KOBE – Taller sobre las DNSSEC (1 de 3)
Miércoles, 13 de marzo de 2019 – 09:00 a 10:15 JST
ICANN64 | Kobe, Japón

RUSS MUNDY: Vamos a aguardar un poquito más porque esta sala está un tanto alejada del resto de las salas en el evento. Aguardaremos un par de minutos antes de comenzar. Creo que tenemos suficientes puestos libres aquí en la mesa de oradores. Los invito a sentarse aquí junto a nosotros.

JACQUES LATOUR: Buenos días. Estamos listos para comenzar con la sesión. Bienvenidos al taller sobre DNSSEC en Kobe. Vamos a comenzar con la presentación que generalmente hacemos acerca de cómo se emplean las DNSSEC alrededor del mundo, su nivel de implementación a nivel mundial.

¿Quiénes están aquí por primera vez? Muy bien. Ya me parecía. Aquí también van levantando la mano. Muy bien. Otro participante nuevo en estos talleres. Tenemos algunas caras nuevas. Aquí tenemos a los integrantes del comité de este programa en esta sesión.

Como les decía, estos son los integrantes del comité de este programa. Les cuento acerca de este taller. Nos reunimos una

vez por semana y luego armamos el programa para el próximo taller. Este es un taller que hacemos todo el año y siempre tratamos de aprender sobre la versión del taller anterior en la reunión pasada para mejorar los temas que presentamos en la próxima versión del taller.

Esto es algo muy importante. Hoy tenemos un almuerzo. Tenemos muchos patrocinadores. Steve está trabajando justamente en la recaudación de fondos y en conseguir patrocinadores para tener este almuerzo en el taller del DNSSEC. Gracias a nuestros patrocinadores por financiar este almuerzo. En el día de ayer también tuvimos un evento sobre las DNSSEC a cargo de uno de nuestros anfitriones, JPRS, el registro local.

El taller de las DNSSEC es una iniciativa conjunta entre el Comité Asesor de Seguridad y Estabilidad de la ICANN, el SSAC, y también trabajamos con ISOC, con la Sociedad de Internet con su programa Deploy360. En el día de hoy vamos a tener tres bloques principales en nuestro taller. Tenemos la sesión con nuestros panelistas, como siempre, en la cual las personas en la región hablan acerca de la implementación de las DNSSEC y las iniciativas a tal fin. Luego tenemos una pausa y antes del almuerzo tenemos otro panel sobre DNS sobre TLS, DNS en HTTPS. Es una sesión muy interesante. Luego tendremos una sesión de preguntas y respuestas y pasaremos a nuestro almuerzo. Necesitan tener este cupón, por favor, para poder

ingresar al almuerzo. Si no lo tienen, no van a poder almorzar. Creo que tenemos más que suficientes. Habrá para todos. Alcanzará para todos.

Después del almuerzo tenemos una sesión especial para hablar acerca del traspaso de la KSK, de la zona raíz. Vamos a ver con qué frecuencia vamos a hacer esa sesión o ese debate, si va a ser semanal o con qué frecuencia. Muy bien. Vamos a ver la implementación de las DNSSEC en todo el mundo y vamos a ver cifras, cifras, cifras, estadísticas, números al respecto.

Muy bien. En los últimos meses vemos una tendencia descendente antes del traspaso de la KSK pero ahora está retomando su crecimiento esta tendencia y aproximadamente el 19% de las estadísticas que vemos en pantalla están haciendo resolución de DNSSEC. Esta es una prueba que hace APNIC para medir en todo el mundo la capacidad de validación de las DNSSEC por parte de los resolutores.

Aquí tenemos estadísticas de Asia sobre la implementación de las DNSSEC. Tenemos Micronesia con 66% y luego sigue bajando la cantidad de validación. Después tenemos quiénes utilizan el DNS de Google versus los proveedores de Internet que utilizan sus propios servidores de DNS.

Aquí vemos otro gráfico. En la primera columna vemos el .COM con una cantidad de dominios firmados. Creo que el número es

800.000. 876.000 para .COM. Luego viene .NL con 640.000 y luego .NET con alrededor de 100.000. Perdón, el segundo era [.SE], luego .NET con 100.000. Luego tenemos el próximo dominio con 4.000. Creo que necesitamos seguir trabajando. Hay mucho por hacer para lograr que más dominios tengan esta firma, esta validación de las DNSSEC.

ORADOR DESCONOCIDO: Estas cifras no son correctas. No están bien.

JACQUES LATOUR: Si nos puedes ayudar.

DAN YORK: Sí. Están mal. Esto está mal. Estas cifras no están bien. Hay que repasarlas. Hay que corregirlas.

RUSS MUNDY: Muchas gracias. Necesitamos justamente que nos vayan diciendo todo esto, que nos den sus comentarios, sus perspectivas. Sí, tiene razón. Sí. Estos son los resultados que vemos de SecSpider.net.

JACQUES LATOUR: Muy bien. En la próxima sesión vamos a tener mejor información. Luego lo que hacemos es un mapa que muestra las distintas instancias de implementación en los distintos ccTLD. Por ejemplo, en algunos casos anunciaron que van a firmar su TLD y en otros casos ya tenemos registros de DS en la raíz o bien no se cuenta con soporte para CDS. Por último, tenemos en color verde oscuro las DNSSEC en plena implementación.

Vemos un mapa y vemos que avanzamos porque hace cinco o seis años había muchos lugares en color rojo. Todavía tenemos algunas áreas en las cuales nos tenemos que concentrar en África y en algunas partes de Asia y de Latinoamérica. Tenemos distintas iniciativas en esta región para que los ccTLD firmen las DNSSEC. Esto requiere un trabajo técnico, científico que es sencillo y es bastante asequible. Tenemos a Sudán en África, .SD, que anunció que va a firmar las DNSSEC en su ccTLD. Desde la última reunión de la ICANN, este es el único ccTLD que anunció que iba a firmar DNSSEC. Es el único cambio que vimos en estos meses. En Asia tenemos trabajo por delante. Tenemos algunos registros DS en la raíz. Para nosotros el desafío es ver en qué momento el registrador acepta los registros DS en cada caso en ese TLD. Sí, hay que decirle a Dan, le tienen que informar a Dan o tienen que enviar un correo electrónico a la lista correspondiente de la ISOC para informar que están haciendo esta validación. De lo contrario, no podemos enterarnos de esta

situación. Cuando no hay registros DS en la raíz, entonces es más sencillo.

Tenemos aquí en este mapa un lugar que está en color verde más claro. Ah, no. Hay dos. Dos lugares en ese color verde más claro. ¿Cuáles son? ¿Croacia? Tenemos que trabajar en esos dos lugares para llegar al 100% de implementación.

STEVE CROCKER: Creo que en la zona de Escandinavia hay una pequeña isla.

ORADOR DESCONOCIDO: Hay un pequeño lugar entre Suecia y Finlandia. Creo que es .AX, Aland. No sé si pronuncio bien el nombre del lugar.

ORADOR DESCONOCIDO: Deberían comenzar rápidamente para poder trabajar en esta implementación.

JACQUES LATOUR: Quizá deberíamos pintarlo de otro color en el mapa. De todas maneras, estamos avanzando. En Latinoamérica van bien encaminados también. Creo que se están focalizando en lograr una mayor cantidad, un mayor nivel de firma de DNSSEC y Fred se está encargando de eso. Siga adelante. Yo pensaba que Groenlandia iba a estar también en color verde oscuro. Tenemos

que ver qué pasó. Eso fue lo último que supimos de Norteamérica.

Pueden descargar este mapa desde este enlace que ven en pantalla y si saben de algún ccTLD en la región que está avanzando o que ya está firmando las DNSSEC, por favor infórmenlo en la lista de correo correspondiente. La ISOC está trabajando también en un proyecto de la historia de las DNSSEC. Pueden ir a ese enlace que ven en pantalla y actualizar la información según les parezca pertinente. Con esto finalizo mi presentación. Ahora responderé sus preguntas.

RUSS MUNDY: Hay un participante en la sala que puede responder sobre el mapa.

ORADOR DESCONOCIDO: Hola, sí. Con todo gusto voy a darles información acerca de todo lo que venimos rastreando e informando y haciendo seguimiento en estos últimos años. Tenemos un corpus de datos que tiene muchísima información. Podemos darles todos estos datos. Podemos hablar con ustedes al respecto.

ORADOR DESCONOCIDO: Sí. Hay muchas firmas ya de DNSSEC.

RUSS MUNDY: Yoshiro, por favor, le damos la palabra para empezar con los panelistas de la región. Adelante, por favor. Como ven, tenemos cuatro panelistas de la región. No sé si tenemos diapositivas para esta sección. Fantástico. Vamos a comenzar entonces por el orden de la lista que figura en el programa. Kenny Huang es de Taiwán y hará la primera presentación.

KENNY HUANG: Buenos días a todos. Yo soy CEO de TWNIC. Haré una breve introducción primero de la introducción de DNSSEC en Taiwán. Esta es la tendencia que nos muestra Google de DNSSEC en el mundo. La siguiente diapositiva, por favor. Hay que pulsar.

La introducción sobre la estructura y las actividades de la gobernanza del ecosistema de la Internet. Las estructuras de gobernanza es un modelo de incentivo. Hay incentivos para promover las tecnologías. Por ejemplo, tenemos que considerar tres componentes. El primero es la demanda del mercado. El segundo componente es la red, tanto el proveedor upstream como downstream. La jerarquía representa el modelo de regulación del modelo de gobernanza. Tener suficiente regulación que promueva la implementación de tecnología.

Aquí tenemos una muestra de DNSSEC… Perdón. Desde el punto de vista del mercado hay muy baja demanda de resolución de DNSSEC segura. El mercado entonces es bastante débil desde este punto de vista. Se ha venido desarrollando DNSSEC desde la IETF promoviendo el despliegue en toda la región. Desde el punto de vista de la jerarquía, los organismos gubernamentales de Taiwán respaldan el desarrollo de DNSSEC. TWNIC desarrolló el proceso de firma de .TW pero el contrato con el registrador no requiere la implementación de DNSSEC. En la próxima etapa intentaremos hacer algún ajuste relevante.

Como ven, esta es una lista de los registradores de TWNIC. Hay una marca arriba del registro que indica quiénes han desplegado DNSSEC, cuántos son. Solo seis registros de los 13 tienen servicio DNSSEC por lo cual estamos conversando con estos registros a ver cuál es el problema, cómo podemos alentarles para que desplieguen DNSSEC.

Aquí vemos algunas estadísticas de DNSSEC, en especial para el segundo nivel como en el caso de com.tw donde tenemos casi un cero por ciento. EDU.TW está casi en un 10% de DNSSEC implementado. Todavía hay mucho por hacer para promover DNSSEC en el .TW.

Hablemos un poquito de los comentarios operativos que nos permiten mejorar la implementación de DNSSEC. DNSSEC

permite mitigar los ataques de intermediarios pero no garantiza el tema de la seguridad. De hecho, un sitio malicioso, un nombre malicioso es una situación que encontramos con frecuencia. DNSSEC no les brinda a los proveedores de servicios demasiado valor agregado. Por eso los grandes servidores tienen cierta reticencia a implementarlo. Para ellos, DNSSEC es demasiado nuevo, aun cuando existe desde hace años. En su experiencia operativa ellos prefieren tener configuraciones o despliegues de software más conservadores. Si algo anda mal, ellos dicen que DNSSEC tiene la culpa y que puede perderse la presencia en Internet por completo.

En Taiwán tenemos que trabajar mucho para mitigar situaciones de riesgo. ¿Cuál es nuestra estrategia de penetración de DNSSEC? Tenemos tres dimensiones. La primera, la aplicación de los contratos para involucrar a los registradores y solicitarles que respalden DNSSEC. Hemos visto objeción y seguiremos hablando con los registradores para aplicar DNSSEC a través de la aplicación del contrato.

El segundo componente. Estamos haciendo desarrollo de capacidades. Hemos hecho mucha capacitación en DNSSEC, práctico, operativo, con los operadores. Seguimos trabajando con los recursos en desarrollo de capacidades.

El tercer componente. Promovemos el hosting de DNSSEC. Si algún registrador o incluso un registratario que tiene un registrador que no tiene hosting, nosotros podemos, en la situación actual, proveerles a ellos el hosting o el alojamiento del DNSSEC. Esa fue mi presentación. Bien sencilla. Si tienen preguntas, aquí estoy. Gracias.

RUSS MUNDY: Gracias, Kenny. Bruce, ¿quiere continuar usted? Bruce Tonkin, de AUDA.

BRUCE TONKIN: Gracias, Russ. Quisiera ahora hacer una actualización sobre la implementación de DNSSEC en Australia en la zona .AU. Hace años que está pero la adopción ha sido bastante baja. Unos 1.400 dominios han sido firmados y un total de 3.2 millones de nombres. Un gran número de nombres los hemos analizado individualmente para tener algún tipo de sentido o idea de cuáles son las organizaciones que han firmado. Las corporaciones conocidas en Australia, solo tres de ellas han firmado Una, una consultora. Otra que es Accenture y otra que es Scania. No hay bancos. No hay organismos gubernamentales que hayan firmado. Son muy pocos los que han firmado. A excepción de estas empresas corporativas hay unos poquitos negocios, algunos poquitos registratarios, algunas compañías de

alojamiento que han firmado sus zonas con DNSSEC. Hay una gran concentración en el mercado entre estos tres grandes registradores, alrededor del 80% del mercado, las tres ofrecen DNSSEC pero es algo que se promueva entre los clientes de todos modos. Si uno es una pequeña empresa y no conoce qué es DNSSEC va a los grandes registratarios y verá que no hay zonas firmadas. Eso se hace en realidad a través de los equipos de atención al cliente más que a través de una interfaz en línea. Un recurso conveniente que permite firmar en línea. El proceso es complicado.

A excepción de estas tres empresas grandes, la otra gran categoría es la industria de la pornografía. Parece que para ellos la seguridad es más importante que para los bancos. La pregunta sería por qué ha sido tan limitada la adopción. Yo he hablado con una de las grandes empresas de telecomunicaciones en Australia y su perspectiva, me dijeron, es que como hay tan pocos resolutores de DNSSEC en el mercado que chequeean las firmas de los DNS en sus resolutores, ellos temen que si los clientes no pueden llegar a los sitios van a culpar a la compañía de telecomunicaciones, que es la empresa en cuestión por el mal servicio y que el gran competidor de esta empresa de telecomunicaciones pudiera entonces ocupar el lugar. Las compañías que no mantienen las firmas del DNS adecuadamente resultan en el bloqueo del cliente y eso da una

mala imagen al servicio. Se preguntan por qué no se puede llegar al sitio e inmediatamente asumen que hay un problema con la compañía de telecomunicaciones. Desde el punto de vista de la reputación, para ellos eso básicamente es una cuestión de competitividad. El problema en Australia requiere que consigamos que los ISP más grandes colectivamente empiecen a chequear las firmas de DNSSEC y la resolución de DNSSEC. Eso entonces les daría el incentivo a los bancos y a otras organizaciones a empezar a firmar sus zonas.

Una de las iniciativas en Australia ahora es la siguiente. Tenemos un proyecto que estamos patrocinando para desarrollar un sitio para testear. Cuando las empresas ponen sus nombres de dominio, nosotros chequeamos el sitio web y vemos qué características de seguridad tienen o tienen. Una de las cosas que vamos a chequear y notificar luego a la gente es esta, la firma de DNSSEC.

Creo que además necesitamos algún otro tipo de testeo. Es tentador registrar aquí las grandes marcas corporativas y armar sitios web con firmas falsas. Cuando esto aparece en la firma, aparece en una página donde no debería estar. Luego aparece un mensaje: “Contactar al ISP para saber por qué no tiene resolutores de DNSSEC”. Es desde el lado del cliente que le empuja al cliente a ir al ISP. Hay algunos sitios que cuando se

visitan aparece esta advertencia de que no está bien configurada la infraestructura.

Una de las tendencias en Australia es que empezamos a usar resolutores públicos. El resolutor de Google es muy popular. Otros como Cloudflare y Quad9. Al gobierno australiano no le interesa tener una zona firmada. Es la segunda zona más grande que no está firmada. La otra es gov.au. Estamos en este proceso de firmar gov.au. El gobierno ha llamado a licitación para un servicio de resolutores a ser usado por las agencias del gobierno que el resolutor del DNSSEC cobraría una tasa por eficiencia y bloquearía los usos de sitios que tienen malware u otro tipo de cosas.

Esos resolutores también chequearían las firmas de DNSSEC. En el área gubernamental hay un poquito de avance pero es lento. En resumen, en general, no tenemos demasiados nombres de dominio firmados. Una de las razones es la ausencia de resolutores en Australia entre los ISP de las empresas de telecomunicaciones que chequeen DNSSEC. Por eso deberíamos trabajar en forma colectiva para usar y tener resolutores apropiados en las redes y después de eso podríamos pasar a promover la firma de los nombres de dominio.

RUSS MUNDY: Gracias, Bruce. ¿Hay alguna pregunta para Bruce? Paul, adelante.

PAUL: Con respecto al comentario sobre la reputación de las empresas de telecomunicaciones, yo me imagino que es más una preocupación o inquietud sobre los costos. La pregunta que tengo es la siguiente. Las cifras son de hace dos años, de Comcast. Tenemos medio billón de queries por días. Hay alguna cuestión relacionada con DNSSEC. La gerencia de Comcast no tendría problema en cobrar unos 25 dólares por query. Yo diría que el costo de soporte de un ISP para el caso de que una zona haya crecido ha bajado radicalmente.

BRUCE TONKIN: No sé si entendí.

PAUL: Medio billón de queries por día resulta en un número muy importante por mes, un buen porcentaje.

BRUCE TONKIN: Si usted tiene datos sobre esto, me gustaría conocerlos. Sería muy útil.

PAUL: Tendría que hablar con el equipo de Comcast.

BRUCE TONKIN: Es una comparación de costo de servicio y lo que se está haciendo actualmente.

RUSS MUNDY: Un comentario que tendría que haber hecho al comienzo. Estamos en una sala que tiene servicios de traducción simultánea. Les vamos a pedir que intenten hablar de manera lenta para que los intérpretes puedan seguir la presentación. También debemos siempre decir nuestro nombre, no olvidar decirlo. Yo soy Russ Mundy y tengo una pregunta para Bruce.

Considerando las estadísticas sobre la adopción, el trabajo de APNIC, Geoff Huston ha trabajado con otros pero básicamente estas estadísticas son de Geoff. Incluyen el uso de los resolutores públicos de DNSSEC. ¿Ha tenido alguna interacción con Geoff, con alguien en la organización de Geoff para ver si hay informaciones posibles basadas en ese trabajo que ustedes hacen, que podrían usarse para convencer a las ISP? Teniendo en cuenta el hecho de que las ISP no tienen los datos y el flujo de tráfico que quieren por el hecho de que no tienen DNSSEC. Por ejemplo, van a Google o 999 para hacer validación.

BRUCE TONKIN: No sé si por defender la firma se conseguiría más tráfico. ¿Es eso lo que usted quiere implicar?

RUSS MUNDY: Las personas que usan Google o algún otro resolutor público no lo hacen por DNSSEC. Podría esto ser una buena medida o una buena comparación porque a menudo… No debería decir a menudo pero la razón por la cual la gente opera servicios públicos es porque ellos consiguen los datos y materiales con los que trabajar. Los proveedores de servicio de Internet también pueden adquirir información de los datos que vienen por el tráfico.

BRUCE TONKIN: Sí, monitoreo de datos de tráfico. Es posible. Creo que Geoff sin duda ha sido consultado en este proyecto de este sitio web para trabajar con pequeñas empresas para testear sus nombres. Esto está basado en el trabajo de los Países Bajos, un sitio web donde se pone un nombre de dominio y se hacen varios chequeos. Estamos trabajando con Geoff. El debate es cómo comprometer el DNSSEC, cómo determinar la calificación, el puntaje, cuánto vale DNSSEC, un punto, dos puntos. Tenemos este debate interno. Cómo hacer un sistema de puntaje. Pero si pudiéramos tener una combinación de los datos de Comcast y los informes de Geoff quizás les podamos brindar a quienes toman las

decisiones en el área técnica de los ISP datos válidos que les puedan resultar útiles. Sí.

RUSS MUNDY: Warren.

WARREN KUMARI: Una corrección de algo que dijo Russ. Al menos uno de los proveedores de DNS públicos grandes no recibe información. Recibimos una declaración de cuestiones de privacidad de 8.8.8.8 que no hacen este tipo de cosas, etc. La gran pregunta es por qué nosotros brindamos el servicio. Sencillamente lo hacemos porque muchos resolutores de los ISP o bien inventan respuestas o son muy lentos. La razón por la cual Google hace esto es porque una Internet más rápida significa que más gente pueda usarla para que más gente se conecte, así Google gana más dinero. No es totalmente altruista pero es un servicio que nosotros administramos para que la gente tenga respuestas rápidas.

RUSS MUNDY: Gracias.

WARREN KUMARI: Lo tenía que decir porque los abogados me obligan.

RUSS MUNDY: Barry.

BARRY: Otra corrección muy menor de lo que dijo Russ. Son intérpretes. No traductoras como dijo Russ. Es muy importante. Aquí, además del inglés tenemos francés y español. Lamentablemente no podemos hacer japonés.

RUSS MUNDY: ¿Alguna otra pregunta? ¿Algún otro comentario para Bruce? Gracias, Bruce. Ahora tenemos a David Morrison, de InternetNZ.

DAVID MORRISON: Sí, de Internet Nueva Zelanda. Hola a todos. Voy a dar mi presentación. Quiero pasar a la próxima pantalla, por favor. Quiero darles una presentación no tan técnica acerca de la adopción de las DNSSEC en Nueva Zelanda. Nosotros tenemos una práctica especificada en nuestro sitio web. Lo pueden consultar. Les cuento un poco que comenzamos en 2012 con la implementación de las DNSSEC. Hemos evolucionado nuestras operaciones, nuestras operaciones clave. Logramos una muy buena evolución y tenemos un plan de recuperación ante desastres y continuidad de nuestras operaciones comerciales.

Tenemos 88 registradores autorizados y solo 2 ofrecen firma de las DNSSEC y 7 ofrecen soporte para registros DS. Tenemos mucho trabajo por delante, como dijo Bruce también con respecto a .AU. Estoy tratando de avanzar a la próxima diapositiva, a ver. Me está costando un poquito. Lo logré.

Nosotros tuvimos éxito en .gov.nz, que tiene firma de DNSSEC en el 41% de los nombres dentro de este dominio así que es un muy buen grado de adopción. El gobierno en Nueva Zelanda hizo una licitación para nuevos registradores y uno de los requisitos era proveer el servicio de las DNSSEC porque estamos pasando a una nueva plataforma. De los 714.000 dominios tenemos una muy baja adopción de DNSSEC. Si vemos los nombres más populares y vemos el tráfico del DNS vemos que solamente 195 de los sitios web principales en Nueva Zelanda utilizan esta tecnología. Hay mucho por hacer. Trabajamos con nuestro equipo técnico para tener el sistema DANE y SMTP. Creo que estamos haciendo un buen trabajo al respecto. Tenemos proveedores de servicios de Internet muy importantes que permiten lograr una cobertura en el 60% de todos los usuarios de Nueva Zelanda que tienen servidores que están validados.

Bien. Tenemos que trabajar educando a los usuarios finales en todo el ecosistema, a los registradores para que todos entiendan la complejidad de esta tecnología y en los últimos años tenemos nuevas tecnologías para automatizar los procesos de las

DNSSEC. Queremos educar a las personas para que entiendan que no es tan complejo como parece. Además, también tenemos que ver el tema de la economía del cambio. Tenemos que ver, por ejemplo, lo mismo que pasó cuando se adoptó el protocolo HTTPS, el IPv6. Tenemos que abordarlo de la misma manera.

Por último, en cuanto a la adopción por parte de los registradores, no creemos que vayamos a obligar a los registradores a que trabajen con DNSSEC sino que más bien queremos incentivarlos para que entiendan que le pueden brindar un mejor servicio en términos de seguridad a sus clientes. Esta es la breve reseña que les quería dar acerca de esta situación en Nueva Zelanda. Muchas gracias.

RUSS MUNDY: ¿Alguien tiene una pregunta? Sí, adelante.

JOHN: ¿Cuál es el proceso para lograr un registro del DNS en la zona si ustedes no tienen DNSSEC?

DAVID MORRISON: Es una pregunta técnica y no estoy capacitado para responder ahora pero puedo buscar la respuesta y dársela más adelante.

RUSS MUNDY: ¿Alguien tiene más preguntas para David? Si nadie tiene una pregunta, yo tengo una. Veo que hay un alto nivel de adopción en cuanto a validación. Usted dijo que eso se debe principalmente a que los ISP más importantes adoptaron la validación. Desde esa adopción de la validación, ¿ve algún cambio en la cantidad de zonas firmadas? Es decir, ¿la mayor validación da como resultado un efecto observable, medible?

DAVID MORRISON: No. Dadas las cifras que tenemos, no, no es significativo ese aumento.

RUSS MUNDY: ¿Tienen algún programa educativo de capacitación que estén tratando de implementar, sobre todo teniendo en cuenta la cantidad de validadores que ya tienen? Quizá lo puedan hacer con sus colegas de Australia, la región, para educar a las personas.

DAVID MORRISON: Tenemos un programa que vamos a comenzar a analizar con un operador de ccTLD y con nuestra comunidad de registradores en el próximo año y las DNSSEC serán parte de este programa en lo que respecta al tema de la seguridad en Nueva Zelanda. Sí, vamos a abordarlo desde el costado de la seguridad. También

queremos trabajar con los registradores con este objetivo específico.

RUSS MUNDY: ¿Alguien más tiene alguna pregunta para David? Si no hay más preguntas, le agradecemos a David por su presentación. Ahora vamos a tener la presentación de Yoshiro Yoneya de JPRS. Es parte de una de nuestras entidades anfitrionas.

YOSHIRO YONEYA: Hola. Buenos días. También soy miembro de la junta del dominio .JP del ccTLD en Japón que tiene una comunidad muy activa. Les voy a hablar acerca de cómo está la implementación de las DNSSEC y también acerca de nuestras actividades de difusión y alcance. En primer lugar, les quiero hablar acerca de la situación de las DNSSEC en Japón y de su implementación. Tenemos algunos ISP principales que brindan validación de DNSSEC a sus usuarios. Algunos de ellos proveen un servicio completo y otros lo proveen de manera optativa porque hay muchos ISP que todavía están muy preocupados por un posible fallo o una falla de las DNSSEC porque si los usuarios se ven afectados por esta falla de las DNSSEC, los operadores de soporte tienen que asistir a los usuarios y los operadores de soporte no conocen la causa raíz de la falla. Como también dijeron, el costo operativo se está tornando cada vez más alto.

Con respecto a la firma de DNSSEC vemos que tenemos muy pocas zonas firmada en Japón. En la tabla vemos ciertas organizaciones que son muy importantes y que han firmado la zona. Por ejemplo, los organismos gubernamentales que tienen alrededor de 800 agencias pero solo 15 han firmado las DNSSEC. Pueden ir al sitio web dnsops.jp con todos los detalles que vemos en pantalla para ver estas estadísticas.

Muchos operadores de DNS esperan que cobre impulso la implementación de las DNSSEC. Por ejemplo, los juegos olímpicos de Tokio en 2020 van a impulsar la implementación de las DNSSEC porque constituyen una parte importante de la ciberseguridad y permiten mitigar incidentes de seguridad. También vamos a tener en mayo próximo de este año la reunión del G20 en Osaka y también un campeonato mundial de rugby en este mismo año en nuestro país. Todos ellos implican la necesidad de contar con un alto nivel de ciberseguridad, con lo cual se utilizarán las DNSSEC para proteger a sus sitios web. Luego tenemos una mejora en los servicios de registros, registradores y proveedores de DNS. Lo que vamos a hacer es brindar un soporte de la criptografía de curva elíptica y también habrá soporte para gestión de claves y automatización de DNSSEC o DNSSEC automatizadas. Todavía no tenemos ningún anuncio oficial pero he conversado con los operadores correspondientes y me han indicado que procederán con estas

implementaciones. Soy optimista al respecto y espero que esto suceda en el futuro cercano.

Ahora les voy a contar acerca de nuestras actividades de difusión, de alcance con respecto al traspaso de la KSK en la raíz. En Japón comenzamos a informar y a generar conciencia acerca del traspaso de la KSK desde el año 2015. Comenzamos muy temprano. Brindamos muchas presentaciones en conferencias de Internet, en reuniones de grupos de redes de operadores que son muy importantes en Japón y también en reuniones de comunidades dentro del DNS y sus operadores. A veces utilizamos términos o expresiones muy fuertes como fragmentación de IP o interrupción del servicio en toda Internet. ¿Por qué? Queremos atraer la atención de las personas y convocarlas a estos eventos que realizamos.

También distribuimos documentos en japonés. Distribuimos documentos técnicos. Tenemos un comité técnico que tiene muchos documentos en inglés, al igual que la ICANN, pero hay muy poquitos en japonés. Muchos de nuestros operadores no manejan el idioma inglés con lo cual fue importante contar con la traducción de estos documentos.

El gobierno de Japón a través del Ministerio de Asuntos Internos y Comunicaciones está impulsando la implementación de las DNSSEC y también impulsó la preparación para el traspaso de la

KSK en muchos organismos gubernamentales. Esto realmente generó un muy buen impacto y una muy buena toma de conciencia sobre estos temas en Japón.

Como resultado, gran parte de los operadores del DNS en Japón realmente llevaron a cabo pruebas de producción muy, muy buenas, muy efectivas para el uso del software necesario para implementar estas tecnologías. Algunos de ellos fueron bastante críticos de los documentos técnicos correspondientes y, como resultado, hubo que trabajar con los documentos técnicos de la ICANN acerca de anclajes de confianza.

También llevamos a cabo encuestas dentro de la comunidad en Japón. Ustedes pueden ver los resultados en los enlaces que vemos en pantalla y un tercio de los ISP según los resultados de la encuesta indicó haber comenzado a brindar validación de DNSSEC. La mayoría de ellos indicó también otras características acerca de su servicio y también manifestó haberse preparado para una eventual falla del traspaso de la KSK. Con lo cual, los operadores en Japón realmente se tomaron muy en serio el traspaso de la KSK y se prepararon muy bien.

Con respecto al traspaso de la KSK, aprendimos lo siguiente. Como les dije, nuestros proveedores de servicios de Internet se prepararon muy seriamente para el traspaso. También utilizaron documentos técnicos que no les parecieron suficientes, entonces

prepararon su propio entorno de prueba. Como consecuencia de esta situación, creo que es muy importante contar con estos documentos técnicos para futuras pruebas y futuros entornos de prueba. También tuvieron un canal para hacer el monitoreo como un canal en Twitter y también un blog en tiempo real. Monitorearon un evento en tiempo real y necesitaban saber qué iba sucediendo a medida que pasaban las cosas.

Por último, quisiera decir que la comunicación bilateral entre los operadores es muy importante porque ellos nos dan comentarios, puntos de vista muy prácticos y muy realistas acerca de la parte operativa. Su conocimiento y el hecho de que lo comparten con otros es algo muy importante para prepararnos para estos eventos y para que todo funcione bien y para el éxito de la implementación de las DNSSEC. Gracias.

RUSS MUNDY: Muchas gracias. ¿Tenemos alguna pregunta para nuestro orador? Le agradecemos a Yoshiro. ¿Alguna pregunta para Yoshiro?

JOHN: ¿Ustedes están contemplando la automatización de CDNSKEY?

YOSHIRO YONEYA: .JP no se está encargando de esto pero sí hay algunos operadores y proveedores que se están preparando para implementar [CDNSKEY].

RUSS MUNDY: Tengo una pregunta para Yoshiro. En vista de esta preparación tan exhaustiva que hicieron sus ISP para el traspaso de la KSK, no sé si esa información se compartió por ejemplo si hicieron pruebas o procedimientos de pruebas por escrito y compartieron esos documentos. De todas maneras, sería muy bueno tener esa documentación y esos documentos para presentaciones en futuros talleres de DNSSEC. Si hay materiales o presentaciones o documentos disponibles y alguien los quiere compartir, los recibiríamos con todo gusto.

Por otra parte, y teniendo en cuenta el grado de preparación y la cantidad limitada de firmas que lograron, no sé si recuerdo bien la cifra pero había alrededor de 800 agencias gubernamentales y muy pocas tienen zonas firmadas. ¿Usted cree que habrá una mejora o una mayor cantidad de zonas firmadas antes de estos acontecimientos sobre todo por parte del sector gubernamental?

YOSHIRO YONEYA: Con respecto a su primer comentario, muchos de los operadores japoneses son muy tímidos y no quieren explicar sus experiencias o compartirlas en público. Si se puede garantizar su anonimato, entonces sí, podemos compartir nuestras experiencias. Espero que tengamos interpretación en japonés<>inglés y traducción también.

Como les mencioné, los juegos olímpicos son un evento internacional y realmente serán el motor de la firma de las zonas de las DNSSEC en los organismos gubernamentales. La información que les brindemos a los turistas o a los periodistas es muy importante. Es muy importante para nosotros en Japón la confidencialidad de la información. También es muy importante porque si se publicara información falsa en un sitio web falso, el usuario tiene que estar protegido. Hay que proteger al usuario de la información falsa. Espero que muchos organismos gubernamentales y algunos portales digitales de noticias firmen su zona de DNSSEC y tengan la certificación correspondiente.

RUSS MUNDY: Una última pregunta sobre este tema. ¿Ha visto algún aumento de la adopción de DNSSEC en especial en relación con DANE y el encriptado de correo electrónico, la criptografía? ¿Ha habido

alguna modificación de la tendencia o no hay algo que tenga especial visibilidad?

YOSHIRO YONEYA: No veo para nada DANE en Japón.

RUSS MUNDY: Muchísimas gracias, Yoshiro. Nuevamente, quiero agradecer en nombre de todos los presentes a los panelistas por las presentaciones. Ha sido muy útil y muy interesante recibir información de primera mano de lo que está ocurriendo. Espero que a partir de ahora podamos ayudarnos mutuamente y avanzar. Veo que estamos adelantados algunos minutos del programa. Eso permitirá que Bruce termine su presentación y después nos permita ir al café a tiempo. Bruce, si quiere comenzar entonces con su presentación sobre la transición del DNSSEC. Bruce.

BRUCE TONKIN: Por supuesto, aquí estoy. Primero en respuesta a una pregunta previa acerca de qué pasa si una pequeña empresa pone una entrada de DNSSEC y el registro no lo soporta, por lo menos en Australia la respuesta general sería que se transfiera a un registro que sí lo tenga. En el mercado hay distintos registros y registradores que ofrecen distintos servicios. Recomendamos

entonces que aprovechen la oportunidad de transferir los nombres a un proveedor de servicios que tenga DNSSEC. Esa sería la respuesta más general.

Primero algunos antecedentes. .AU, yo trabajo para el administrador. Somos el backend del registro .AU. Hicimos la transición de Neustar a Afilias en 2008. Opera varios servidores: com.au, net.au, org.au y otros. Son los nombres de servidores que surgieron en Estados Unidos: .COM, .MIL, .EDU, etc.

Operamos entonces el TLD de .AU. Operamos las registraciones y tercerizamos las operaciones de DNS para el segundo nivel. El año pasado hicimos la transición de 3.2 millones de nombres de dominio al nuevo registro. La meta era completarlos para el 1 de julio. Las cosas que complicaron la transición fueron: Primero, era la mayor de la historia. Más de tres millones de nombres. Se complicó en varios niveles. No solo teníamos nombres en segundo nivel sino también tercero y cuarto y quinto nivel en muchos registros. Por ejemplo, teníamos escuelas en el estado de New South Wales en el dominio educativo. La transición de los nombres de dominio además de los registros DS se daba a múltiples niveles. En algunos casos hasta cinco niveles de transición.

El registro hizo la migración el 1 de julio. El abordaje que quisimos tener debido a la escala y la complejidad era tratar de

completar lo más posible en el mes previo al 1 de julio para que el punto de corte de la migración tuviera un mínimo de cosas que hacer. Tener 48 horas para el corte y lo logramos hacer en menos de 24 horas porque gran parte del trabajo ya se había hecho.

Con respecto a los registros del DNSSEC, registramos los nuevos servicios con el nuevo operador en paralelo con los servidores del nombre del anterior y también empezamos a introducir la mayor parte de los registros a medida que atravesábamos las distintas capas para poder ponerlos en la caché por lo menos y luego permitir que se propagara la constelación de servicios del DNS en torno a ellos. También pudimos hacer gran parte de las pruebas, de los testeos con antelación. Hicimos primero en backend antes de hacer en producción para verificar que la configuración fuera la adecuada.

Veamos los pasos. Sé que la mayoría de ustedes en esta sala son expertos pero pensé que sería útil tener de alguna manera documentado el abordaje que hicimos. El primer paso fue hacer el traspaso de nuestras claves a una frecuencia quizá más alta de lo que maneja la ICANN. Tenemos un traspaso de la clave, que lo hacemos todos los años. Hemos hecho varios traspasos de KSK en los últimos años. Hicimos el traspaso de la ZSK cada trimestre. Básicamente, cada 90 días hacemos el traspaso de la

ZSK. Lo que dijimos conscientemente es no hagamos un traspaso de la KSK en el medio de la transición.

El primer paso fue congelar estos traspasos. No traspasar. El siguiente paso fue generar los nuevos KSK. Generar entonces nuevas claves para los niveles teniendo en mente que no íbamos a hacer la transición de la KSK para el nivel superior porque eso estaba corriendo el .AU de nivel superior pero sí hicimos la transición de los niveles inferiores. .COM, .NET, etc. Para cada uno de los niveles generamos nuevas KSK, ZSK y los registros DS relevantes. Luego enviamos estas claves al operador de registro actual. Él publicó las claves en las zonas. Para entender la jerarquía publicamos un registro de DS. El operador actual publica el registro de la clave en el siguiente nivel de .AU y para los niveles que le siguen. Eso se publicó el 5 de junio. Casi un mes antes de la transición que era el 1 de julio ya habíamos publicado los registros de DS en todos los niveles de la jerarquía, a excepción de .gov.au, que lo reservamos para el día de la transición. No firmamos .gov.au en ese proceso.

Algunos detalles más. El operador nuevo configuró los servidores de nombres en paralelo con el operador existente. El operador nuevo comenzó a publicar las zonas que fueron firmadas por el operador previo. Comenzó el 25 de junio. Antes de esta fecha venía recibiendo copias de la zona. Se hacía un query del servidor de nombres. Podía ver que la respuesta aparecía activa.

Los registros SOA, cuando se publicaban, el público podía ver esos servicios antes de esa fecha pero el 25 de junio pusimos los registros de los servidores de nombres en vivo y el público podía empezar a firmar las zonas.

Luego redujimos los tiempos de vida con los distintos registros de DS y también el SOA, redujimos el tiempo de vida a 300 segundos. Eso lo logramos el 26 de junio. Una semana desde que publicamos las zonas corrientes en los servidores de nombre, la zona fue firmada por el operador anterior, luego redujimos el TTL de algunos registros y eso nos permitió hacer los cambios con bastante rapidez. Luego el operador actual dejó de brindar servicio a las zonas el 26 de junio. En este momento el nuevo operador ya estaba haciendo todos los servidores de nombres de DNS públicos pero el operador previo estaba creando las zonas que se actualizaban todos los días con nuevos registros de nombres y el operador previo estaba firmando las zonas usando la infraestructura de firma de clave.

Luego, el 30 de junio cerramos a los registradores, los congelamos, para que no pudieran hacer ningún cambio de los registros. Aquí se hizo un congelamiento para que no se pueda hacer ningún tipo de cambio de la zona. El nuevo operador luego comenzó a generar las zonas y a firmar las zonas utilizando sus claves. Todavía tenemos los registros de DS de las claves anteriores del operador anterior, que estaban todavía

publicadas en la zona pero estábamos firmando usando la infraestructura de firma de clave del operador nuevo. Eso ocurrió el 30 de junio. Luego, el 1 de julio comenzamos el corte de la migración y ahí el operador publicó los registros con sus propias claves de firma. Después de eso removimos los registros DS y DNSKEY de la zona y aumentamos los tiempos de vida a 900 segundos. Esa fue la serie de pasos.

Unos cambios más recientes. Mencioné la frecuencia de traspaso de las claves. .AU, hacemos la ZSK una vez por año. Eso es un error. Debería decir KSK. La KSK es 2048 bits y la ZSK en 1280 bits. Hubo un pedido del gobierno de aumentar el nivel de encriptación que teníamos para la clave de firma o en realidad la longitud de la clave. Ese entonces fue un cambio que pusimos en práctica para que la KSK pasara a 2048 bits que es bastante sólido considerando que el traspaso se hace una vez por trimestre. Me gustaría saber qué están haciendo los demás con respecto a la longitud de sus claves, si también han aumentado el tamaño del paquete de una manera similar a lo que nosotros hacemos. Me gustaría saber cuáles son entonces las otras acciones. Esto lo hemos hecho siguiendo las recomendaciones del gobierno australiano. Me parece que esto es todo a tiempo para el café.

RUSS MUNDY: Gracias, Bruce. Seguramente hay preguntas. Veo a Paul.

PAUL: ¿Cuál es el algoritmo que está usando para las claves?

BRUCE TONKIN: Acabamos de actualizar los módulos de firma y soportamos algoritmo de curva elíptica. Vamos a pasar a esto. La realidad es que no queremos cambiar demasiadas cosas a la vez. Lo que estamos cambiando ahora es la longitud de la clave. Esto está en suspenso pero la idea es pasar a algoritmos y curva elíptica también.

PAUL: Ese será otro ejercicio muy interesante. Le deseo buena suerte.

BRUCE TONKIN: Es una zona muy grande y la infraestructura crítica en Australia es importante así que queremos ver primero cómo lo hacen otros con zonas más pequeñas y nosotros después entraremos gradualmente.

ORADOR DESCONOCIDO: Tenemos participación remota. “Soy Mohamed, un NextGen. Una pregunta para Bruce y Yoshiro: ¿Existe algún tipo de

colaboración con las universidades o las instituciones académicas que les permitan aumentar el conocimiento y así que más pequeñas empresas y usuarios lleguen a firmar sus dominios?" Esa es la pregunta.

YOSHIRO YONEYA: Para ser franco, consultamos. Hicimos una consulta con el público y las universidades y la academia son parte del público pero no tenemos una sesión o un tutorial especial para el mundo académico, para las pequeñas empresas porque el alcance es bastante estrecho y los recursos son limitados. Este tipo de actividad no se ha hecho antes. Si la implementación del DNSSEC fuera más amplia, podríamos hacer estas actividades pero en este momento no lo hemos hecho.

DAVID MORRISON: En Nueva Zelanda tampoco tenemos actividades en el espacio académico de DNSSEC. No obstante, sí hemos trabajado con los grupos de operadores haciendo un trabajo de educación en nuestras organizaciones sobre validación. Es algo que hemos explorado. La respuesta sería similar. Nuestros recursos son limitados pero esperamos cambiar el año próximo.

BRUCE TONKIN: Igualmente. Tampoco tenemos demasiada participación o consulta con las universidades sobre DNSSEC. Considerando la lista de nombres firmados, veo que hay una universidad que sí ha firmado. Por lo menos así lo ha indicado. Es la Universidad de Bond en el norte de Australia. Ninguna otra universidad tiene zona firmada pero está disponible en .edu.au para quienes quieren usarlo. Creo que corresponde decir que la relación con las universidades se da más a nivel del departamento de política. Es como en ICANN, donde hay más abogados que gente técnica.

RUSS MUNDY: Un comentario que yo tengo en relación con esta pregunta es que cada vez hay más universidades que vienen desarrollando y promoviéndose a sí mismas o promoviendo programas de estudio en el espacio cibernético, en el tema cibernético. No sé si hay una posibilidad. La empresa para la cual yo trabajo se relaciona con universidades en muchas de estas cosas. He visto muchos programas de estudios, temas tales como desarrollo de DNSSEC, fundamentos de DNSSEC. Quizá podrían incluso conseguir el apoyo de estudiantes en programas de mentoría, ese tipo de cosas. Es una posibilidad.

BRUCE TONKIN: Tenemos un miembro del consejo universitario, Nigel [inaudible], de la Universidad de New South Wales. Levante la

mano. Está aquí con nosotros. Sí. Tenemos algún tipo de relación con las universidades.

DAVID MORRISON: Tenemos un contacto con las universidades en el área de investigación. Tenemos un programa de subvención para investigación. Quizá en el futuro podemos alentar la investigación en el área de la adopción de DNSSEC. Debemos seguir evaluando este espacio.

RUSS MUNDY: ¿Esa era la única pregunta en línea, [Kathy]? Muy bien. ¿Alguna otra pregunta para Bruce y para esta última presentación? Bueno, debo decir que hemos sido sumamente puntuales. Es casi la hora del café. A las 10:30 reanudamos. Muchísimas gracias, Bruce.

[FIN DE LA TRANSCRIPCIÓN]