SAN JUAN – DNSSEC para todos: Una guía para principiantes
Domingo, 11 de marzo de 2018 – 17:00 a 18:15 AST
ICANN61 | San Juan, Puerto Rico

WES HARDAKER: Bienvenidos a todos. Esta es la charla de DNSSEC para principiantes, la guía del principiante. Al final de esta sesión van a haber entendido los conceptos básicos de cómo funciona el DNSSEC para proteger la infraestructura del DNS. ¿Todos los que están atrás me escuchan? ¿El audio funciona bien? Muchas gracias. Vamos a ver DNSSEC y cómo funciona. Vamos a empezar desde el principio. Desde el amanecer del DNSSEC. Vamos a hablar de los orígenes, del año 5000 a.C.

Voy a contar esto como la historia de Ugwina. Ugwina vive en una cueva en el borde del Gran Cañón. En un momento esto va a resultarles importante, saber dónde vive. Ahora espero que lo puedan ver mucho mejor. La linda foto de Og que también vive en una cueva del otro lado del Gran Cañón. Realmente es un largo camino. Hay que bajar y subir y Ugwina y Og son muy buenos amigos pero no conversan mucho porque es muy difícil cruzar el Gran Cañón. Una de las pocas veces que se ven, ven que sale humo de la fogata de Og y pronto empiezan a conversar en forma frecuente utilizando señales de humo hasta que un día el

cavernícola Kamisnky, que fue responsable de un ataque de DNS en 2008, se mudó al lado de Og y empezó a mandar señales de humo también.

Pobre Ugwina, del otro lado del otro lado del Gran Cañón. Está muy confundida. No sabe a qué señal de humo creerle. Ugwina empieza a descender por el cañón para tratar de dilucidar todo esto. Ugwina y Og consultan con los sabios del pueblo. El cavernícola Diffie, que tomó el nombre de una criptografía usada en DNSSEC, Diffie piensa que puede tener una buena idea. Se levanta y corre rápidamente hacia la cueva de Og y en el fondo encuentra una pila de arena coloreada que solo está en la cueva de Og, en ningún otro lugar. Sale corriendo y tira parte de la arena sobre el fuego y el humo se vuelve azul. Ahora, Ugwina y Og pueden conversar felizmente sabiendo con seguridad que nadie puede interferir en su conversación. Ahora tienen una forma mágica de detectar cuando alguien manda una señal falsa. Esto va a ser importante más adelante. Este es entonces el diagrama general de DNSSEC y cómo funciona. Ahora vamos a entrar en esto en detalle.

Yo trabajo para una universidad del sur de California. Dan es la persona que siempre organiza esto pero no pudo venir aquí. Hoy van a tener que escucharme a mí. Lo que es más importante, al final de la sesión podrán acercarse a hacer preguntas. Si tienen preguntas, vayan anotándolas. Tenemos una enorme cantidad

de expertos en DNSSEC aquí que pueden ayudarnos a responder cualquier pregunta que ustedes puedan tener.

Hablemos en general del DNS. Seguramente ustedes ya saben cómo funciona el DNS a nivel superficial. Después vamos a ver los detalles. El DNS está estructurado como un árbol. Un resolutor sabe dónde está la zona raíz y cómo empezar todo el proceso DNS y recorre el árbol DNS de arriba hacia abajo y en cada nivel se refiere al resolutor del próximo nivel hasta que finalmente se responde la pregunta. El resolutor avanza por ese árbol hasta llegar a la respuesta y después la lleva a quien la hizo.

Una cosa importante es que el resolutor pone toda esa información en la memoria caché para usos futuros. Si ustedes vuelven a www.icann.org en un segundo, los resultados van a encontrarlo más rápidamente porque recordarán esa información por un tiempo. No todo recorre el árbol siempre. Hay un tema importante. Cuando se diseñó el DNS, no tenía seguridad. No había forma de saber, como las señales de humo que vimos antes. Recibimos dos respuestas de dos personas y hay que elegir a cuál creemos. No hay forma de saber cuál es la correcta. Los nombres se pueden usurpar fácilmente y una vez que esa información errónea está en la memoria caché, una vez que alguien envenenó la caché de los resolutores, uno va a

volver a ese mismo lugar, una y otra vez hasta que se vence el tiempo en que la información está en la memoria caché.

Como no alcanzaron las historietas anteriores, ahora es el momento de hacer nuestra pequeña representación teatral. ¿Quiénes ya la vieron? ¿Quiénes son los que siguen volviendo simplemente para ver esta representación y por eso están aquí? Tengo algunos actores que me van a ayudar hoy aquí. Vamos a representar cómo funciona DNS. Les vamos a mostrar cómo funciona ese diagrama de árbol. Tenemos aquí algunos participantes. Ella es Cathy, que va a ser la raíz del DNS. Allí es donde empieza. Es la parte de arriba del árbol. Este es el director. Ustedes pueden decidir dónde se ponen.

Él es .COM. Sabe dónde está todo en .COM. Es Warren. Este es Russ, que va a ser .BANK. Yo voy a ser un usuario. Cuando tenga que hacer una operación bancaria, ¿qué hago? Me siento frente a mi computadora e ingreso. Tengo que verificar mi saldo bancario y ver cómo está. Ingreso: www.bigbank.com. Mi buscador busca el resolutor que está en mi ISP. Aquí tenemos ejemplos. Pero esta no es la pregunta correcta. Sí lo es. Nos apuramos. Llegamos a último momento y no estamos bien organizados. Voy a mi ISP y le digo: “Señor ISP, tengo que ir a www.bigbank.com para ver mi saldo”.

ORADOR DESCONOCIDO: Hola, Joe. Recibí tu pedido. Quieres ir a bigbank.com pero yo soy un ISP. Yo soy un resolutor y no sé nada. Tengo que ver dónde está bigbank.com. El primer lugar donde voy a buscar es en la raíz. Raíz, ¿sabe usted dónde está www.bigbank.com?

CATHY: No, señor. Pero sí sé dónde está .COM. .COM está en 1.1.1.1.

ORADOR DESCONOCIDO: Muy bien. .COM, ¿sabe usted dónde está www.bigbank.com?

WARREN KUMARI: No. No sé eso pero sí sé que bigbank.com está en 2.2.2.2. Pregúntele a él.

ORADOR DESCONOCIDO: Hola, bigbank.com. ¿Sabe usted dónde está www.bigbank.com?

RUSS MUNDY: De hecho yo sí sé dónde está www.bigbank.com. Está en 2.2.2.3.

ORADOR DESCONOCIDO: Muy bien. 2.2.2.3. Lo voy a recordar. Joe, la dirección de bigbank.com es 2.2.2.3.

WES HARDAKER: Ahora puedo ir a mi página web. Tengo un millón de dólares en mi cuenta. Maravilloso. Esperen un minuto, muchachos. Vamos a seguir. Así es como funciona el DNS hoy en día sin DNSSEC. Es el equivalente al resolutor Ugwina chateando con el servidor Og. Esto continúa así pero el problema es qué pasa cuando está por llegar el mal. No sé dónde está el mal. Vamos a hacer exactamente lo mismo, a la misma representación pero con un problema. Un problema importante en negro. Yo tengo aquí un millón de dólares. Me puedo comprar una propiedad. Voy a mi computadora y transfiero mi dinero a quien me va a dar la hipoteca. Entro a www.bigbank.com pero el navegador no sabe dónde está. Voy a ver si el ISP lo recuerda de ayer. Esto fue ayer, quizá no recuerde.

ORADOR DESCONOCIDO: ¿Cómo se llama usted?

WES HARDAKER: Soy Joe.

ORADOR DESCONOCIDO: Hola, Joe. Un placer conocerlo. ¿Quiere ir a www.bigbank.com? No sé dónde es. Primero voy a ir a la raíz. Hola, raíz. ¿Sabe usted dónde está www.bigbank.com?

CATHY: En realidad no lo sé pero puedo enviarlo hacia .COM. 1.1.1.1.

ORADOR DESCONOCIDO: 1.1.1.1. Buen día, .COM. ¿Sabe usted dónde está www.bigbank.com?

WARREN KUMARI: No, no sé. Lo siento. Pero sí sé que el servidor de nombres de bigbank.com está en 2.2.2.2. Pregúnteles a ellos.

ORADOR DESCONOCIDO: 2.2.2.2. Muy bien, conozco ese lugar. Hola, 2.2.2.2. Hola, señor bigbank.com. Quiero ir a www.bigbank.com. ¿Sabe dónde está eso?

DR. EVIL: En realidad sí lo sé. Sé dónde está. Está en 6.6.6.6.

ORADOR DESCONOCIDO: Interesante. Muchas gracias. Perfecto. Le voy a dar esa información al usuario. Joe, la dirección del banco es 6.6.6.6.

WES HARDAKER: Muchas gracias. Clic, clic. Transfiero el dinero. Listo. Ya está. Pueden ver cómo funcionan las cosas. En realidad, mi ISP, el resolutor, no tiene ni idea de si creer a la señal que vino de la gran caja negra o no, así que elige la primera respuesta que recibe. Como el malo de la película se adelantó, recibió esta información y le creemos. Ese es el equivalente a Ugwina, la resolutora, sintiéndose confundida. No sabe cuál es el Og verdadero y real.

Hablando de DNS en términos generales, en cualquier punto del árbol puede haber un envenenamiento. Podemos ver que todas las respuestas que recibe el resolutor desde arriba hasta abajo sean correctas. Si no lo es, puede parecer que hay dos Big Bank abajo. Uno que es el correcto y uno que no. No sabemos cuál recibimos.

DNSSEC es la solución para todo esto y ha sido desarrollado en las últimas décadas. La raíz ha estado firmada desde hace seis o siete años. 2010. DNSSEC utiliza firmas digitales para garantizar que la información es correcta. Esto es lo equivalente al humo azul, para que nadie pueda usurpar o interferir en una respuesta y causar confusión. Las claves y las firmas se utilizan para verificar que la información esté también guardada en DNS. Si está en la memoria caché, también queremos que esté en el DNS, para que se puedan verificar las firmas y los datos reales. Como DNSSEC es un sistema de búsqueda, se puede buscar

como cualquier otra cosa. Es decir, las claves pueden recuperarse a través de DNS también.

Un resolutor sabe cuál es la llave de la raíz. Tiene que saber dónde empezar. No puede memorizar las llaves de toda la jerarquía de DNS. Es demasiada información. Necesita un punto de inicio seguro. Lo hace con una cadena de confianza que empieza de la raíz hacia abajo. Cada nivel de la llave firma el nivel siguiente, el nivel subsiguiente, hasta que se completa todo el trayecto. Solo hay que conocer la llave de la raíz y así se va a ir verificando que cada respuesta sea correcta y se trabaje con un servidor autoritativo. El resolutor va marcando las respuestas correctas. Sabe de esta manera que el casillero rojo no es el correcto porque verificó que la firma no es la correcta. Espera, espera, hasta que llegue la respuesta adecuada.

Veamos cómo esto cambia con DNSSEC. Vamos a ver la misma representación, acto final, con DNSSEC incorporado. ¿Adónde va la pregunta? Otra vez voy a verificar mi saldo bancario para ver si se aprobó mi préstamo y si la transferencia se hizo.

Hola, raíz. Soy el resolutor y solo conozco la llave de la raíz. Sé que puedo confiar en que Cathy es la raíz porque este es mi anclaje de confianza. Mi sticker violeta es parecido al color del de ella, que es rosa.

WARREN KUMARI: Ahora yo debo darle mi firma a Cathy para que Cathy sepa cuál es mi firma. Aquí la tienes. Tenemos solo dos manos. Te voy a ayudar con el micrófono. Cathy, esta es mi firma. Es de un lindo color verde.

CATHY: La acepto. Me parece bien.

WARREN KUMARI: Ahora yo tengo que saber cuál es la firma de Big Bank. Hola, bigbank. ¿Cuál es su firma?

RUSS MUNDY: Hola, .COM. Mi firma es una flecha azul brillante y te la doy para que sepas cómo es firma.

WARREN KUMARI: Excelente.

WES HARDAKER: Ahora puedo ir al banco, ahora que se crearon todas estas cadenas. Mi resolutor no necesita conocer toda la cadena. Tiene que usar solamente un sticker. Es muy importante porque hay muchos resolutores, muchos ISP y solo se debe recordar un elemento de información. Todo lo demás es automático. Voy a

mi ISP y le digo: “Traté de conectarme con mi banco, www.bigbank.com. Quiero ir otra vez. ¿Me puedes ayudar?”

ORADOR DESCONOCIDO: Sí. ¿Cómo fue tu última experiencia con el banco? No sé dónde está bigbank.com. Lo siento. Voy a buscarlo. En primer lugar, voy a la raíz. Señora Raíz, ¿sabe usted dónde está www.bigbank.com?

CATHY: Hola otra vez. No, no sé dónde está www.bigbank.com pero sí sé dónde está .COM, 1.1.1.1. En primer lugar te voy a decir que la firma de 1.1.1.1. Tiene que ser así. Verifícala.

ORADOR DESCONOCIDO: Gracias. La voy a verificar. Voy a verificar mi firma y verifico la tuya. Muy bien. Los colores son iguales. Está bien. 1.1.1.1. Hola, .COM. Quiero ir a www.bigbank.com. ¿Sabes dónde está?

WARREN KUMARI: No lo sé pero sí sé que bigbank.com está en 2.2.2.2. Esta es mi firma y la firma de bigbank.com es de un azul muy lindo. Como este.

ORADOR DESCONOCIDO: Lo voy a verificar. Te verifico a ti, 2.2.2.2. Me verifico a mí. Verifico a la raíz. Verifico todo. Muy bien. Gracias. Voy a 2.2.2.2. Hola, bigbank. Quiero ir a www.bigbank.com. ¿Sabes dónde está?

DR. EVIL: En realidad sí, lo sé. Está en 6.6.6.6.

ORADOR DESCONOCIDO: Lo voy a verificar. Voy a verificar mi firma, la tuya. No. Esa no es la dirección correcta. Sal de aquí. Ándate. Seguridad por capa. Muy bien. Bigbank, soy yo otra vez. Quiero ir a www.bigbank.com. ¿Sabes dónde está?

RUSS MUNDY: Sí, lo sé. Muchas gracias por preguntarme. Tengo un sticker de un lindo azul que voy a poner aquí y que es igual a la estrella que tienes tú. Muy bien. 2.2.2.3.

ORADOR DESCONOCIDO: Las firmas son válidas, todo es válido. Perfecto. Sé que eres quien dices ser. Hola, Joe. Esta es la dirección y te garantizo que esto es lo que estaba en la fuente de nombres.

WES HARDAKER: La vez pasada también me dijiste algo parecido. ¿Estás seguro?

ORADOR DESCONOCIDO: Esta vez sí.

WES HARDAKER: Muchas gracias por haber mejorado tus mecanismos de seguridad. Démosles un aplauso a los actores. Muchas gracias, como siempre. Fue brillante y maravilloso. Sigamos entonces a partir de aquí. Así como vimos antes, Ugwina puede verificar los mensajes y asegurarse de que las respuestas de DNS sean correctas.

A partir de aquí, le voy a dar la palabra a mi colega Russ Mundy, que les va a explicar por qué necesitamos DNSSEC. Le va a dar más información y más ejemplos de cómo funcionan estos ataques y cómo funciona el DNSSEC para que ustedes no sean atacados.

RUSS MUNDY: Voy a tratar de encontrar un lugar donde no me ciegue la luz. Algo más sobre el foco básico de por qué necesitamos DNSSEC. ¿Quién ataca al DNS? Nadie lo ataque porque quiera un ataque al DNS sino que atacan las cosas que el DNS soporta. Email, chat, acciones bancarias y mucho más. Cualquier cosa que se haga en Internet. Por eso la gente intenta atacar el DNS, porque así puede atacar aplicaciones.

Hoy hay muy pocas aplicaciones que se usen en Internet que no tengan DNS. Aquí vamos en la dirección correcta. ¿Cuáles son los resultados? ¿Cómo se pueden hacer estos ataques? Cuando uno hace un inicio de sesión, por ejemplo se conecta a la cuenta de correo electrónico, se lo hace desde la máquina local pero a veces cuando el email se manda a otro lugar, a veces hay que poner una contraseña que puede ser robada. Si se hace un login remoto a una computadora a través de una red, algo similar puede ocurrir. Es decir, hay aplicaciones que ayudan a prevenir el hurto de contraseñas. No obstante, hay otras que permiten que tal cosa suceda.

Si se hace secuestro del DNS a través de la interferencia de las comunicaciones del chat, uno puede hacer un escrutinio de todo lo que está pasando. Nuevamente, hay mecanismos asociados a esto que pueden servir para prevenirlo. Si alguien quiere más detalles de cuáles son estas aplicaciones avanzadas, pueden anotarse para el taller del miércoles del DNS donde se hará un par de presentaciones que darán muchos detalles para mejorar la seguridad del DNS, del correo electrónico y otras seguridades a través de las tecnologías disponibles hoy día pero lo que debemos recordar aquí, un concepto simple de lo que es el DNS, es que en el pasado explicábamos lo que era el secuestro del DNS. Ya no lo hacemos porque es un poquito aburrido. A lo largo de los años que hemos hecho esta presentación a veces nos

enteramos de que era ilegal explicar cómo se hacía un secuestro del DNS, por eso no lo hacemos más, por las dudas.

Hablemos de las herramientas disponibles. Hay muchas herramientas que hace por lo menos 10 años que están disponibles en la Internet que se pueden cargar en la computadora, configurar y secuestrar sesiones de DNS y otras sesiones que soportan DNS. Ustedes vieron el ejercicio, el sketch. Vieron a Ugwina, vieron el humo azul. El DNSSEC es como el humo azul. Cuando el usuario Joe finalmente recibió la respuesta de su ISP, si está firmada, eso es garantía de que la información recibida tiene lo que se denomina integridad de datos y autenticidad de la fuente. Uno sabe entonces que es la correcta y además se sabe de dónde proviene. Eso es lo que nos dice esto.

Aquí tenemos un ejemplo con imágenes que muestran al usuario Joe que envía un query, una consulta. Cuando el usuario Joe envía su query, va al resolutor recursivo local, su ISP, y luego sale a buscar la respuesta. La pregunta se formula, se da la respuesta y después que llega la respuesta él puede hacer lo que quería hacer, que es comunicarse con su banco. Esta es la ilustración pictórica de lo que vieron en el sketch. A veces es más difícil verlo en diapositivas o en figuras más que en un sketch. Es más fácil.

Cuando hacemos una marca, cuando vemos una tilde como esta, es una indicación de que la conexión pasó la comprobación de DNSSEC. Este es un ejemplo de un browser que fue modificado que permite visualizar las comprobaciones de DNSSEC. Este es un navegador que no fue modificado para usar el check de DNSSEC. Si miramos con cuidado, lo que vemos aquí es que el texto en ambos es el mismo… No sé por qué no está avanzando. Ahora sí.

Aquí está el Dr. Evil. Nuevamente se hace la pregunta, va al servidor recursivo pero qué pasó. Llegó el secuestrador, que está ahí sentado y dijo: "Aquí tengo un query. Yo voy a adelantarme y le voy a dar la respuesta". Eso es lo que hace. Cuando hace eso, en lugar de apuntar al sitio web correcto, el doctor del mal va a redirigir a otro a su propio sitio web. Mientras otras queries van y vienen con respuestas, el browser del usuario Joe ya fue al sitio web del Dr. Evil.

Con DNSSEC, cuando la respuesta regresa y falla la validación del DNSSEC, en lugar de ir al sitio web del Dr. Evil, va al sitio web real. Entonces Joe recibe la respuesta correcta. En este caso, lo que hicimos es lo siguiente. Estas son imágenes de pantalla de un secuestro real de DNSSEC que hicimos hace un tiempo. El navegador que ven ahí arriba tiene DNSSEC mientras que el browser que vemos abajo no tiene DNSSEC. Fíjense que el contenido en la página no es el mismo ya. De hecho, lo que se

hizo en esta ilustración, aquí ejemplificamos cómo se puede hacer un hijack o un secuestro del DNSSEC es insertar información.

Este es el mismo sitio web con una pequeña diferencia. Esta URL y este nombre de DNS están indicando que fueron secuestrados y el usuario cree que está viendo la información correcta pero no es así. Está viendo información agregada. Esto se hizo en la época en la que Steve Crocker era el presidente de la junta. Todos los conocían. La mayoría de la gente aquí probablemente lo siga conociendo. Él dice que el DNSSEC no va a resolver el hambre en el mundo.

¿Cuántas queries del DNS se dan al mismo tiempo? Para una página, la cantidad de queries y respuestas que se requieren para completar una página. Esa es la misma página cinco años después. Fíjense que se van complejizando las queries del DNS antes de completar cualquier página antes de mostrarla en el navegador.

Aquí lo importante que debemos recordar es que lo que el DNSSEC hace es proteger la información del DNS propiamente dicha. No entraremos en los detalles de cómo esto se logra. Solo recuerden que la información en la zona del DNS es tan importante como el material criptográfico que se muestra en la zona del DNS, que se usa para cumplimentar las funciones del

DNSSEC. Aquí la cuestión entonces es que los datos de la zona del DNSSEC son retornados de manera validada al browser.

Otra ilustración de cómo va y viene la información. Esto es sin DNSSEC. Pensé que la siguiente también era una imagen pero tenemos más palabras. Algunas palabras sobre la implementación. Volviendo a esta imagen, si ustedes están aquí sentados en la localización del usuario Joe, con el cliente, y no corren DNS ustedes, tienen un tercero que lo corre por ustedes. Tienen que determinar de qué manera se van a proveer los servicios del DNS. Verán que algunas organizaciones que vienen a la ICANN son muy céntricas, están muy centradas en el DNS en sus negocios. Tienen muchísima experiencia y conocimientos sobre el DNS dentro de sus organizaciones y se ocupan de administrarlo solas, mientras que hay otros que no tanto.

Si en su organización conocen DNS y tienen información, probablemente vayan a administrarlo ustedes directamente. Las actividades del DNS son importantes pero pueden algunos no ser expertos, entonces se tercerizan o ustedes en su organización no lo hacen y lo hacen en otras partes de la organización. Esa es la parte de la organización que tenemos que considerar. Primero hay que preguntarse si vamos a hacer la administración nosotros del DNSSEC o lo va a hacer un tercero, lo vamos a tercerizar.

Como ven entonces, aquí la cuestión importante es proteger los datos de la zona. Asegurarnos de que esté validada para los usuarios o de que los usuarios la puedan validar. ¿Cómo se maneja en las operaciones del DNS? Hay que hacer un paralelo con la operación del DNSSEC. Será una capacidad adicional que se incorporará al DNS. Eso va a definir cómo se manejarán las actividades del DNS hoy día.

Cuando se incorpora la información del DNSSEC, como vimos en el sketch, para este intercambio de claves, cuando vuelve el servidor recursivo, cuando ha recopilado todas las claves y ha comprobado que son las correctas, en esta ilustración muy sencilla, aquí es donde la zona se firma y aquí abajo es donde se valida. Esos son los dos pasos adicionales, la funcionalidad adicional que se va a agregar a la operación del DNS y que ya se tenga, más allá de cuál fuera esta.

Como resultado, no importa cómo se opere el DNS, ustedes son el operador de DNS, saben que funciona, saben si están haciendo la firma y la validación del DNSSEC, una o las dos dentro de la organización. Si se terceriza, si no es la organización de ustedes la que lo hace directamente, tendrán que trabajar con el proveedor tercerizado para saber si él se lo puede proveer. Si no puede, les recomiendo que empiecen a buscar proveedores de DNS que puedan ofrecer capacidades de DNSSEC.

Estas eran entonces nuestras presentaciones. Como decía Wes antes, tenemos aquí varias personas en la sala que conocen el DNSSEC de arriba abajo. Les pido por favor que hagan preguntas y le doy la palabra a Wes.

WES HARDAKER: Gracias, Russ. Quisiera cerrar con un poquito más de información. No tenemos diapositivas todavía pero habrán notado que el DNSSEC viene continuamente agregando información y, si se fijaron en estas sillas que están libres, en realidad no estaban reservadas para nadie. Les pido que se acerquen. DNSSEC está en el momento de un cambio. Habrán notado que hay un humo azul. Los criptógrafos recomiendan cambiar a una clave diferente. Es como cambiar el color del humo. Hay un proceso para hacer eso, para hacerlo de manera segura. La mayoría de las personas ya lo saben. Cuando el humo cambia de color, si cambia de azul a verde, se pone azul y verde durante un tiempo para que Ugwina sepa que este es el nuevo color que tengo que empezar a buscar. Ese es el ejemplo más simple que se me ocurre pero así estamos ahora.

En la ICANN, la IANA están transmitiendo en este momento tanto azul como verde. En algún momento en el futuro vamos a quitar el color azul. Exactamente cuándo esto va a ocurrir, no sé. Hay algunos desafíos técnicos. Antes tenemos que asegurarnos de

que todos tengan la nueva llave porque todo tiene que funcionar. ¿Alguien tiene alguna pregunta sobre todo lo que vieron hoy? ¿El despliegue del DNSSEC? Por favor, presenten su pregunta y alguien les va a dar la respuesta. ¿Tenemos otro micrófono?

LENDON TELESFORD: Soy Lendon, de Granada. Antes de mi pregunta, felicitaciones por la presentación, el sketch y la ilustración. La verdad es que yo no soy un experto en este entorno. Soy fellow. Es mi primera vez. Me pregunto: La ilustración me parece que muestra que es esencialmente una cadena de confianza, ¿verdad? Yo no vi ningún mecanismo, quizá está oculto, entre el cliente y el resolutor. Me pregunto si hay manera de comprometer al resolutor.

WES HARDAKER: ¿Tenemos alguna estrella dorada? La pregunta que hizo es fantástica. ¿Alguien la puede responder? Viktor.

VIKTOR DUKHOVNI: Para aplicaciones que dependen críticamente de la seguridad con DNSSEC necesitamos un resolutor en la misma máquina donde se corre la aplicación y algo en el medio entre el usuario y el resolutor. La validación se da en la máquina propia y ahí uno

puede tener la certeza. Si se le pide al resolutor del ISP y no hay resolutor que haga validación en la máquina propia, hay problemas. El ISP no va a comprometerse con datos antiguos. Si parece dar la respuesta correcta ahora y cinco minutos después se le pregunta, él va a dar la respuesta correcta porque nunca dio la respuesta incorrecta. Era alguien en medio que dio la respuesta incorrecta cinco minutos antes que era el intermedio y ahora tiene la respuesta correcta.

WES HARDAKER: Otro dato más. El problema se llama el problema de la última milla. Todo lo que pasa arriba del resolutor puede resolverse técnicamente pero el cliente a veces no hace las cosas con seguridad. Una cosa es que hay que hacerlo en la máquina propia. Viktor es la persona que ayuda con la instalación de mails seguros. Es un experto.

Otro comentario es el siguiente. El IETF, que es el organismo que crea los protocolos de la Internet, cómo funciona HTTP, cómo funciona el mail y demás, en este momento está manejando la privacidad del DNS y asegurarse de que cuando se envía una solicitud del resolutor no haya un intermediario. Una conexión segura entre cada cliente y el resolutor. En el futuro, ese mecanismo de protección también se usará para privacidad y permitirá proteger al hombre en el medio. Va a ser una cadena

distinta del DNSSEC arriba pero va a proteger efectivamente. ¿Está claro? Russ.

RUSS MUNDY: Quería agregar que mucha gente se preocupa cuando yo digo: "Mecanismos criptográficos". A ver, esto lleva mucho poder de procesamiento y computación. Eso no es un problema con DNSSEC. Es otro factor considerando el diseño desde el principio. Yo no tengo conmigo el script pero solía llevar un celular conmigo que hace DNSSEC en el mismo celular, incluso estos dispositivos portátiles pueden hacer DNSSEC desde el mismo dispositivo. Ahí es donde eventualmente esperamos llegar, a este punto en que la validación solo se haga en los dispositivos, incluso en los más pequeños.

WES HARDAKER: Otra pregunta. ¿Andrew?

GERARD BEST: Soy Gerard Best, de Trinidad y Tobago. Voy a tratar de hacer una pregunta que también merezca una estrella dorada. Mi pregunta tiene que ver con los resolutores abiertos como 8.8.8.8. Recientemente se lanzó 9.9.9.9. Quiero saber las perspectivas de los expertos en cuanto a la utilidad o robustez de esos que mencioné como mecanismos de seguridad de DNS.

WES HARDAKER: Otra pregunta que merece una estrella. El mismo problema de comunicación que está entre usted y el resolutor. No hay forma de hablar de manera segura con los servidores de Google pero yo sé que hay alguien que puede responder su pregunta y que está aquí. ¿Warren? Warren, ¿podrías responder esto? Adivinen dónde trabaja Warren

WARREN KUMARI: Hola. Soy Warren Kumari. Trabajo para Google. Sí Los resolutores 8.8.8.8 son usados por millones de usuarios todos los días y hacen una validación DNSSEC completa. De hecho, el DNS público de Google y Comcast fueron los primeros resolutores públicos que empezaron a utilizar DNSSEC. Sí, hay una serie de personas que lo gestionan, que se toman el tema muy en serio. Creo es seguro. Yo lo uso pero cada uno debe decir si lo utiliza o no.

WES HARDAKER: ¿Hay alguien aquí de otra organización que pueda responder? ¿Puede responder si PCH hace lo mismo?

ORADOR DESCONOCIDO: Sí. Quad9 hace validación de DNSSEC. También tenemos una dirección de IP que pueden usar en el caso de que sospechen que alguna validación del DNSSEC creó otra dirección que no sea correcta. También tenemos DNS sobre TLS.

WES HARDAKER: Lo interesante de esta empresa es que hacen DNSSEC sobre TLS. Se puede proteger el mecanismo para ver que estemos obteniendo una respuesta correcta de parte del resolutor y también del ISP. ¿Hay alguna otra pregunta?

RAPHAEL VICENTE ROSA: Soy Raphael, NextGen. Vimos ese gráfico de cómo una pregunta simple que va a cnn.com se resuelve. Mi pregunta tiene que ver con el impacto en el desempeño, si tenemos DNSSEC sobre este gráfico o aquí ya vemos la intervención del DNSSEC.

WES HARDAKER: Esto lo creamos juntos Russ y yo. Una de estas partes es mi laptop y la otra es la suya. Esto lo hicimos hace bastante tiempo y sí, aquí vemos DNSSEC. Si miramos con cuidado, las líneas naranjas no tienen seguridad. La mayor parte de esto no tiene seguridad pero allí hay incluidos unos elementos verdes. Esto fue al principio de la implementación DNSSEC. Russ y yo hablamos de repetir esto y lo vamos a hacer. Quizá a fines de

esta semana porque este gráfico se vería mejor. Todavía hay muchas implementaciones por hacer. Con respecto al desempeño o performance, ¿alguien quiere contestar esto? Russ ya dijo algo al respecto. ¿Ustedes hicieron estudios con por ejemplo DNSSEC versus una conexión de TLS por la web?

ORADOR DESCONOCIDO: En la mayoría de los casos la infraestructura de DNS está en la memora caché. En general obtenemos respuestas un poco más grandes pero no se hacen más consultas en especial si somos un consumidor que hace una consulta a un ISP, vamos a hacer la misma pregunta y recibir la misma respuesta. Es el ISP el que quizá tenga que hacer algunas consultas adicionales pero esto no afecta a los usuarios. En general lo que busca el usuario ya está en la memoria caché porque muchos usuarios piden los mismos sitios.

WES HARDAKER: ¿Respondimos la pregunta con esto? Sí. Warren.

WARREN KUMARI: También hay algo más para decir aquí. En algunos casos, DNSSEC hace que las cosas sean más rápidas porque recibimos una respuesta y una prueba que nos dice que la respuesta es correcta. En esos casos, las respuestas negativas como por

ejemplo, cometemos un error de tipeo, eso se resuelve inmediatamente y también algunas respuestas que vienen de un registro que dice: “Cualquier cosa es compatible con eso”. Esa respuesta la recibiría directamente el resolutor sin tener que ir a consultar con todos los otros servidores autoritativos. En realidad, el aumento de la velocidad es muy pequeño.

WES HARDAKER: ¿Hay alguna otra pregunta?

ORADOR DESCONOCIDO: En términos del intercambio de la llave que se hace entre todos los servidores, ¿eso se da cuando se hace una pregunta? El usuario o la persona tiene que saber con quién está hablando. ¿En qué capa se hace un caché de las claves? ¿Cómo funciona eso?

WES HARDAKER: Excelente pregunta. La voy a responder yo. Recuerden, al principio dije que las claves se pueden buscar por DNS así como se busca cualquier otra cosa. Podríamos avanzar por una cadena muy compleja para ver cómo los requerimientos de DNS incluyen la capacidad de transferir la clave. No lo mostramos en nuestro sketch porque sería el doble de largo. En el proceso de ir a ejemplo.com, una de las cosas que haría el ISP es preguntar no

solamente dónde está www.example.com sino que también preguntaría cuál es la clave y verificaría la firma.

Ya vieron que la verificación de firma se hizo en el sketch pero en realidad se consultan y se verifican otras cosas en paralelo. Hay más cosas que suceden y hay dos o tres verificaciones de firma cuando vamos avanzando de un nivel al otro en el árbol. ¿Respondí su pregunta con esto? Bien. ¿Hay alguna otra pregunta?

ORADOR DESCONOCIDO: Entonces aparentemente la seguridad de todo este proceso depende de los pequeños stickers que usted repartió al principio del sketch. Eso es lo que más me confundió en ese sketch. ¿Cómo se organiza la entrega de estos stickers? ¿Con qué frecuencia hay que hacerlo? Quizá esto debería ser parte de la pregunta que hizo la otra persona.

WES HARDAKER: Excelente pregunta. Viktor.

VIKTOR DUKHOVNI: Yo quería hablar de esto. Si nadie lo planteaba, yo iba a hacer la pregunta. Unas cosas que no se mencionaron en el sketch es que gran parte de las historias de seguridad se dan no tanto entre el

usuario y el banco sino entre la autoridad de certificación y el banco, porque en el mundo real, dejando de lado el sketch, la seguridad real depende del certificado que obtuvo el banco y de si ese certificado es correcto o no.

La seguridad realmente se da en el momento en que la autoridad de certificación entrega el certificado al banco porque ellos saben que es el banco el que lo está recibiendo pero no, en realidad no lo saben. Es todo humos y espejitos de colores. En realidad las autoridades de certificación les dan a sus clientes los certificados y saben exactamente quiénes son. Esto se llama validación de dominios. Ustedes se sorprenderían de ver que eso es muy poco seguro. DNSSEC puede ayudar a aumentar la seguridad aquí. El foro de navegadores está agregando cada vez más elementos de DNSSEC para que los dominios firmados con DNSSEC tengan mayor protección en cuanto a se emita el certificado. Eso termina protegiendo al usuario.

¿Por qué hablo de los CA? Se dice que esa parte controla el dominio pero quien realmente controla el dominio es el registrador. Ustedes registran una cuenta, compran un dominio y ya está. Los stickers que reciben son publicados por el registrador en el DNSSEC y ustedes le dan al registrador los datos a través de un canal seguro. Ustedes firman un dominio, ustedes le dicen al registrador cuál es su sticker y el registrador lo manda al registro. No hay un tercero externo. La autoridad de

certificación no dice: “Ah, la llave de Big Bank es esta. Simplemente estamos suponiendo pero créannos que es así”. No. No es así. En realidad es el registrador con quien tenemos relación directa, no un tercero que presume de saber todo. Es el registrador el que publica la llave. Esto hay que hacerlo en forma periódica a medida que cambian las llaves. Si nunca cambiamos las llaves, nunca tenemos más stickers. Hay que coordinar. Si cambiamos las llaves hay que coordinar el traspaso de la llave con el registrador. Es un resumen porque no les estoy contando toda la historia pero espero que se entienda.

WES HARDAKER: Esto equivale a otro ejemplo. Si uno quiere registrar un dominio con un registrador, el registrador sería GoDaddy, por ejemplo, u otros. Cuando registramos un dominio, los que utilizan DNS tienen un casillero donde podemos poner nuestra llave. Esto es lo que agrega esa transición del sticker. El dueño de un dominio lo hace cuando está registrándolo. ¿Se entiende?

RUSS MUNDY: Quería mencionar la parte de mi presentación donde dije que la forma en que participan las organizaciones de los DNS existentes, ya sea a través de un ccTLD o un gTLD. Si ustedes, sean quienes sean como organización, manejan su propio DNS, quizá tengan también que manejar todos los mecanismos de

DNSSEC asociados con eso. Trabajando a través del registrador, mandando la llave directamente al sistema de DNS.

Si un tercero opera el DNS por ustedes, quizá lo opere el registrador, por ejemplo, y esto es muy común, el registrador mismo puede hacer todo esto. Hay recomendaciones en cuanto a la frecuencia de hacer un traspaso de la llave pero eso se puede automatizar. En la mayoría de los casos, la opinión general es que es mejor si todo está automatizado porque no hay personas tocando teclados que quizá se olviden de hacer un cambio que tengan que hacer. Un periodo de 30 días, seis meses o un año, según sea la frecuencia del cambio.

WES HARDAKER: Muchos registradores tienen un casillero que dice: "Si nosotros vamos a prestar servicios de DNS, dígannos si quieren que hagamos también el servicio DNSSEC". Muchos ya lo tienen como predeterminado. Ni siquiera nos preguntan.

MUJIBULLAH SHAMS: Soy Mujibullah Shams, becario de ICANN. DNSSEC firma las preguntas y las respuestas. Quisiera saber qué tipo de mecanismo criptográfico utiliza DNSSEC para firmar estas consultas y respuestas. La segunda pregunta es: Cuando se da

un traspaso, ¿qué tipo de mecanismo se utiliza para compartir la llave entre todas las partes?

WES HARDAKER: Es una buena pregunta. Es un mecanismo de llave pública-privada, parecido a la forma en que funcionan los certificados web, etc. El dueño, propietario de la llave tiene una copia y nadie puede tener una copia de esto y después reparte una llave o clave pública. Esto puede variar entre 512 y 4096 bytes. Hay un mecanismo para hacer una curva elíptica. Si ustedes saben esto, hay diferentes tipos de cosas que se hacen. En relación al traspaso, hay una recomendación de la IETF que define el mecanismo de traspaso. Si hablamos del traspaso de la KSK a nivel de la raíz, si ustedes son dueños de una zona, cuando tengan que cambiar la lleva tienen que dirigirse al registrador y actualizarla. En ese caso, los .COM van a publicar referencias a las dos claves por un tiempo. Después de un tiempo se pasan a la nueva llave. Hay un periodo durante el cual todo el mundo sabrá que ustedes tienen dos llaves y que las dos son válidas. En algún momento se retira la llave vieja. Fue una buena pregunta. Gracias.

WARREN KUMARI: Quiero decir algo al respecto. La llave anterior firma la nueva llave. Así es como se hace.

TARAU BAUIA: Hola. Soy de Kirabati. Dependemos de 8.8.8.8 y quiero preguntar si podemos saltear el ISP y utilizar el DNS de Google. ¿Podemos tener nuestro propio elemento recursivo o DNS duplicado en nuestra propia raíz?

WES HARDAKER: Ustedes pueden manejar un resolutor de validación de DNSSEC en su propia red. Eso lo pueden hacer con el de Google o el de Comcast. Creo que todos estos ofrecen resolutores de DNSSEC. Pueden usar esos que son abiertos o pueden usar uno propio. Los dos abordajes son posibles. Los abiertos y los más importantes hacen la mayoría de las validaciones DNSSEC. Hay una serie de consultas validadas que se dan, no sé cuál es el porcentaje, pero la mayoría viene de estos cuatro o cinco resolutores más importantes. Vamos a tomar una pregunta de la mesa ahora.

ABDULKARIM OLOYEDE: Hola. Yo soy Abdulkarim. Quisiera saber, por ejemplo, si ustedes tienen estos certificados web que reciben, si por ejemplo nos conectamos a su sitio web y nos dicen: “Ah, este sitio web no es seguro por algún motivo”. ¿Cuál es la relación entre ese mensaje que recibimos y DNSSEC?

WES HARDAKER: Excelente pregunta. ¿Alguien la quiere responder? Bueno, la respuesta rápida sería, y es una buena pregunta, que en general no están relacionadas estas cosas. Cuando vamos a un sitio web que nos dice: "Están tratando de ir a un sitio seguro y no confiamos en el certificado", en realidad es el navegador de ustedes que está verificando el certificado del sitio web. Es decir, ustedes ya tienen la dirección, ya hicieron el DNS y el navegador trató de ir a ese sitio web pero no confía en el sitio. Eso es diferente. El DNSSEC interviene antes, cuando empezamos a buscar www.bigbank.com y mandamos la consulta. ¿Qué pasa? El ejemplo que no mostramos en nuestro sketch es el siguiente. Si el ISP no recibe una respuesta válida, vuelve al usuario y le dice: "Lo siento. No encontré nada". No acepta las respuestas. Ahí el mensaje: "No se encontró el sitio" o "No se encontró el host".

Si escriben una dirección incorrecta les va a decir que no se encontró ese sitio web. Hay algunos ejemplos más complejos de lo que falta. Hay que ver si el navegador entiende el DNSSEC, etc. y otros aspectos.

ABDULKARIM OLOYEDE: Tenemos dos tipos de certificación.

WES HARDAKER: Sí. Son dos formas de hacer certificación. Es mejor contar con ambas. Viktor.

VIKTOR DUKHOVNI: Donde se superponen es aquí. La autoridad de certificación que emitió el certificado, muchas veces utilizó un método no seguro para verificar que un sitio sea quien dice ser. Aparentemente, si solo utilizan DNS y alguien parece que ha cambiado un registro, habría que publicar y verificar que los datos sean los correctos pero puede haber un intermediario. Si el tráfico se reenruta, si hay un ataque de secuestro, etc. el atacante puede estar obteniendo certificados para diferentes sitios a través de los cuales el tráfico no suele pasar. La superposición es que la validación del certificado de autenticidad de los dueños de los dominios es muy poco segura. En general, no se ataca, por eso tenemos bastante seguridad, porque en general esos ataques son poco frecuentes pero son posibles.

WES HARDAKER: Si el DNSSEC estuviera totalmente implementado, esto resolvería el problema.

VIKTOR DUKHOVNI: Siempre y cuando la validación se haga correctamente.

LAUREEN BURKHART: Soy Laureen, de los Estados Unidos. Tengo una pregunta muy básica. No tenía ningún conocimiento técnico hasta ayer. Ustedes dijeron que se puede verificar el casillero en el formulario de registrador, el que maneje nuestro DNSSEC. ¿En qué medida se hace esto y por qué quizá uno no elegiría que sí se haga? Una vez que esté totalmente implementado, ¿qué podemos hacer?

WES HARDAKER: Es una pregunta excelente. Una de las personas que sabe más sobre este tema está sentada allí. Voy a decir algo antes de darle la palabra a Viktor, que monitorea la mitad de las cosas. Hay un programa llamado SECSpider y pueden buscarlo. "SECSpider". Es una base de datos donde se están tratando de identificar todos los dominios que han sido firmados. El porcentaje no es tal alto como quisiéramos. En el caso de .COM es .5%. Si van al taller del DNSSEC van a escuchar estas cifras. Pero .5% de .COM son muchos sitios, pero no son todos. Hay razones técnicas por las cuales algunas de las empresas importantes no han aceptado esto todavía. Viktor.

VIKTOR DUKHOVNI: Yo tengo estadísticas. En este momento estoy haciendo un seguimiento de 5.2 millones de dominios. La mayoría están en el norte de Europa, especialmente en Holanda, Suecia, Alemania, Noruega, algunos en los Estados Unidos, República Checa. En el resto del mundo no hay tantos. La distribución DNSSEC es muy desigual. .COM tiene dos tercios, 813.000 dominios firmados. Suecia, más de la mitad de los dominios están firmados. Holanda, más de la mitad también. Todos los dominios de .BANK están firmados, pero son pocos y la mayoría están dejados de lado. Se los registra y son utilizados. Lo mismo pasa con .INSURANCE. Hay muchos dominios de seguros. Todos están firmados y ninguno se está utilizando.

En general, el número varía entre dos tercios y un 1%. En algunos lugares el uso es muy alto. En los Países Bajos, DNSSEC es más económico. El registrador nos da un descuento si utilizan un dominio con DNSSEC.

WES HARDAKER: Los nuevos gTLD que soportan DNSSEC, más del 50% de los códigos de países están firmados. .COM, .ORG, .NET, .EDU, .BIZ, .INFO, todos están firmados. Hay un gran número de muchos nombres de nivel superior que están firmados. Están promoviendo que sean más.

LAUREEN BURKHART: ¿Hay una explicación sencilla por la cual no se querría firmar? ¿Es una cuestión de tiempo y trabajo?

RUSS MUNDY: Ambas cosas. Como decía Wes antes, hay algunas organizaciones que han aprovechado diversas cosas que se pueden hacer con el DNS que les sirven desde su perspectiva comercial y las cosas que están haciendo van a dejar de funcionar si siguen las reglas del DNS. Cuando empiecen a aplicar DNSSEC, se va a identificar que hay algo que no funciona bien. Hay casos así.

Además, uno de los mayores problemas que tenemos es el de la educación, que es uno de los motivos por los cuales hacemos estas sesiones, porque queremos que la gente se familiarice con los fundamentos de lo que involucra la seguridad del DNS para que haya más gente en el mundo que tenga un entendimiento general y que vaya de vuelta a sus organizaciones y empleos y empiece a hacer preguntas. ¿Por qué nosotros no hacemos seguridad del DNS? ¿Qué puedo hacer yo para progresar en esto? Esa es una función muy importante que tiene esta sesión en particular. Gracias por preguntar.

JACQUES LATOUR: Soy Jacques Latour. Soy de .CA. En este momento tenemos 2.7 millones dominios en Canadá y tenemos mil firmados con DNSSEC. Muy bajo porcentaje. Muy cerca de cero. Cero punto algo. Nuestro desafío actual. Algunos soportan DNSSEC. Los registratarios necesitan pagar más dinero a estos registradores que tienen DNSSEC. Tienen que pagar más para tener más seguridad. Hay gente que simplemente compra lo más barato. Entonces no tiene DNSSEC.

WES HARDAKER: ¿Andrew?

ABDALMONEM GALILA: Soy Abdalmonem, de Egipto. Yo no confío en mi ISP. No voy a poner validador en mi máquina. Creo que es mejor alejarse de los ataques de intermediario entre mi máquina y el ISP. ¿Por qué la ICANN o ustedes no pueden asesorar que tengamos un validador local en cada máquina?

VIKTOR DUKHOVNI: Si la máquina es móvil, si la lleva a aeropuertos, como las laptops, lamentablemente estos entornos son hostiles al DNSSEC por las infraestructuras que tienen. Capturan portales. Simplemente uno acepta los términos y listo. No importa qué dominios se tipea. Aparece google.com y uno termina en el

portal del hotel. Toda esta tecnología, por un motivo u otro, para poder cumplir con las políticas hay que modificar las respuestas del DNSSEC. Hoy día las laptops normalmente no pueden cumplir. En un centro de cómputos, obviamente se despliega en la máquina local. Me sorprende que los sistemas operativos no lo hagan por default pero cada vez más lo harán.

WES HARDAKER: Russ.

RUSS MUNDY: Sí. Como decía Viktor hay distintas formas de manejar problemas de tal naturaleza. Hay un software que se llama DNSSEC-Trigger, de NLnetLabs, que está diseñado específicamente para situaciones así y tienen una serie de mecanismos incorporados que identifican los distintos caminos de conectividad para hacer DNSSEC.

Si mal no recuerdo, para entornos como el que describía Viktor, la primera consulta o la primera conexión tiene que ser configurada con el hotel porque bloquea la ruta si no se contacta uno con ellos, pero después tienen DNSSEC. Se puede correr después. Yo personalmente lo hago distinto. Una vez que tengo el okey del hotel, del servidor que bloquea y manda al hotel, yo

entro en mi servidor, al servidor de mi ISP que tiene DNSSEC. Hay distintos mecanismos pero no siempre es fácil de sortear.

WES HARDAKER: Está mejorando. Herramientas como DNSSEC-Trigger y DHCP también para hacer el login en el sistema operativo actual aparece una ventana emergente que requiere la conexión. Hay distintas cosas que se pueden configurar en la red. Se puede configurar DNSSEC localmente. Si ustedes son expertos les recomiendo que practiquen. Yo lo hago pero estamos trabajando. Algunos proveedores de software Linux lo tienen por default activado en sus configuraciones de software pero solo hay un par. Está avanzando pero lentamente. ¿Alguna otra pregunta, Andrew? Ahí atrás.

FRANSLEIDY DE JESÚS: Soy Fransleidy de Jesús. Soy NextGen. ¿Puedo hacer la pregunta en español?

WES HARDAKER: ¿Alguien tiene un receptor de traducción o alguien sabe algo de español? Mi español es muy malo. Adelante.

FRANSLEIDY DE JESÚS: Uno de los problemas que tiene DNS con la clave cuando está encriptada… Cuando viene la información del DNS, él no sabe si la información está adulterada. Por eso cambiaron la zona raíz a KSK. Ese es uno de los cambios principales en febrero. Cuando ustedes hagan el cambio, ¿qué están haciendo ustedes para que ese problema no suceda?

WES HARDAKER: Si quiere aguardar un segundo para que se haga la traducción.

JACQUES LATOUR: Estamos cambiando la clave porque la que tenemos hoy día podría comprometerse. Eso no es lo que pasó. ¿Es esa su pregunta?

FRANSLEIDY DE JESÚS: En febrero, cuando lo hicieron en Los Ángeles para cambiar la clave del DNS, la KSK, la información, no se sabía que la información era incorrecta o se tenía más información. Se cambió la zona raíz. No lo sé explicar.

JACQUES LATOUR: En febrero…

WES HARDAKER: Ella habla de la generación de la nueva raíz.

ORADOR DESCONOCIDO: Yo podría traducirlo. Son dos cosas. Hubo un evento en febrero, quizá podemos hablar de eso, cómo se relaciona con el traspaso de la llave. La pregunta es qué se hace en relación con el traspaso de la llave para garantizar su éxito. De qué trató el evento en febrero, qué fue lo que se postergó para el resto del año. Esas dos cosas.

RUSS MUNDY: Hay un proceso bien documentado y muy extenso que describe cómo se generan los cambios de la llave, cómo se generó la primera, cómo se generó la nueva. Son personas independientes, separadas, que han sido identificadas previamente como personas de apoyo de la comunidad que actúan como testigos de que todas estas cosas se hagan de manera apropiada en un área extremadamente segura.

El almacenamiento de la llave, una vez generada, se almacena en un dispositivo de hardware, se mantiene en un dispositivo de hardware que está literalmente cerrado con llave cuando no se usa. Así es como se generó la nueva KSK y así es como la nueva KSK se generará.

La parte pública de la KSK está invisible y no está disponible para nadie. La parte privada está extremadamente protegida y asegurada. Cuando se hace la ceremonia de cambio de llave, esta es filmada y se pone a disposición para que cualquiera pueda verla en cualquier momento. Está disponible en el sitio web de la ICANN.

La norma ISO 9000 se usó para diseñar esta instalación y que es auditada creo que dos o tres veces por auditores independientes. Son muchísimas las cosas que se hacen para garantizar que la clave, la clave privada, esté sumamente protegida y resguardada. La razón del cambio, no tiene nada que ver con ningún tipo de compromiso. Se cambia porque los procedimientos asociados a la raíz estipulan que hay que cambiarla con cierta frecuencia. Esa es la razón del cambio. No porque haya existido ningún tipo de compromiso. ¿No sé si es eso lo que usted estaba preguntando?

WES HARDAKER: Quisiera agregar algo. Desde el punto de vista operativo, es una buena idea cambiar las llaves, aun cuando no haya ningún problema. Es una prueba. Garantiza que todo el mundo vaya a buscar la nueva llave. Es bueno hacerlo si no hay problemas porque si hay problemas y uno se apresura, las chances de hacerlo mal aumentan.

Su otra pregunta es sobre los tiempos. La generación de la nueva llave se hizo en febrero del año pasado. El traspaso a la nueva llave se suponía que iba a ser en octubre. Nosotros estábamos midiendo la cantidad de gente que usaba la llave antigua. Fue poca la gente que empezó a pasar a la nueva llave y a validarla, por eso la ICANN retrasó, postergó a la espera de lo que se llama el aporte, la contribución de la comunidad hasta el próximo octubre. Hay tiempo para que la gente entienda más el tema, para que formule sus opiniones. Este es el momento entonces de leer ese documento y hacer comentarios públicos porque habrá un periodo abierto hasta octubre. Creo que es 3 de octubre. ¿Alguna otra pregunta? Me parece que tenemos tiempo para una pregunta más nada más.

ABDELMONEM GALILA: ¿Con qué frecuencia tendrá lugar el cambio de la llave?

WES HARDAKER: ¿Cuánto tiempo va a llevar? Bueno, originalmente, hasta que se postergó, se iba a hacer en cinco meses. Iba a durar cinco meses.

ORADOR DESCONOCIDO: La pregunta es con qué frecuencia se cambia.

WES HARDAKER: La frecuencia. Bueno, esto es tema de debate. Creo que la política actual publicada dice cada cinco años, la política de la ICANN. Si la frecuencia disminuye, me imagino que una vez que cambiemos esta, esa política será revisada y actualizada. La verdad, no sé si la van a continuar o la cambiarán. La política dice cinco años pero anticipo que será revisado este periodo después del cambio. ¿En relación con lo mismo? Rápidamente.

ABDELMONEM GALILA: ¿ICANN tiene autoridad para restringir a los ISP, para hacer validación de DNSSEC para dar cabida, para permitir el cambio de la llave y que luego se haga automáticamente el cambio de la clave?

WES HARDAKER: ICANN no tiene ningún tipo de autoridad en ningún lugar del mundo sobre ninguna ISP. Los gobiernos la tienen pero no existe ningún gobierno que haya intentado ejercer tal mandato. Buena pregunta. Nunca se me había ocurrido. Gracias a todos. Este es el final de nuestra sesión. Fantásticas preguntas. Espero que hayan aprendido algo. Gracias.

[FIN DE LA TRANSCRIPCIÓN]