto, estamos abiertos a considerarlo, a subrayar la importancia de esta cuestión. Creemos que es un tema importante. En parte tenemos que tener en claro que lo urgente significa urgente. No es la operatoria habitual.

MARCO HOGEWONING Gracias, Ram, por esta respuesta. Estoy de acuerdo. Obviamente, como usted sabe, el GAC mencionó las solicitudes urgentes creo que en los últimos cinco comunicados, por lo menos de los que yo me acuerde. También el asesoramiento. Hay algunos colegas en los equipos reducidos que están también tratando este tema. Desde mi perspectiva vamos avanzando.

Estoy de acuerdo con su observación respecto de que las solicitudes urgentes no están avanzando con la urgencia que necesitamos pero sí, estamos alineados con Ram y tengamos esto presente y consideremos si un esfuerzo conjunto podría ayudar a que todo avance más rápidamente. En algún momento lo volveremos a ver esto. No sé si hay alguna pregunta más. Russell, adelante.

RUSSELL WORUBA

Gracias, colegas. Gracias a los colegas del SSAC, que están haciendo un trabajo excelente. Soy un seguidor del SSAC y creo que es una fuerza que recibimos con agrado. Creo que muchos de los países en las regiones subatendidas dependen enormemente del software de código abierto para manejar el DNS a nivel de ccTLD ciertamente. Ahora, con todo el panorama y los cambios que se avizoran estamos atentos a los resultados de este estudio. ¿Tendrán alguna base como para decirnos cuál es la situación en las distintas regiones? Gracias.

MAARTEN AERTSEN

Gracias por la pregunta. Le puedo dar un adelanto. Con respecto a esta encuesta del panorama actual donde tratamos de obtener datos duros de quién usa qué, creo que tenemos previsto en el borrador actual, este todavía no se va a publicar, decir que el DNS global utiliza software de código abierto así que no son solamente ustedes. Tenemos algunas estadísticas para respaldar esto.

En el espacio de los ccTLD 20 de 25 operadores principales utilizan este tipo de software. Si ustedes suman el espacio de los gTLD, 9 de cada 10. Si nos fijamos en el sistema de servidores raíz, son 9 de 12 que utilizan este tipo de software. Creo que este es uno de los valores que puede aportar este informe. Traer a la superficie para un público más amplio y aquellos que son nuevos en la tecnología que el software está en todas partes y esperamos proporcionar esta información porque en algunas regiones vimos que el software se está regulando y que este software de código abierto es como que no está tenido en cuenta. Tal vez la estrategia actual en términos de financiación tampoco es la correcta.

MARCO HOGEWONING Creo que Alemania pidió la palabra.

RUDY NOLDE Rudy Nolde, de Alemania. Originalmente quería preguntar qué consejos tenían para los formuladores de políticas de políticas porque en la última diapositiva hablaban de algunas pautas para los formuladores de políticas y creo que nos dio un adelante pero, como soy un poco impaciente, quisiera preguntarle si tal vez nos podría decir de manera preliminar en qué dirección van a ir con estas pautas para nosotros como formuladores de políticas.

MARCO HOGEWONING No les quiero robar tiempo a mis colegas pero voy a tratar de ser breve. Cómo lo estamos pensando. Queremos dejar visibles

algunos de los conceptos equivocados. Uno que es bastante natural es que se pueden utilizar las relaciones contractuales para tener un mecanismo en el ámbito de la política. Podemos decir que regulamos a los operadores de infraestructura crítica en la región pero luego se imponen requisitos a los proveedores. Los proveedores van a imponer requisitos a sus propios proveedores.

Esto puede funcionar bien para los productos físicos, a veces para el software pero no funciona cuando el software se descarga de Internet porque ahí no hay una cadena. Esta es una concepción errada. En la práctica no funciona así porque hay mucho software que se desarrolla y es mantenido por un grupo específico pero cuando se trata del uso, esto va mucho más allá de la existencia de ese contrato de soporte.

Desde el punto de vista de lo que podemos asesorar, tal vez podemos ofrecer algunos comentarios, algunas reflexiones en ese ámbito en particular. Cómo manejar los desarrolladores en este sentido pero también si le imponemos requisitos a los operadores esto podría restringir su capacidad de elegir el software que es el mejor en su clase, que tal vez podría ser este tipo de software. Tal vez no se cumpla con la política que uno espera cumplir. Vamos en ese sentido pero primero tenemos que publicar el informe y después podré hablar en mayor detalle sobre esto.

MARCO HOGEWONING Sí. Creo que vamos a esperar el informe, a esperar a la publicación y luego continuaremos con este análisis. Ahora vamos a pasar al

próximo tema, uno que me interesa muchísimo. Es el bloqueo del DNS. Lo vamos a ver desde una nueva perspectiva.

GREG AARON

Muchas gracias. Vamos a presentar dos documentos que el SSAC escribió hace 12 años y un nuevo documento que los actualiza. Nos pareció oportuno actualizar estas dos publicaciones previas porque hay muchos ejemplos acerca del bloqueo del DNS a escala mundial y vemos los resultados correspondientes. A la vez se ha desarrollado nueva tecnología que afecta al bloqueo del DNS y a cómo la gente puede acceder a recursos en Internet. Trabajamos 20 miembros del SSAC en esta iniciativa.

Veamos. ¿Qué es el bloqueo del DNS? Cuando ustedes están frente a su computadora y quieren ir a un sitio web ustedes ingresan la dirección, el nombre de dominio de ese sitio web y envía esa consulta a un resolutor del DNS o resolutor recursivo que está administrado por su ISP. Ese resolutor recursivo traduce esa dirección IP del sitio web al que ustedes quieren llegar y el DNS se da cuenta de cuál es el sitio web al cual ustedes quieren llegar y así se permite la conexión.

Normalmente este proceso es prácticamente instantáneo. Sin embargo, el resolutor recursivo puede bloquear a un nombre de dominio. Eso significa que el resolutor nos va a dar una información distinta de la esperada. Básicamente esto se hace de dos maneras. Primero, en primera instancia, el resolutor recursivo les puede decir que aquel dominio que están buscando no existe, cuando en

realidad sí existe. Por ejemplo, Wikipedia. Quieren ir a Wikipedia y no se pueden conectar a esa página. Si no, en lugar de llevarlos al sitio web que ustedes quieren visitar, se los lleva a otro destino en Internet.

El resolutor recursivo les dice algo inesperado o incluso les está mintiendo, como dicen algunas personas, porque no les da la respuesta que sí existe en el DNS. El bloqueo del DNS es una técnica, es una herramienta. Como toda herramienta, se puede utilizar con distintos fines. Se la puede utilizar de manera experta o se la puede utilizar torpemente, al igual que un martillo. Podemos utilizar un martillo para construir una cosa o para pegarle en la cabeza a alguien y eso no es deseado.

Básicamente, esta herramienta está diseñada para que la gente no pueda acceder a los contenidos o a un servicio. Esto no solo afecta a los sitios web sino también a los correos electrónicos, a la gestión de redes. Todo lo que sucede en el DNS.

Si un resolutor del DNS fuese Gandalf, estas referencias nos encantan en el SSAC, esto es lo que diría ese resolutor recursivo. No pasarán. El bloqueo del DNS se utiliza con distintos fines, con lo cual la motivación es importante. En primer lugar es utilizado con fines de seguridad. Un resolutor quizá… Disculpen. Se ha cortado la luz. Bloquearon la electricidad. Muy bien. Continúo.

Un resolutor del DNS puede estar configurado de manera tal que las personas no accedan a sitios que tienen phishing, malware. Sitios engañosos. Este es un servicio beneficioso, positivo. Todos

nosotros en cierto modo estamos protegidos por el bloqueo del DNS. Los buscadores web, por ejemplo, tienen un sistema que nos alerta cuando estamos a punto de acceder a un sitio web que comete phishing, por ejemplo.

Esto es algo endémico en múltiples sistemas y está muy presente. En general la idea es proteger y ayudar a las personas. Se hace por lo general a nivel local. Por ejemplo, ustedes quieren que una empresa los ayude con la seguridad de su red y trabajan de esta manera.

También se bloquea el DNS para bloquear contenido. Por ejemplo, su biblioteca local quizá no permita que se acceda a algunos contenidos. Por ejemplo, sitios de pornografía o sitios de apuestas, porque a esa biblioteca concurren niños. También dentro de empresas se bloquea contenido porque algunas empresas no quieren que sus empleados por ejemplo accedan a sitios web de apuestas o a sus cuentas de redes sociales mientras están trabajando en la red de la empresa. En ese caso la empresa tiene una política al respecto.

Hay algo que es muy controvertido. Utilizar el bloqueo del DNS para que la gente no acceda a contenidos, sobre todo si se bloquea el DNS a escala nacional. Por ejemplo, gente de todo un país no puede visitar tal o cual sitio web o no puede ver tal o cual contenido. Por eso queremos presentarles esta información a quienes formulan las políticas, a los miembros del GAC por ejemplo, porque estas decisiones afectan a muchísimas personas.

A veces el bloqueo se fundamenta en una ley. Algunos países, por ejemplo, no permiten que sus ciudadanos visiten sitios que tienen pornografía infantil para proteger a los niños y para proteger a los ciudadanos de ese país. Los países tienen una lista de esos dominios y son distribuidos a sus ISP pero hay algo más controvertido aún. En algunos países se bloquea el DNS para acceder a contenido que refleja opiniones políticas. Con lo cual ahí hay censura.

Queremos hacer una diferencia entre suspensión de nombres de dominio y bloqueo del DNS. En ambos casos se bloquea el acceso al contenido. Sin embargo, en el bloqueo del DNS no se elimina el contenido. Otras personas pueden acceder al mismo.

Cuando se suspende un dominio, ese dominio es retirado de Internet. Es decir, deja de funcionar en Internet y esto se hace en todo el mundo para prevenir algunos problemas o el uso indebido. Por ejemplo, el phishing. A veces estas medidas obedecen a resoluciones judiciales. Aquí vemos una imagen que indica que un sitio web ha sido incautado como resultado de una resolución judicial. A veces o se lo retira completamente o se hace un redireccionamiento del sitio web y es colocado en otros servidores de nombres pero en definitiva el objetivo es evitar el acceso al sitio.

Aquí vemos un extracto del documento. En este documento, el SSAC habla acerca de las técnicas utilizadas para bloquear al DNS, los motivos por lo cual esto se hace. En algunos casos quizá la gente no esté de acuerdo con los casos prácticos porque lo que es

legal en un país quizá no lo sea en otro. Algunas personas no estarán de acuerdo con los fundamentos de una resolución judicial en cada caso.

WARREN KUMARI

Como dijo Greg, el bloqueo del DNS es una herramienta que tiene fortalezas y debilidades. Tenemos que entender cómo funciona para justamente no quedar nosotros mismos aislados del contenido. Lo que se hace es poner listas en el resolutor recursivo de lo que se puede mostrar y lo que no.

Esto se aplica a los usuarios de ese resolutor recursivo en particular. Con lo cual, si el usuario va a otro resolutor recursivo, va a eludir este bloqueo. Aquí vemos un usuario que manda sus consultas a un resolutor estándar de su ISP. Ellos buscan un nombre y si ese nombre está aprobado se resuelve la búsqueda normalmente pero si está en una lista de bloqueo del DNS, a veces la respuesta dice que el nombre no existe o bien el resolutor recursivo nos va a redireccionar en la búsqueda. Si el usuario va a otro resolutor recursivo donde no hay bloqueo, entonces podrá acceder a ese contenido en Internet normalmente.

¿Cómo hacen los usuarios para utilizar un resolutor distinto? Hay una gran cantidad de resolutores públicos que son utilizados por una gran cantidad de usuarios. Tenemos aquí que alrededor del 21 % de los usuarios utilizan los resolutores públicos conocidos mundialmente. Aquí vemos algunos ejemplos como el DNS público de Google, luego CloudFlare tiene su propio resolutor y también

Quad9, pero también hay resolutores de los gobiernos. Por ejemplo, DNS4EU, que es un servicio público de resolutores. Esto es fácil. Incluso para los usuarios sin conocimiento técnico. Ellos pueden configurar sus resolutores y ver hacia dónde van en el DNS.

Si en los últimos años utilizaron servicios de streaming, habrán visto publicidades de VPN. Hay marcas muy conocidas en el mercado que ofertan estas VPN que nos dan beneficios, mejoran nuestra privacidad, entre otras cosas pero también en esos anuncios se deja claro que sirven para sortear las restricciones geográficas.

Si viajamos y queremos ver algo en una plataforma de streaming de nuestro país de origen, podemos conectarnos a una VPN que muestre en Internet que estamos en ese país. También, si están en un país donde quieren ver un contenido que justamente no está disponible en nuestro país de origen, podemos justamente comprar un servicio de VPN y elegir otro país. Internet piensa que estamos allí y podemos ver el contenido.

Esto significa, entre otras cosas, que estamos utilizando un conjunto diferente de resolutores recursivos y por lo tanto Internet piensa que no estamos en ese país. Es decir, que si hay un bloqueo en unos resolutores recursivos podemos sortear ese obstáculo simplemente con una VPN. Muy bien. Le cedo la palabra a otro panelista.

MAARTEN AERTSEN

Muy bien. ¿Qué puede salir mal o no tan bien? A veces hay un bloqueo excesivo cuando el bloqueo es demasiado amplio. Por ejemplo, se puede bloquear un dominio de tercer nivel. Luego uno de segundo nivel o luego a nivel de TLD. Si el bloqueo es demasiado amplio, quizá se evita el acceso a más de un destino o más de un sitio web. Esto es un problema para quienes quieren visitar esos sitios web que quizá no son problemáticos.

Eso sucede cuando hacemos un bloqueo en el sitio equivocado. Hay muchos casos prácticos, muchos ejemplos en el documento. Les sugerimos que lean el documento y vean esos casos prácticos. Hay un caso de bloqueo excesivo. Por ejemplo, Italia le da algunos nombres de dominio a sus ISP y sin querer incluyeron un dominio en esa lista que se usaba para infraestructura. Eso fue un bloqueo excesivo que derivó en el bloqueo de Google Docs para los usuarios de Italia por un breve periodo hasta que alguien descubrió el error.

Ese error generó inconvenientes para los usuarios que no podían acceder a contenido que no era problemático en absoluto. Este es un daño colateral. Si no lo hacemos bien el bloqueo vamos a afectar a personas que no deberían haber sido afectadas.

Como dijo Warren, la gente puede eludir un bloqueo. Cada vez que hay un bloqueo hay que suponer que un usuario va a encontrar una vía alternativa, sobre todo si tiene un motivo suficiente, puede usar su VPN, puede usar otros resolutores. De hecho, hay tecnologías que permiten que los usuarios accedan a contenido o hagan que el contenido siga estando disponible. El bloqueo del DNS es una

cuestión gradual. Alguien supone que si bloqueamos un dominio y le enviamos una orden a un ISP en el país el problema se solucionará. Sí, para una cantidad de usuarios pero no para todos.

WARREN KUMARI

Cuando se bloquea un dominio, el resolutor recursivo puede responder de dos maneras. Uno, el dominio no existe y dos, vemos que el resolutor recursivo redirecciona al usuario hacia otro destino. Esto, a nuestro criterio, es bastante peligroso porque si el usuario está tratando de llegar a un sitio y es redireccionado a otro sitio, el buscador web nos va a dar una alerta y nos va a decir: "Quieres llegar a tal sitio pero en realidad estás llegando a otro". Vamos a recibir esos mensajes de alerta que tienen repercusiones en materia de seguridad.

A veces ignoramos esas alertas pero a veces puede ser que la ignoremos y estemos tratando de llegar al sitio web de nuestro propio banco. Por favor, si van a bloquear el DNS, no hagan un redireccionamiento. Ahora creo que vamos a pasar a la sección de recomendaciones. Okey. Continúo yo con la presentación.

Como dijimos previamente, el bloqueo del DNS es una herramienta y al igual que cualquier herramienta se la puede utilizar para el bien pero si no sabemos utilizarla o no conocemos las instrucciones, podemos resultar perjudicados. Si van a utilizar el bloqueo del DNS, asegúrense de saber cómo funciona y cuáles pueden ser las consecuencias colaterales.

GREG AARON

Además, el SSAC recomienda que si vamos a hacer que sea obligatorio un bloqueo del DNS dentro de una empresa a nivel nacional o dentro de un ISP tenemos que seguir estas pautas. En algunos casos estas pautas se basan en el principio médico de no hacer daño. Tenemos que ver cómo va a lograr nuestros objetivos este bloqueo del DNS. Si sirve para ello. Quizá hay algunas medidas alternativas. Tenemos que pensar si el bloqueo nos va a ayudar o si no va a ser suficiente.

Tenemos que tener una política clara de qué es lo que queremos bloquear y cómo lo vamos a hacer. Tenemos que tener procedimientos bien definidos para analizar qué incluimos en la lista de bloqueo y minimizar el riesgo. También saber cómo corregir un error. No recomendamos políticas y procedimientos específicos porque dependen de sus propios objetivos y tareas pero este es un principio importante.

Tercero. Hay que implementar esto de manera tal que se minimice el bloqueo excesivo o el daño colateral para los usuarios. Por ejemplo, en una empresa a sus empleados que podrían verse perjudicados.

Por último, no hay afectar a las personas que están fuera de su responsabilidad administrativa. En Europa, por ejemplo, hay muchos países y algunos de los ISP europeos tienen clientes en más de un país. Si están en el país A y el ISP tiene clientes en el país A y B, qué pasa si el ISP recibe una orden del país A de hacer un

bloqueo. Cómo bloquea ese ISP al DNS sin afectar a los clientes que tiene en el otro país, fuera de su jurisdicción territorial. Vemos las fronteras nacionales en un mapa pero la Internet no se correlaciona con esas fronteras. Cuidado. Tengan cuidado de no afectar a las personas que no tienen derecho de afectar. Voy a ser rápido porque nos quedamos sin tiempo.

WARREN KUMARI La última recomendación tiene que ver con los operadores de los servidores recursivos. Es decir, que utilicen RFC para los códigos de error extendidos que incluyen el bloqueo. Creo que podemos recibir preguntas.

MARCO HOGEWONING No nos queda mucho tiempo para las preguntas. Muchísimas gracias. Es un trabajo sumamente detallado como parte del público al que va dirigido. Se lo agradecemos. Tenemos poco tiempo pero creo que podemos recibir una pregunta breve. Veo a Papúa Nueva Guinea en el chat, que hizo un comentario. No sé si quiere hacer la pregunta también aquí.

RUSSELL WORUBA Gracias, Marco. Como país hemos sido invitados a participar en ensayos sobre el servicio de protección de nombres de dominio. Quería hablar de esto en particular y preguntarles si podrían comentar al respecto.

MAARTEN AERTSEN Sí. El servicio de protección de nombres de dominio se puede utilizar a través del bloqueo de DNS. Por ejemplo, estos resolutores públicos que mencionamos se ocupan de esta protección contra el malware y el phishing. Por ejemplo, lo bloquean para proteger a sus usuarios. Esa es una técnica que se puede utilizar para proteger a los usuarios.

También queremos mencionar que este documento se ha utilizado para aportar información para tomar decisiones en el ámbito político, sobre todo en Japón, que están considerando bloquear determinado contenido específico en el país.

WARREN KUMARI Claudflare es una de las organizaciones que ofrece resolutores públicos. Ofrecen tres direcciones diferentes. Por lo menos tres. Una es la estándar. 1.1.1.1, donde no hacen bloqueo. Luego tienen 1.1.1.2, para bloquear malware. Después tienen el 1.1.1.3, que ofrece más protección, bloquea malware y también otro tipo de contenido para adultos.

Nosotros decimos que si se va a ofrecer un servicio de protección a un grupo más grande, los usuarios deberían poder elegir cuál es el nivel de protección que quieren. Si uno es padre, podría elegir proteger contra determinado contenido. Podría utilizar el servicio de protección de DNS que impida ver ese contenido pero tal vez si no está en esa situación, puede optar por ver ese contenido. Se podrían tener distintos niveles de bloqueo para distintos grupos de personas afectadas. Si uno elige hacerlo, uno decide que quiere

tener esa protección, tal vez eso sea más manejable que una protección que se impone de otro lado directamente.

MARCO HOGEWONING

Gracias, Warren. Hay tres personas que han pedido la palabra. Voy a cerrar la lista de intervenciones aquí. Sean breves. Un minuto para cada pregunta y respuesta de ser posible, para que luego tengamos tiempo para hablar del otro tema. Creo que en primer lugar tenemos a Blaise.

BLAISE AZITEMINA FUNDJI

Blaise Azitemina, de la República Democrática del Congo. Tengo una preocupación con las VPN. Si bien estoy agradecido por el nivel de seguridad que nos ofrece una VPN, al mismo tiempo, desde la perspectiva de política me preocupa la deslocalización porque en los países en desarrollo muchos utilizan las VPN, no por la protección o la seguridad que ofrecen sino básicamente para ocultar otra dirección de un país, para mostrar que están en otro país a veces.

En ocasiones esto es una violación a las políticas de seguridad de nuestros países. Vemos plataformas de streaming que parecen haber encontrado una solución. Cuando uno se conecta a través de una VPN de un proxy les va a decir que no califican o que no tienen acceso. Cuál es el equilibrio entre la seguridad, la protección y al mismo tiempo la exactitud de la posición geográfica. Gracias.

MAARTEN AERTSEN

Creo que el SSAC no ha considerado todas las implicancias. La verdad es que las VPN están ampliamente disponibles al igual que otras herramientas. Se utilizan con buenos propósitos y con malos propósitos. También los delincuentes las utilizan para ocultarse donde están. Las VPN aprovechan las ventajas del funcionamiento de la Internet y están aquí para quedarse. Algunas empresas mantienen listas de IP de VPN conocidas. Por ejemplo, la utilizan para calificar los riesgos del tráfico que proviene de esas direcciones. Hay herramientas para detectar y entender el tráfico de las VPN.

WARREN KUMARI

Si me permiten agregar, las VPN están diseñadas para verse como un tráfico normal de Internet. En algunos lugares que se ha tratado de prohibir su uso, en empresas o en países, parecen bloquear los grandes servicios de VPN pero los usuarios quieren poder acceder. Entonces los usuarios van a una lista de VPN con seguimiento y tal vez puede ser mucho más inseguro eso. A veces hay consecuencias negativas cuando se trata de bloquear una técnica que los usuarios utilizan para llegar a acceder a ese contenido. Van a encontrar la manera de acceder a ese contenido.

MARCO HOGEWONING

Por favor, las próximas preguntas que sean breves. India.

SUSHIL PAL ¿Creen que el DNS4EU puede ser una solución? Las VPN sí, tienen importancia. Hay algunas que son conocidas, ¿pero los organismos de seguridad están buscando alguna manera de monitorear las VPN que no son conocidas?

MARCO HOGEWONING Ashwin, su pregunta.

MAARTEN AERTSEN Lo que les puedo decir con respecto a DNS4EU es que ellos han armado el sitio web sobre la base de la soberanía. En lugar de enviar el tráfico a resolutores comerciales grandes, ahora ofrecen este sistema para que el tráfico esté en Europa a través de DNS4EU. Si los organismos de seguridad buscan maneras de monitorear las VPN desconocidas, no lo sé.

MARCO HOGEWONING Indonesia, última intervención.

ASHWIN SASTROSUBROTO Estaba pensando en este comentario sobre el bloqueo y los impactos negativos. ¿Qué pasa si no se permite directamente acceder al ciberespacio con el DNS? Solamente a lo que queremos. Por ejemplo, si es .ORG, no lo permites. Si decimos .COM, sí es autorizado. En lugar de bloquear se bloquea todo y luego se va autorizando el acceso al DNS con cierta aprobación.

WARREN KUMARI

No sé si realmente eso es viable. Hay millones de sitios en Internet. Escribir una lista de aquello que sí se puede ver sería difícil pero incluso aunque fuera posible técnicamente no es posible en estos días, bloquear todo el acceso al DNS. Hay nuevas tecnologías, DNS sobre TLS, DNS sobre HTTPS, DNS sobre QUIC donde no está visible que la consulta sea una consulta en sí misma. Solamente mira todo como tráfico de Internet. No se puede desconectar al país de la Internet porque afectaría a otros proveedores de servicios de Internet como Starlink, por ejemplo. Muchos van a quedar aislados.

MAARTEN AERTSEN

Las tecnologías que mencionó Warren básicamente están relacionadas con la encriptación y están diseñadas para proteger las identidades de los usuarios finales que están haciendo las consultas. Por lo tanto, estas tecnologías son intentos para ofrecer mayor privacidad en Internet.

MARCO HOGEWONING

Gracias. Les pido disculpas. Es muy interesante este tema. Veo que hay mucha interacción. Vale la pena darle seguimiento. Tenemos el código de QR para acceder al informe completo. Por favor, accedan a él. Léanlo. Está publicado hace un tiempo.

Muchísimas gracias, Ram, Greg, Warren, Maarten. Siéntanse libres de quedarse por aquí. Sin más demora, quisiera ahora pasar a lo

que creo que es un seguimiento sobre la conversación que tuvimos sobre computación cuántica y algunos de los riesgos. Esto lo hablamos en Seattle. Quiero recibir a Cristian Hesselman de SIDNLabs para que nos comente cuál es el impacto en DNSSEC y nosotros, como representantes de gobierno, qué podemos hacer para mitigar alguno de los problemas. Adelante, Cristian.

RAM MOHAN Antes de eso quiero agradecer al GAC por esta invitación. Valoramos mucho nuestra colaboración. Muchísimas gracias.

MARCO HOGEWONING Gracias, Ram. Ahora sí, Cristian.

CRISTIAN HESSELMAN Gracias, Marco. Con esta presentación vamos a hablar de la computación cuántica y DNSSEC, y el impacto que las futuras máquinas podrían tener. Al final de esta charla incluí algunas acciones sugeridas que podría adoptar el GAC desde la perspectiva gubernamental. ¿Qué pasó con las diapositivas? Desaparecieron. Voy a seguir hablando. La imagen que acaban de ver la obtuve del centro de computación cuántica en Alemania, donde se está trabajando básicamente en una fase experimental que casi se parece a la ciencia ficción. Aquí estamos. Siguiente, por favor.

En primer lugar, cuáles son las expectativas respecto de las computadoras cuánticas. Yo no soy experto en computadoras cuánticas. Sí en sistemas distribuidos. Creo que las computadoras

cuánticas, ese conocimiento lo tienen los físicos pero yo no soy una de estas personas. Esto es lo que yo leí a partir de la biblioteca. Las expectativas respecto de las computadoras cuánticas es que haya nuevas aplicaciones, descubrimiento de nuevos fármacos, distintos métodos médicos, la mejora del aprendizaje automático, el desarrollo de materiales revolucionarios pero, como dijo Greg, se puede utilizar la tecnología de distintas maneras. Este es el ejemplo del martillo. Lo podemos utilizar de manera positiva pero también lo podemos utilizar de alguna manera que presente algunos riesgos.

La desventaja es que estas computadoras pueden romper los algoritmos criptográficos que estamos utilizando actualmente. Unos podrían ser los algoritmos para el DNSSEC, por ejemplo, que se utilizan para autenticar los mensajes de DNS y verificar la integridad de dichos mensajes. Desaparecieron las diapositivas nuevamente. ¿Quieren que continúe o espero a que presenten las diapositivas en la pantalla? Ahí están. Muy bien. Hemos vuelto.

Los riesgos de las computadoras cuánticas en términos del DNSSEC es que potencialmente podrían alterar los algoritmos criptográficos que utiliza DNSSEC para verificar la autenticidad y la integridad de las respuestas del DNS. Potencialmente esto podría redireccionar esto o firmar nuevamente los mensajes con una clave comprometida fingiendo que los mensajes son reales y en realidad podríamos llegar a sitios incorrectos a los que uno no debería ir.

Aquí suponemos que todos vivimos ya en la era poscuántica. No sería ahora si no en el futuro. Esto tiene más que ver con un ataque que no ocurre ahora sino en el futuro pero en tiempo real podría comprometer todas las claves que se utilizan para las firmas en DNSSEC. Los expertos piensan que esto no va a pasar por lo menos hasta dentro de 10 o 15 años. El interrogante es por qué tendríamos que trabajar ahora en este tema. Siguiente, por favor.

Porque al remplazar los algoritmos criptográficos en DNSSEC, esto insume mucho tiempo. Esto surge de un trabajo donde se ve el desarrollo de un algoritmo criptográfico en DNSSEC. Desde la primera versión preliminar en el IETF a la izquierda hasta la implementación completa a la derecha, pueden ver que hay muchas actualizaciones, mucho trabajo. Si las computadoras cuánticas van a transformarse en una realidad de aquí a 10 o 15 años, tenemos que pensar qué tenemos que hacer hoy en el ámbito del DNSSEC. Siguiente.

Además de la cuestión temporal, también tenemos un trabajo de despliegue de implementación importante para el DNSSEC. Podemos ver aquí los países que firmaron con DNSSEC su ccTLD. Los que están en verde son los que ya están operativos. Verde y azul. Un 48 % del mundo. A la derecha, ustedes pueden ver la validación. Este es un mapa que tiene más rojo y color ámbar, y es porque la validación de estas firmas tiene un nivel de adopción más bajo.

Hay cosas que todavía deben aprobarse pero como se puede observar. Hay una implementación significativa ya del DNSSEC. Esto hay que considerarlo junto con las computadoras cuánticas, sobre todo si suponemos que la validación va a aumentar en el futuro al igual que la firma que vemos aquí a la izquierda. Siguiente, por favor.

Si queremos proteger el DNSSEC de las computadoras cuánticas tenemos que identificar estas tres estrategias que vemos aquí. Por un lado la que llamamos de remplazo, otra de rediseño y otra de retirar.

Remplazar significa remplazar los algoritmos criptográficos que existen hoy por otros. Es decir, para algunos que sean seguros para estas computadoras cuánticas rediseñar significa rediseñar el sistema de DNSSEC por completo. Es la segunda opción que está en esta tabla. La tercera sería retirar que significa eliminar DNSSEC por completo.

Estos tres abordajes tienen ventajas y desventajas. Por ejemplo, la estrategia de remplazo es relativamente fácil de implementar y de normalizar pero tiene algunos riesgos operativos. Luego hablaremos más de esto. La de rediseño en realidad es como comenzar de cero con DNSSEC, utilizar nuevas tecnologías como los árboles de Merkle, que reducen los riesgos pero básicamente tenemos que renovar todo el sistema del DNSSEC y sus protocolos, lo cual insumiría mucho tiempo.

Luego la opción de retirar el DNSSEC, puede parecer fácil pero tiene un impacto porque si eliminamos el DNSSEC abrimos a todo tipo de ataque. El DNSSEC trata de proteger al DNS de todos esos ataques. En nuestro trabajo optamos más por la primera alternativa, la de remplazo. Por eso la tenemos aquí en verde. Vamos a hablar de este enfoque en particular de ahora en más.

No voy a explicarles este gráfico. No se asusten pero lo que ustedes ven aquí son las interacciones que se producen entre los resolutores y los servidores de nombres autoritativos con los mensajes del DNSSEC que se muestran aquí. Los mensajes en rojo y amarillo significa que tienen ya firmas o llaves públicas. Estos tienen que ser actualizados. Siguiente.

Para darles una idea de cómo se ven estas firmas, estos son dos ejemplos. En la parte de arriba vemos una llave pública a la izquierda firmada o que se está utilizando en DNSSEC. En gris tenemos una firma generada por esa llave. En azul vemos esta llave pública y la firma de DNSSEC, que es creada por un algoritmo poscuántico. Es decir, es lo suficientemente fuerte para proteger de la computación cuántica y pueden ver que es un poco más extensa. Esto es simplemente para darles un indicio de cómo se vería desde una perspectiva técnica. Siguiente, por favor.

Hay distintos algoritmos que son seguros ante la computación cuántica, que se aplican sobre todo en el contexto de NIST, que es el Instituto Nacional de Normas y Tecnología de Estados Unidos que han utilizado especialistas en criptografía para poder

desarrollar un algoritmo que pueda soportar la computación cuántica. Aquí tenemos ejemplos con algunos nombres curiosos. Falcon, SQSign.

Hemos experimentado con estos algoritmos y hemos validado el tiempo que lleva firmar sus propios archivos, por ejemplo, la zona .NL, para poder validar los registros del DNS. También tenemos los tamaños de firmas y los tamaños de las llaves que pueden diferir de gran manera. Como pueden ver a partir de esta tabla, es como una concesión recíproca que se hace. Podemos tener tamaños de firma más pequeños y si tenemos ese tipo de tamaños pequeños, la velocidad de la firma puede aumentar o viceversa. Siguiente, por favor. Siguiente, por favor.

Bien. Aquí vemos el primer experimento que hicimos para la zona de .NL. Firmamos las zonas con dos algoritmos poscuánticos. No les voy a dar los detalles pero vemos que lleva el doble de tiempo prácticamente firmar la zona con estos algoritmos PQC. Por lo general lleva 10 minutos firmar la zona .NL. Con estos PQC, con estos algoritmos, lleva 20 minutos la firma, que no está mal.

Aquí vemos que estos resultados están bien desde el punto de vista operativo. Esta es nuestra situación actual en SIDNLabs. Nosotros identificamos temas que nos gustaría continuar estudiando a futuro que en gran medida tienen que ver con el tamaño de estas firmas y estas claves públicas. También queremos estudiar el tiempo de validación en los resolutores en mayor detalle junto con, por ejemplo, el rol de la memoria caché.

Por último tengo algunas sugerencias para el GAC. Quizá puedan trabajar con la agencia de los Estados Unidos que se ocupa de este tema para ver cómo se están alineando con el algoritmo PQC que ellos están desarrollando. Yo sé que a esta agencia le interesa mucho este tema. También pueden incentivar el desarrollo de software de código abierto que integre los algoritmos PQC al DNS y a su infraestructura.

Quizá esto lo puedan hacer con fondos de NLNet o el Sovereign Tech Fund. Quizá también puedan estimular el despliegue, la implementación quizá con un sitio como Internet.nl, donde pueden ver las propiedades de nombres de dominio y allí también quizá rápidamente puedan incluir verificaciones para ver si sus dominios están listos para la implementación de PQC.

Por último, quiero decir que tenemos que seguir investigando el impacto operativo de estos nuevos algoritmos PQC si vamos a seguir esta estrategia de remplazo y tenemos que ver las repercusiones para el DNS, sus operadores y para la zona raíz.

El software que desarrollamos lo utilizamos para nuestros experimentos. Utilizamos un software de prueba. Es un software de código abierto. Ahí tienen el código QR. Pueden descargar ese software y, por supuesto, con todo gusto responderé a sus preguntas. Muchas gracias.

MARCO HOGEWONING

Muchas gracias por la presentación. Todos vamos a poder descargar entonces este software cuántico. Muchísimas gracias. Tenemos aquí algunas acciones sugeridas que son acciones clave y desde la perspectiva gubernamental en el gobierno de Países Bajos empezamos a hacer gestión de activos. El DNS está en todos lados, con lo cual, las DNSSEC también están en todos lados.

Ya estamos internamente trabajando para ver dónde necesitamos tomar acciones, hacer remplazos. Les puedo decir por experiencia que del dicho al hecho hay un largo trecho. Peter, en línea, quiere tomar la palabra y Barry aquí en la sala.

BARRY LEIBA

Muchas gracias. Quiero aclarar algo. Cuando hablamos de criptografía poscuántica, hay que resaltar que hay un concepto erróneo según el cual las computadoras cuánticas ponen en riesgo todo nuestro encriptado. Cristian hablaba de firma, firmar. Ese es un tipo en particular de encriptado que sí se ve en riesgo a raíz de la computación cuántica. El encriptado general que utilizamos para el tráfico en Internet no se encuentra en riesgo sino el tipo de encriptado que se utiliza para el intercambio de claves y llaves para hacer las firmas digitales.

CRISTIAN HESSELMAN

En general tenemos que ver casos de uso, requisitos específicos. Tenemos que ver cuáles son los casos de uso críticos que nos interesa estudiar.

MARCO HOGEWONING Muy bien. Ahora Peter, que está en línea, quiere tomar la palabra.

PETER THOMASSEN Estoy aquí, en la sala. Soy miembro del SSAC. Quiero hablar acerca de un aspecto. Hay un bajo número de firmas en DNSSEC pero si vemos los números abstractos o generales hay más de 10 millones de nombres de dominio y eso es un número significativo. No sabemos cuál será el método de firma cuando se transicione de las DNSSEC a la firma poscuántica.

Hay más de 10 millones de dominios actualmente. Quizá sean más pero no podremos hacer la transición si no se la coordina bien. Esto es muy importante. En el mapa que usted mostró veíamos países en color azul que tienen ccTLD que justamente están alineados para hacer estos cambios. Si sus países quieren hacer esa transición automática, en el SSAC con todo gusto los vamos a poder ayudar. Estoy a su disposición al igual que otros miembros del SSAC.

MARCO HOGEWONING Muchas gracias. Tenemos algo de tiempo todavía. Podemos seguir tomando preguntas de la sala.

NICOLÁS CABALLERO Muchas gracias. Gracias por esta maravillosa presentación, Ram y equipo. Siempre es un placer recibirlos en nuestra sala. Quiero

decir dos cosas. Primero, Ram, Cristian, quisiera saber si podemos aprovechar que está Jim Galvin aquí. Quisiera saber si podemos aprovechar esta oportunidad para preparar una presentación para la junta directiva en Muscat, para la reunión en Omán. Quizá debamos hacer una versión más liviana de la presentación porque hay tres o cuatro miembros de la junta directiva que tienen un gran conocimiento técnico pero no los demás.

También quiero decir lo siguiente. Aprovechando que está aquí mi estimado colega de Brasil. Estamos organizando una sesión regional de creación de capacidades para países latinoamericanos que será en Brasilia o en San Pablo. Lo tenemos que decidir. Antes o después de la reunión de Omán, ¿podrían ayudarnos a preparar este evento?

Queremos hablar de la implementación de las DNSSEC. Queremos hablar de criptografías métrica y asimétrica. Queremos ver, por ejemplo, qué es lo que está sucediendo. Corríjanme si me equivoco pero hace dos o tres semanas el RSA quedó sin efecto. Se rompió. No sé si esto fue así o no pero eso es lo que escuché. De todas maneras, hay muchísimas ventajas del software de código abierto para los gobiernos. Yo soy un gran usuario de este tipo de software gratuito y de código abierto pero me cuesta explicar de manera simple a quien no tiene un conocimiento técnico, me cuesta explicarle las ventajas no solo técnicas sino también económicas y todas las ventajas que ofrecen todo este tipo de licencias. Quizá

con su ayuda, con su conocimiento técnico, podríamos tener un poquito más de éxito.

Resumo. Dos pedidos. Ayudarnos a preparar una presentación para la junta directiva y ayudarnos a preparar nuestro evento regional de creación de capacidades para Sudamérica para los países de esa región que quizá este evento se haga en Brasilia o en San Pablo.

RAM MOHAN: Nico, muchísimas gracias por este pedido. Nos entusiasma mucho. Queremos colaborar. Quedo a su disposición. Acérquese y conversaremos al respecto.

CRISTIAN HESSELMAN: Igualmente de mi parte.

NICOLÁS CABALLERO: ¿Podría decirnos algo acerca del RSA?

WARREN KUMARI: Creo que usted habla acerca de un documento académico publicado por Google que dice que ahora es más fácil eludir el RSA, que los niveles necesarios ya son menos exigentes, que hay menos complejidad en las computadoras cuánticas necesarias. Hay una menor cantidad de bits cuánticos para tener un sistema confiable.

En el documento se dice que justamente no se necesitan tantos bits como se pensaba pero no queda claro hasta qué grado nos tenemos que preocupar de aquí al futuro. Es decir, el RSA todavía funciona. Lo que pasa es que en algunos años aparentemente sí es probable que deje de funcionar pero las estimaciones no son del todo exactas. Básicamente se toma un promedio de estimaciones formuladas por científicos que se ocupan del tema cuántico. Puede ser mañana, puede ser en 50 años o en 500 años. Es difícil de predecir.

Hay una gran posibilidad de que sea dentro de algunos años pero es como la energía de fusión del átomo. ¿Qué pasó? No se supo cuándo se iba a tener lista esta tecnología hasta que sucedió. Podemos hablar del RSA o de otros sistemas criptográficos que son vulnerables. Tenemos que estar preparándonos para el futuro.

NICOLÁS CABALLERO: Tenemos que arreglar la gotera del techo cuando todavía no está lloviendo. Perfecto.

MARCO HOGEWONING: Tenemos un pedido de la palabra de Australia. Adelante, por favor.

INGRAM NIBLOCK: Quiero ver una tabla donde se ve una comparación entre el tamaño de las claves. Entiendo el tema del tamaño de los paquetes UDP. ¿Cuál sería el efecto práctico de tener tiempos de firma más extensos? Por ejemplo, para .NL, una diferencia de 2 a 10 minutos,

¿eso es problemático? Por ejemplo, si hay que hacerlo reiteradamente. ¿Eso es un problema en el DNS?

CRISTIAN HESSELMAN Tenemos 6,2 millones de dominios en nuestra zona y la publicación es de 30 minutos más o menos. Cada 30 minutos hay que volver a firmar. Si el tiempo de firma lleva mucho tiempo, se nos acaba el tiempo para publicar. Eso es algo que hay que tener en cuenta.

MAARTEN AERTSEN Esto tiene que ver con el modelo de implementación. Cristian tiene un modelo de zona completa pero hay otro modelo de firmas incrementales o firmas en tiempo real para cada consulta. Es difícil dar una respuesta en general pero sí, la velocidad es un factor importante.

PETER THOMASSEN Sí. Quizá cuanto más se tarde en firmar, quizá haya que hacer más cambios en el modelo que se utiliza.

MARCO HOGEWONING Muy bien. Gracias. Espero que hayan sido respondidas las preguntas. Ahora vamos a hacer la pausa para el café. Pueden intercambiar un diálogo, comentarios con los colegas en esta pausa. Quiero agradecerles nuevamente a todos los panelistas que se han unido a nosotros en esta sesión por esta información de

	tanta utilidad y por ayudarnos a comprender todos estos conceptos técnicos. Antes de la pausa para el café quiero decirles que tenemos que volver a la sala del GAC para la sesión sobre WHOIS y exactitud de datos. Espero que hayan disfrutado de esta sesión y que hayan aprendido a raíz de la información compartida. Disfruten el café. Muchas gracias.
SPEAKER NAME	Insert text delivered by speaker – continue entering text here. Continue entering new paragraph from same speaker and use the "enter" or "return" when you need to start a new paragraph from same speaker. Once this speaker is done, use "TAB", twice to generate a new row that should be left empty, and use "TAB" a third time to generate the row to enter next speaker (there should be one empty row between each speaker).
NEW SPEAKER NAME	Insert text delivered by speaker
NEW SPEAKER NAME	Insert text delivered by speaker
NEW SPEAKER NAME	Insert text delivered by speaker

[FIN DE LA TRANSCRIPCIÓN]