COPENHAGUE - DNSSEC para todos: Guía para principiantes
Domingo, 12 de marzo de 2017 - 17:00 a 18:30 CET
ICANN58 | Copenhague, Dinamarca

WES HARDAKER: ¿Por qué tenemos DNSSEC? Vamos a ver cómo proteger la infraestructura y los datos del dominio. Vamos a entrar en los detalles. Antes, una historia. Hay quienes dicen que el DNSSEC tiene su origen en 5.000 años antes de Cristo. A mí me resulta un poco difícil de creer pero vamos a aceptarlo. Tenemos un par de personajes en este elenco. La primera que tenemos es Ugwina, que vive en una cueva en el borde del Gran Cañón. Él es OG. Él también vive en una cueva pero él vive en el otro lado del Gran Cañón. Completamente a través del acantilado, así que no se pueden comunicar. La distancia es larga. Hay que dar un desvío y Ugwina no puede comunicarse con él con mucha frecuencia.

En una de sus visitas observaron que salía humo del fuego de Og y se dieron cuenta de que podían usar el humo para conversar. El humo, a partir de ahora, será como el DNS. Un cliente distante que hace preguntas y podemos responder con señales de humo. Un día, el cavernícola Kaminsky (Kaminsky era una persona que encontró una brecha en el DNS y cometió un acto malicioso) comenzó a enviar señales de humo distintas. Ahora Ugwina está

confundida. Ve estos dos grupos de señales de humo y no sabe en cuáles creer. Una dice: “Me gustas, Ugwina”. La otra dice: “No me gustas, Ugwina”. No sabe si ponerse contenta o triste.

Ugwina baja al cañón. Trata de resolver esta situación y entender qué pasa. Ugwina y Og van a consultar a los sabios de la aldea y el cavernícola Diffie, hace referencia al criptógrafo Diffie-Hellman, piensa en una idea y rápidamente entra a la cueva de Og, donde encuentra una pila de polvo mágico azul que solo existe en la cueva de Og. En ningún otro lado y lo arroja en el fuego y de repente las señalas se tornan de color azul. Esto es de ayuda porque ahora, cuando Ugwina y Og se comuniquen en la distancia, ella solo cree en las señalas de humo azul. Sabe así cuáles son de Og y cuáles son del malvado Kaminsky.

Esta fue entonces la introducción del DNSSEC de la era de 5.000 años antes de Cristo. Vamos a ver ahora cómo es el tráfico moderno en el DNS. Si ustedes no están familiarizados con el DNS, un concepto de nivel muy general es el de un árbol invertido. Los resolutores del DNS que responden las consultas empiezan arriba, en la raíz. La raíz sabe qué hay debajo de ella, como .COM, .UK y cosas parecidas. Cada uno de estos bloques tiene subniveles. Bigbank.com está debajo de .COM. Es una estructura parecida a la de un árbol. Como decía entonces, el resolutor sabe dónde está la zona raíz y recorre la jerarquía para encontrar la respuesta cuando uno va al navegador y tipea un

nombre de dominio. Cada nivel apunta simplemente al siguiente nivel hasta conseguir la respuesta a la pregunta.

Un beneficio es que el resolutor hace la caché de toda esta información para que sea más rápido, para que la próxima vez que bigbank.com haga una pregunta, no tenga que empezarse todo el proceso otra vez. El problema en el pasado es que en este concepto de nivel general no había DNSSEC porque ahora DNSSEC resuelve todos estos problemas. No hay seguridad. Es el humo azul versus el humo blanco. Si no tenemos el humo azul, no podemos saber cuál es la respuesta correcta. Los nombres son fácilmente robados o las cachés son contaminadas. Cuando se pone una respuesta incorrecta en la caché, el resolutor da la respuesta incorrecta porque es la que está en la caché.

Para poder ilustrar este punto vamos a hacer un sketch. Les voy a pedir a mis actores que se acerquen, que se presenten. Vamos a armar una fila aquí adelante. Lamentablemente, porque hay personal enfermo y ausente yo voy a tener que asumir uno de los roles. Les pido disculpas de antemano si cometo algún error. Yo voy a ser el usuario Joe. Soy el usuario de Internet que quiere hacer una transacción bancaria.

No creerían la cantidad de veces que nos pusimos estas mismas camisas. Yo soy el usuario Joe. Voy a hacer la introducción. Este es el señor ISP. Es el que cuando uno va a una página web, es el

primer contacto del usuario. Bigbank.com conoce la información del banco. COM sabe dónde está el banco. Ustedes tienen que cambiarse. La raíz es donde está la fuente de todas las cosas. La raíz sabe donde está COM y el resto de los TLD. Así vamos a comenzar. Yo voy a ir a la computadora y tengo que hacer una transacción bancaria. Voy a chequear mis cuentas. Entro en la máquina. Tengo que ir bigbank.com y espero a que el DNS termine antes de siquiera empezar.

WARREN KUMARI/ISP: ¿Usted quiere ir a Bigbank?

WES HARDAKER/USUARIO JOE: Sí.

WARREN KUMARI/ISP: Hola, raíz. Mi usuario quiere ir a www.bigbank.com. ¿Dónde está?

KATHY SCHNITT/RAÍZ: Hola, ISP. No sé dónde está www.bigbank.com pero sé dónde está .COM, que está en 1.1.1.1.

WARREN KUMARI/ISP: Gracias. Hola, .COM. Soy un ISP. Uno de mis usuarios quiere ir a www.bigbank.com. ¿Dónde está?

JACQUES LATOUR/.COM: Lo lamento. No sé dónde está pero sé dónde está Bigbank. Está en 2.2.2.2.

WARREN KUMARI/ISP: Gracias. Hola, Bigbank. Un usuario quiere visitarle. ¿Dónde está www.bigbank.com?

ERWIN LANSING/BIGBANK: Un segundo. Tengo que buscarlo. Está en 2.2.2.3.

WARREN KUMARI/ISP: Gracias.

WES HARDAKER/USUARIO JOE: Perfecto. Ahora el navegador me permite conocer el saldo que hay en mi cuenta y que es de un millón de dólares. Voy a pensar ahora cómo gasto este dinero. Así es como funciona el DNS cuando no hay problemas. Como recordarán, Ugwina, la resolutora, está chateando con Og el servidor. Tenemos a Ugwina aquí, Warren. El servidor está por allá. Al principio estaba confundida y encontró esta cuestión del polvo mágico. Vamos a

ver qué pasa cuando sucede un problema y cómo el DNSSEC lo resuelve. Imaginen que hay dos Bigbank que quieren dar la respuesta. Una respuesta es correcta y una respuesta es incorrecta. El problema del DNS es que uno cree la respuesta que se recibe primero. El DNSSEC lo resuelve con esas firmas criptográficas, ese humo azul que garantiza que toda la información es correcta y que vienen del lugar correcto. Son las firmas las que se utilizan para asegurar que todo lo que está almacenado está perfecto y no ha sido modificado desde que quien lo publicó, lo generó.

No importa donde esté almacenado. Está en la caché, en el servidor autorizado o en cualquier otro lugar. El DNSSEC tiene un sistema de búsqueda para buscar las claves como cualquier otra cosa. Las claves criptográficas están almacenadas también en el DNS. El resolutor solo necesita saber la clave de un servidor, la raíz. Kathy, levanta la mano. Si conocen esa clave, conocen la clave de todo lo demás en el sistema. No tienen que recordar más que una clave pública y todo lo demás funciona. Se genera una cadena de confianza. De cada nivel que se firma hasta el siguiente nivel, hasta conseguir la respuesta correcta. Aquí lo que vemos, fíjense en la tilde, son tildes que indican que son los lugares correctos. El rojo es el que está mintiendo.

Volvamos a nuestra pequeña dramatización. Voy a tratar de hacer otra transacción bancaria. He decidido que con mi millón de dólares voy a gastar mil dólares en una nueva computadora.

WARREN KUMARI/ISP: Si usted tiene un millón de dólares, le vamos a cobrar acceso de usuario frecuente. Hola, raíz. Uno de mis usuarios quiere ir a www.bigbank.com. ¿Dónde está?

KATHY SCHNITT/RAÍZ: Hola, ISP. Ya somos amigos. La verdad, no sé dónde está www.bigbank.com. Lo lamento pero sé dónde está .COM. Está en 1.1.1.1.

WARREN KUMARI/ISP: Hola, .COM. Un usuario quiere ir a Bigbank. ¿Dónde está www.bigbank.com?

JACQUES LATOUR/.COM: Me parece que tengo un problema de memoria. No sé dónde está bigbank.com pero sé dónde está Bigbank. Está en 2.2.2.2.

WARREN KUMARI/ISP: Voy a preguntar dónde está bigbank.com. Hola, Bigbank. ¿Puedes decirme dónde está www.bigbank.com?

"DR. MALDAD": Oh, sí. Yo sí puedo. Usted puede encontrar www.bigbank.com en 6.6.6.6.

WARREN KUMARI/ISP: Gracias por esa rápida respuesta. De hecho, usted tiene un aspecto mucho más interesante que los demás servidores. 6.6.6.6.

WES HARDAKER/USUARIO JOE: Muchas gracias. ¡Desapareció mi dinero!

¿Entienden el problema? Uno cree a la primera respuesta. Ahora vamos a hacer el mismo caso pero con el DNSSEC. Le voy a preguntar ahora a mi ISP dónde está www.bigbank.com. Señor ISP. Esto lo ensañamos, en serio.

Perdón, señor ISP. ¿Dónde está www.bigbank.com?

WARREN KUMARI/ISP: Se lo averiguaré. Hola, .COM. ¿Me recuerda? Uno de mis usuarios quiere ir a www.bigbank.com. No recuerdo bien las cosas. ¿Me puede decir dónde está?

KATHY SCHNITT/RAÍZ: Su usuario hace demasiadas transacciones. Yo no sé dónde está bigbank.com pero sé dónde está .COM, que está en 1.1.1.1. Me parece que antes de ir ahí, yo debería firmar esto.

WARREN KUMARI/ISP: Un segundo. Sí, se parece a su firma. Hola, .COM. Un usuario quiere ir a www.bigbank.com. ¿Me puede decir dónde está?

JACQUES LATOUR/.COM: Perdón. No sé dónde está www.bigbank.com pero sí sé dónde está bigbank.com. Está aquí. En 2.2.2.2.

WARREN KUMARI/ISP: ¿Puede por favor firmármelo para creerle? Muy bien.

JACQUES LATOUR/.COM: Ahí lo tiene. Firmado.

WARREN KUMARI/ISP: Se parece a su firma. Voy a ir a 2.2.2.2. Hola, 2.2.2.2. ¿Me puede decir dónde está www.bigbank.com?

“DR. MALDAD”: Sí, puedo. Puede encontrar a www.bigbank.com en 6.6.6.6.

WARREN KUMARI/ISP: Fantástico. Un segundo. Esta firma no se parece a la real. No creo en esta firma. Hola, Bigbank. ¿Puede decirme dónde está www.bigbank.com?

ERWIN LANSING/BIGBANK: Me encantaría ver a mis usuarios así que le digo que está en 2.2.2.3. Y esta es mi firma.

WARREN KUMARI/ISP: Esa firma coincide con la mía. Aquí tiene, usuario. 2.2.2.3. Yo lo he verificado y puede confiar en ella.

WES HARDAKER/USUARIO JOE: Aquí sí sigo teniendo el dinero en mi cuenta. Así funciona. Vamos a darles un aplauso a nuestros actores. Ahora vamos a sacarnos todos la remera, que es parte del entretenimiento. Espero que con esto hayan tenido una idea general. Si hay un mensaje que sacar de aquí, los detalles vendrán en el resto de la tarde pero la idea era explicar fundamentalmente cómo funciona. Los dominios pueden asegurar las respuestas para que el Doctor Maldad no pueda interferir. Este es un ejemplo de por qué el DNSSEC es necesario y una guía sencilla para iniciarse. ¿Por qué nos tenemos que preocupar por el DNS? Porque los usuarios piensan en términos de nombres. Nadie recuerda las direcciones de IP y las tipea. Siempre usamos nombres, desde el

mismo comienzo de la Internet. Las solicitudes primariamente también usan nombres. Cuando uno busca algo en el navegador, no busca información de un nombre sino imágenes, códigos Java y distintas cosas incluidas en las páginas web. Después lo vamos a ver. La Internet, de hecho, usa direcciones. A partir de ahí se usan direcciones IP y direcciones IPv4 o IPv6.

El DNSSEC es el pegamento que traduce las direcciones en lo que el software necesita para cumplir su función. Que el DNS funcione es absolutamente necesario. Es un componente crítico del funcionamiento de la Internet. El problema es que puede ser secuestrado como vimos en la dramatización. Los ataques constituyen una manera de desviar las solicitudes de los usuarios. Los usuarios pueden ser mandados a otra página web. Pueden ser redirigidos a una dirección IP distinta, que se ve igual cuando se hace el inicio de sesión con las credenciales pero el nombre de usuario y la contraseña son robados. Ese es un ataque de intermediación. Hace tiempo que existen estos tipos de ataques. Algunas universidades incluso las usan en sus clases. Les piden a los estudiantes que demuestren cómo secuestrar la infraestructura de un tercero.

El DNSSEC es la respuesta. Es el equivalente a esas tarjetas adhesivas en las tarjetas que demuestra que se está en el lugar correcto. Se demuestra que criptográficamente, sin lugar a dudas, se están recibiendo los datos del sistema que fueron

generados por el dueño. El mantenedor de la zona original creó los datos y los firmó. No importa cómo se hayan distribuido los datos, podrían haber sido distribuidos en un avioncito de papel pero tiene la firma validada. El ejemplo del secuestro que acabamos de ver muestra cuando hay un problema. Hay otros ejemplos. Este es un diagrama pictórico de algo similar. Este es un intercambio normal del DNS. No voy a entrar en detalles pero es algo similar.

¿Tenemos un puntero? Aquí está. Tenemos un servidor de nombres autorizado, tenemos un servidor web, servidor de nombres recursivos que usan los ISP para hacer las preguntas y al usuario Joe aquí abajo. Más o menos el mismo diagrama de la dramatización. Es en realidad un poco más complejo porque puede haber servidores recursivos varios. Varios servidores web y varios servidores autorizados pero es más o menos lo mismo. ¿Qué hice? No pulsen el botón incorrecto. Una lección para la vida. De hecho, yo pulsé dos a la vez.

El usuario presenta una consulta que va al ISP, como vimos en el sketch. El resolutor recursivo la envía al servidor autorizado para recibir la respuesta. El servidor de nombres autorizado envía la respuesta al resolutor recursivo y ese resolutor recursivo se la devuelve al usuario. Bastante directo. Se hace una pregunta, se responde. De hecho, como vieron en la dramatización, se está

hablando con muchas partes. Al final, el usuario ha ido al lugar correcto que es el servidor web donde quería ir.

Con el navegador Firefox, lo modificamos para hacer validación DNSSEC de páginas web. Esta diapositiva es un ejemplo. Fíjense en esa marca verde. Si van a dnssec-deployment.org y utilizan un navegador validado o un ISP validado… Por cierto, que el resolutor público de Google hace validación. Van a ver esta tilde verde. Si tienen un entorno de validación que no cumple con DNSSEC, van a ver esta señal de advertencia, que el DNSSEC está desactivado. Está en OFF.

Volviendo al ejemplo del secuestro, que muestra cómo el DNSSEC está en off, tenemos acá al Dr. Maldad, que ahora está sentado allí abajo. Una vez más, el usuario envía una consulta al servidor recursivo pero el Dr. Maldad está al lado y puede responder rápidamente, mucho más rápidamente que el ISP, que tiene que ir a hacer todas esas otras preguntas. “No importa qué vas a preguntar. Voy a enviar la misma dirección errónea a todos. Quiero que todo venga a mí”. Lo que ocurre es que el usuario es redirigido a un sitio web alternativo que puede controlar el hacker.

Esta es una ilustración del hecho de que el resto sigue pasando pero la información llega tan tarde que los usuarios no ven la respuesta correcta. DNSSEC funcionalmente es igual a detener

esto, impedir esta parte, impedir que cualquier otro pueda secuestra la información y garantiza que siempre lleguemos al lugar correcto, que el usuario siempre obtenga la respuesta correcta. Estas no son mis diapositivas. Me olvido de en qué parte está la animación. Hay dos personas más que normalmente hacen esta presentación. Yo tuve que remplazarlos porque soy el remplazo. Por suerte, también conozco bien esta información.

Volviendo a este ejemplo, esa marca de verificación verde ocurrió porque tuvo lugar la validación y no aparece el cartel o el logo de DNSSEC. No está funcionando. Una de las cosas que la gente no tiene en cuenta es que si vamos a cnn.com, ¿saben cuántas búsquedas de DNS tienen lugar para ir hasta un sitio web? Muchas más de las que podrían imaginarse. De hecho, hace 5 o 10 años trabajé con Russ Mundy y le pedí que utilizara su laptop como servidor de DNS y puede llegar a todos estos puntos. Cada una de esas rayas verdes y azules son una consulta diferente para ir a una única página web. Pueden ver que hay muchísimo tráfico de DNS, que uno no tiene ni idea que ocurre detrás de escena.

Este es otro ejemplo ilustrado de lo mismo, descrito de una forma diferente. Es lindo todas esas líneas pero no se imaginan lo que es entender eso. Incluso los expertos ni tratan de entender la ubicación de cada imagen, de cada código, de todo lo que

ocurre. Esto incluye los vínculos de Like de Facebook, de Twitter. Todo termina con una solicitud de DNS diferente. Hay algunas funciones básicas de DNS, algunos roles básicos que existen en el mundo de la gente que trabaja con datos de DNS. No se trata de una sola persona la que arma todo esto. En última instancia lo que cuentan son los datos. Por eso se creó DNSSEC, para proteger los datos independientemente de quién más esté involucrado. Siempre y cuando se autoricen los datos, no importa por dónde pasan.

Este es un ejemplo de lo complejo que es incluso el mecanismo de publicación de datos. Acá a la izquierda tenemos lo siguiente. Necesito agregar este registro a mi zona. Lo pongo en los datos de mi zona. Se publican. Pasan al servidor autorizado que es el lugar donde el servidor recursivo hace consultas sobre la base de los datos previamente publicados y el cliente, por supuesto, le hace preguntas al servidor recursivo. En un segundo vamos a volver a ver este diagrama con la parte de DNSSEC agregada.

La implementación de DNSSEC depende básicamente de las mismas funciones pero tiene información adicional. DNSSEC consta de varias partes: servidor de nombres, usuarios de aplicación, los que publican la zona, el aspecto de aproximamiento. Tenemos actividades con funciones grandes y complejas de DNS. Estas actividades tienen actividades de implementación más complejas. Si es una configuración simple,

es fácil empezar a utilizar DNS. Si son más complejos, será más complejo. Por ejemplo, un registro responsable de la operación de un gran TLD como .COM debido a que tienen que autorizar cosas continuamente, para ellos es más complejo que para la persona promedio, que solamente autoriza cada tanto. .COM agrega dominios continuamente. Todo el tiempo.

Una empresa importante, con muchos componentes que van cambiando con el tiempo o que cambian periódicamente como HP.com, ellos probablemente tengan que pensar mucho más en la implementación de DNSSEC. Las empresas basadas en Internet con una serie de zonas de negocios críticos y un mensaje importante es que si ustedes van a hacer esto en una zona de negocios crítica, dediquen tiempo y energía a tener un sistema de monitoreo para saber cuándo están saliendo mal las cosas. Lamentablemente, no solemos hacer eso con el DNS hoy en día. Si alguien secuestra su zona, ustedes probablemente no se enteren porque no son muchas personas las que se dedican a monitorear esto también. Hay empresas que ofrecen productos que pueden ayudarlos a monitorear esto en caso de que quieran comprar una solución tercerizada.

Luego tenemos actividades en zonas de DNS que no son críticas: net-snmp.org es un ejemplo. No hay tantas personas que van. Es un proyecto de código abierto. No es un banco. Es algo que todavía es bastante importante. Es un proyecto de software muy

importante. Después, por supuesto, la página de imágenes que uno comparte con la familia. Hay distintos de producción, distintos niveles de DNSSEC y distintos tipos de infraestructura de DNSSEC que puede ayudarlos.

¿Dónde encaja DNSSEC en todo esto? Es necesario para evitar que se use de manera indebida el contenido. El mensaje importante es que es bueno siempre y cuando protejan los datos de su zona. Si ustedes no alojan sus datos en una máquina decente, entonces DNSSEC no los va a ayudar mucho porque los atacantes van a ir detrás de la base de datos que se puede atacar fácilmente. Tienen que asegurarse de proteger los datos de la zona y también protegerse con DNSSEC. Esto no resuelve otros problemas de secuestro de servidores. Solamente protege los datos.

Volviendo a este diagrama, ahí tenemos partes adicionales importantes que hemos agregado con DNSSEC. Tenemos ahora una parte de firma o autorización después de agregar datos. En lugar de enviarlos directamente al servidor autorizado, primero los vamos a autorizar y vamos a publicar la copia firmada. Luego tenemos aquí este candado que representa la clave criptográfica entre los datos firmados y el servidor recursivo que hace la validación para saber que está validado. Tal como dijimos en nuestra dramatización, este es el símbolo que necesita el

servidor recursivo. El resto pueden hacerlo preguntándole a .COM en el ejemplo que vimos antes de .COM, por ejemplo.

Como principio general, si tienen una red realmente activa, una zona realmente activa tienen que dedicar más energía a mantenerla y también a protegerla con DNSSEC. DNSSEC escala igual que DNS. Si hacen algo chico y trivial no necesitan mucho del lado de DNSSEC. Si están haciendo algo muy complejo y muy grande, entonces van a necesitar un poco más de DNSSEC.

Habiendo dicho esto, vamos a hacer una breve pausa para ver si hay alguna pregunta. Es la última, ¿no? Sí. Matt Larson, ¿está aquí en el público? Le voy a dar cinco minutos a Matt antes de pasar a la parte de preguntas y respuestas. Matt Larson, de la ICANN, va a hablar acerca de qué va a pasar en un futuro cercano con la llave de la raíz. Los ISP tienen que saber lo que pasa con esto. Matt les va a hacer una breve revisión sobre ese tema.

MATT LARSON: Soy Matt Larson. Soy vicepresidente de investigación en la oficina del director de tecnología de la ICANN. Soy una de las personas involucradas en el proyecto para el traspaso de la clave de la llave de la zona raíz. Esta es la clave que creamos cuando firmamos la llave por primera vez. No ha cambiado en todo este tiempo. El objetivo no era que permaneciera igual. En la documentación que preparamos dijimos que la clave se iba a

traspasar después de cinco años. No dijimos exactamente a los cinco años. Dijimos después de cinco años. Ese es el punto en el que estamos en ese momento.

Voy a hablar brevemente acerca del punto en el que estamos en este proyecto. Estamos en el medio del proyecto en este momento. Este proyecto va a llevar bastante tiempo y esto es a propósito. Queremos hacer el cambio lentamente y de manera deliberada. No hay apuro. No tenemos ninguna razón para creer que hay ningún problema con la KSK actual. Por lo tanto, no hay nada malo en iniciar este proyecto y trabajar de forma conservadora. Estos son los hitos recientes. La nueva KSK se creó en octubre del año pasado. La ICANN utiliza dos lugares diferentes en los que guarda la KSK. Son dos lugares que están conservados dentro de un hardware criptográfico. Es decir, se guardan en un lugar y luego se lleva al otro lugar. Se crea en la costa este y se lleva a la costa oeste.

Hay una razón para utilizar la KSK. Una vez por trimestre sacamos la KSK y firma la ZSK. Por lo tanto, lo que decidimos hacer es incorporar todos los eventos relacionados con KSK en esta cadencia trimestral. En el primer trimestre de este año pasamos la clave a la otra instalación en la costa oeste y una vez que pasó por los dos lugares dijimos que ya estaba listo, desde el punto de vista operativo. El próximo hito que tuvo lugar hace poco tiempo fue en la ceremonia de la clave del segundo

trimestre. Fue cuando se publicó esto y se utiliza por primera vez. Ahora la clave está disponible y es visible. Va a aparecer en el DNS en julio, el 11 de julio. Ahí está la fecha. El lanzamiento tendrá lugar el 11 de octubre de 2017. Está en negrita en la diapositiva y lo voy a repetir: 11 de octubre de 2017. Esa es la fecha que tienen que tener en cuenta porque es la fecha en la que vamos a dejar de utilizar la KSK actual y vamos a comenzar a utilizar la nueva.

Vamos a llamarlas KSK 2010 y 2017 respectivamente. En ese momento, si ustedes operan algún software que hace validación de DNSSEC que tiene configurada la zona raíz con KSK van a tener que haberla modificado antes de esa fecha. Por eso esa fecha es tan importante. Antes del 11 de octubre de 2017, todo software que haga validación de DNS que tenga configurada la KSK tendrá que tener configurada la nueva KSK. Tenemos mucha información en este URL. Esta es una página web que cambia continuamente. Continuamente agregamos información actualizada sobre el traspaso de la clave. Pueden buscarlo en la sección de vínculos. Sé que hice una presentación muy breve porque no esperaba que me fueran a dar estos cinco minutos pero voy a volver a presentar esto. Si vuelven a otra de las sesiones me van a escuchar a mí haciendo presentaciones sobre este tema y también a otras personas. Este es el momento para que hagan preguntas.

WES HARDAKER: Este es el panel de expertos. Me gustaría que otros expertos también se acerquen. En general, el resto de la tarde es un periodo de preguntas y respuestas. Si tienen preguntas acerca de cómo comenzar, qué significa DNSSEC, cómo funciona. Matt habló acerca de la clave para la firma de la llave. Si tienen alguna otra pregunta, podemos profundizar en estos temas. Por favor, adelante. Haga la primera pregunta.

MICHAEL OGHIA: Hola. Soy Michael Oghia. Es la primera vez que asisto a una reunión de la ICANN y soy becario por primera vez. Tengo una pregunta acerca de DNSSEC. Quizá les parezcan preguntas muy básicas pero estoy aquí en parte porque quiero aprender más sobre este tema.

WES HARDAKER: Está en el lugar adecuado. Por favor, no se sienta mal con respecto a ninguna pregunta que quiera hacer.

MICHAEL OGHIA: La primera pregunta es: La DNSSEC y otras herramientas de seguridad, ¿cómo se complementan? Sé que algunas están a nivel de aplicación y DNSSEC está a nivel de protocolo pero

quisiera saber cómo juntas crean una especie de suite de seguridad para los usuarios. Tengo otra pregunta también pero pueden responder quizá mi primera pregunta.

WES HARDAKER: Quédese ahí mientras alguien responde a su pregunta.

MICHAEL OGHIA: Puedo repetir la pregunta.

WES HARDAKER: ¿Jacques?

JACQUES LATOUR: DNSSEC, a nivel de DNS, conforma la integridad del DNS. Para asegurarse de que vaya al servidor web adecuado cuando tipea un nombre de dominio, DNSSEC garantiza que eso ocurra, que la dirección IP que usted reciba sea válida. DNSSEC no encripta datos. No hace lo que hace https. Eso es a nivel de servidor. Esa es la primera parte de su primera pregunta.

MICHAEL OGHIA: ¿Por qué necesito DNSSEC si tengo https?

WES HARDAKER: ¿Warren?

WARREN KUMARI: Es discutible que si tenemos https, DNS ya no sea tan importante porque si llegan a un lugar incorrecto, seguramente lo van a detectar porque no va a tener el certificado adecuado. Esto en general se dice pero lamentablemente no funciona en todos los casos. En algunos casos es posible que usted llegue a un sitio que está a cargo de un atacante que tiene un certificado. Esto ocurrió hace un tiempo en algunos países. También, si no tiene DNSSEC, un atacante podría darle siempre una respuesta equivocada y usted iría siempre al lugar equivocado. DNSSEC también permite hace otras cosas muy buenas. Se pueden agregar por encima de DNSSEC. Se puede utilizar con protocolos subyacentes para agregarle otras cosas interesantes. Es una muy buena pregunta porque mucha gente no entiende que hacen cosas diferentes.

MICHAEL OGHIA: Muchas gracias. Ahora entiendo muy bien la diferencia. En términos de los datos que se envían a través de un sitio web, van a ir a un canal https encriptado mientras que el sitio inicial que me van a mostrar como usuario final quizá sea algo malicioso. Gracias.

WES HARDAKER: Hay niveles de seguridad. DNS puede enviarte al lugar adecuado y no hay seguridad DNS que pueda ayudarte si fuiste al lugar equivocado. La seguridad de enrutamiento te asegura llegar al lugar adecuado y la seguridad de las aplicaciones se necesita para asegurarse de que tenga los datos correctos. Sí, es complejo.

MICHAEL OGHIA: Un atacante podría tener un sitio web encriptado. La segunda pregunta es un poco diferente. ¿Por qué no todos los registradores ofrecen DNSSEC para cada uno de los TLD? Por ejemplo, yo tengo una dirección .ORG y mi registrador no ofrece DNSSEC y no entiendo por qué. Estoy dispuesto a pagar por DNSSEC.

WES HARDAKER: Yo tampoco entiendo por qué. Siempre puede pensar en cambiar de registrador. Hay muchos registradores. La mayoría creo que lo ofrecen. Ofrecen una opción económica totalmente aceptable.

CRISTIAN HESSELMAN: Inicialmente, las empresas no estaban tan familiarizadas con la tecnología. Por supuesto, implica una actualización de su

infraestructura. Por eso también necesitan ver cuáles son los beneficios. Usted es una de las primeras personas que escucho plantear este requerimiento de DNSSEC porque, en general, los usuarios finales ni siquiera saben qué es DNSSEC. Simplemente se ocupan del nombre de dominio. Por lo tanto, no hay una demanda por parte de los clientes. Es un tema de infraestructura que deben implementar los registradores y no hay una demanda por parte de los clientes por el momento. Muchos registros, y con frecuencia los registros de ccTLD, tratan de motivar a sus registradores a activar la utilización de DNSSEC, ya sea a través de educación o programas de incentivos que en general son programas de monitoreo para lograr que estos registradores firmen sus nombres de dominio.

MICHAEL OGHIA: Hace un par de días tuvimos una conversación diferente en otro evento y ahí también teníamos el aspecto monetario. La falta de demanda de los clientes de DNSSEC. Voy a empezar a escribirles emails a mis registradores diciéndoles: ¿Por qué no tienen DNSSEC? Es ridículo.

WES HARDAKER: Sí. Como dijo el orador anterior, hay algunos que ya lo ofrecen. Contratándolos a ellos, usted puede acceder directamente. Hay

una pregunta en línea y hay una o dos preguntas aquí. Respondamos primero a la pregunta online.

JULIE HEDLUND: Muchas gracias. La pregunta proviene de Alexandrine Gauvin. Dice: "¿Es necesario activar DNSSEC en todos los niveles (ISP, navegador, servidor de registro de TLD, software, etc. para que realmente funcione?"

WES HARDAKER: ¿Quién levanta la mano? Adelante.

ERWIN LANSING: La respuesta breve es sí. Por lo menos, en cuanto a la parte DNS. Es necesario tener toda la jerarquía. Desde la raíz hasta la zona que buscamos tiene que estar firmado. El servidor recursivo tiene que buscarlo. No vamos a hablar acerca de cuánto hay que acercarse al navegador. Si queremos estar realmente seguros, tenemos que utilizar canales seguros. Todavía no llegamos ahí pero, por lo menos, necesitamos considerar esto, considerar toda la cadena completa.

WARREN KUMARI: Hay una pregunta adicional. La mayoría o todos los nuevos gTLD están solicitando DNSSEC. Muchos otros TLD también. Muchos

registradores lo hacen pero no todos. Una gran cantidad de resolutores recursivos también lo hacen, muchos de los grandes. El DNS público de Google, VeriSign, muchos hacen validación de DNSSEC. Geoff Houston, que creo que no está acá, Geoff hizo algunos experimentos y demuestra que el 15% de todas las consultas están protegidas con DNSSEC hoy en día. Esto sin embargo solo los protege en medida del resolutor. Lo bueno sería tener una forma segura de que esa respuesta llegue a la máquina de cada uno de ustedes. Lo mejor sería que cada una de las máquinas hiciera su propia validación. Algo que ahora se puede hacer si uno está dispuesto a dedicar el tiempo y el esfuerzo. El trigger de DNSSEC es un software que existe. Hay navegadores que hacen validación de DNSSEC. Bloodhound es uno. Trabaja con Firefox. Hay algunas extensiones que se pueden agregar al navegador y va a aparecer una tilde de validación que demuestra que se hizo la validación con DNSSEC.

WES HARDAKER: Hay un proceso de traspaso. Todo lo que se traspase antes estará protegido antes. No es que todo el árbol realiza la firma. Se puede firmar de a poco. Si se firma la zona, se registra con el TLD padre que está firmado, sus datos están protegidos. Si su competidor no lo hace, es su culpa. En este momento creo que tenemos 0.5% de la zona .COM ya firmada. Parece un porcentaje muy pequeño pero son como 500.000 dominios en .COM, que es

bastante bueno. Estamos empezando a ver un despliegue mundial importante.

WARREN KUMARI: Hay otros TLD que requieren DNSSEC. Creo que .BANK y .INSURANCE. Creo que ambos requieren que estén firmados por DNSSEC porque es una seguridad que ayuda a sus usuarios a tener más confianza en que van al banco correcto.

WES HARDAKER: Tengo una pregunta por aquí.

CLEMENT GENTY: Soy Clement. Estoy haciendo un doctorado y soy miembro de NextGen. No sé si fue Jean Jacques quien dijo que el DNSSEC era invisible para el usuario final. ¿Es posible que ICANN le pida al registrador que ofrezca DNSSEC para todos los dominios? ¿Por qué no es una obligación tener la escala más baja de seguridad a través de DNSSEC? Gracias.

WES HARDAKER: ¿Matt? Hay un ómnibus que está a punto de atropellarte.

MATT LARSON: Quiero comprobar que haya comprendido la pregunta porque no escuché el comentario de Jean Jacques. ¿El comentario era sobre la firma de los dominios o sobre la incapacidad de las aplicaciones de ver el estado de validación de DNSSEC?

WES HARDAKER: Su pregunta entonces era si los registradores pueden solicitarle más a los registros.

CLEMENT GENTY: ¿Por qué tenemos que pagar por DNSSEC? Esa es mi pregunta. ¿Por qué no viene ya incorporado?

MATT LARSON: Ya está incorporado. ICANN hace tiempo que existe. Cuando DNSSEC no tenía tal despliegue. Hay registros y registradores que tienen un compromiso que predata el despliegue de DNSSEC que tenemos hoy día. Creo que ICANN ha hecho algunas cosas para implementar DNSSEC. Hay ciertos aspectos. Por ejemplo, los modelos de negocios de los registradores. Tienen distintos abordajes de acreditación con ICANN. La venta de nombres de dominio es solo un aspecto de los modelos de negocios. Es simplemente un área que no ha sido especificada por la ICANN y es el mercado el que la maneja en estos momentos.

WES HARDAKER: Como muchos acuerdos entre los gobiernos y las entidades comerciales y distintos organismos, hay muchas cosas preexistentes que no son afectadas por las nuevas reglas. Cada vez que sale un nuevo documento, como que los nuevos gTLD tienen que cumplir con DNSSEC, es porque siguieron un procedimiento de formalización en papel. Los gobiernos entran en esta categoría. A medida que entran nuevas cosas en línea, cada vez vemos más requerimientos oficiales. Es un proceso de traspaso que involucra remplazar primero todo lo antiguo. Tenemos una pregunta en el micrófono primero.

ORADOR DESCONOCIDO: Hola. Soy [inaudible]. Muy nuevo aquí. Tengo esta identificación verde que dice “Recién llegado”. Soy del capítulo noruego de Internet Society. Quiero preguntarles si alguien como yo en un capítulo de la Internet Society, ¿cómo podríamos ayudar a generar visibilidad para el DNSSEC, para todos? ¿Qué tenemos que hacer? ¿Alguna idea, por favor? Me encantaría saberlo.

MATT LARSON: Mi obligación es hablar siempre en lo posible del traspaso de la KSK. Conozco ISP en Noruega que han habilitado la validación del DNSSEC y que no han escuchado las docenas de

presentaciones que hemos hecho con mis colegas para asegurar que sepan que el 11 de octubre de 2017… No sé si ya hablé de esta fecha. ¿Ya la mencioné? 11 de octubre de 2017. Se va a hacer el traspaso. Hablando en serio, ese es un servicio viable. Algo que tratamos de hacer. Presentaciones como estas para que se conozca el tema.

WES HARDAKER: Jacques.

JACQUES LATOUR: Uno de los buenos recursos de ISOC es que tienen el programa DEPLOY360. Hay una sección sobre DNSSEC que incluye mucha documentación. Hemos trabajado mucho en esta documentación para que los principiantes entiendan los fundamentos de la DNSSEC desde la implementación en los ISP, las TLD en las distintas regiones. Dan York es la persona que trabaja con esto, que es la que más tiempo destinó a esta documentación. En el mismo lugar hay algo nuevo, que se llama IPv6. Es nuevo pero es viejo. Está en proceso de implementarse con sus desafíos. ICANN no puede decirle al mundo que haga IPv6 y DNSSEC. Puede recomendar usar protocolos nuevos pero no puede exigir que se usen. Ese es el desafío que enfrentamos ahora.

WES HARDAKER: Warren.

WARREN KUMARI: En ese sentido, la Internet Society ha hecho un muy buen trabajo en la divulgación del DNSSEC. Dan York, y .ORG también, que es manejado por la Internet Society, fue uno de los primeros TLD firmados y sigue mejorando. Lo que usted puede hacer es firmar su zona y hablar con más personas en Noruega. Sugerirles que es algo bueno. Explicarles los beneficios, etc. Como Jacques mencionó el IPv6, tenemos un gran porcentaje dependiendo de qué área estemos trabajando. DNSSEC necesita más trabajo en lo que hace al IPv6.

WES HARDAKER: Antes de seguir, voy a presentarme primero a mí y al panel, rápidamente. Nos presentamos y decimos quiénes somos. Yo trabajo en la Universidad de California.

CRISTIAN HESSELMAN: Soy Cristian Hesselman. Estoy con .NL, el registro de los Países Bajos.

JACQUES LATOUR: Soy Jacques Latour, de .CA, de Canadá.

ERWIN LANSING: Erwin Lansing, de .DK, de Dinamarca. Bienvenidos.

WARREN KUMARI: Warren Kumari. Soy de Google.

MATT LARSON: Matt Larson, de ICANN.

WES HARDAKER: Julie.

JULIE HEDLUND: Sin duda no soy una experta. Julie Hedlund, del personal de la ICANN.

WES HARDAKER: Kathy.

KATHY SCHNITT: Kathy, del personal de ICANN.

WES HARDAKER: Gracias a todos.

OLGA KYRYLIUK: Soy fellow de Ucrania. Mi pregunta puede parecer estúpida pero quiero hacerla. Si el registrador no habilita estas verificaciones de DNSSEC, ¿significa que no estaré autorizada para validar el DNS? Si no habilito en mi navegador, significa que no voy a ver la tilde verde. Usted dijo que el 50% de los registradores los usan pero yo nunca lo he visto. ¿Significa que no habilité la función en el navegador o qué?

WES HARDAKER: Voy a empezar a responder. La tilde verde está en una sola página. Eso es algo que hicimos nosotros en DNSSEC-deployment.org. A lo mejor los confundí. Lo que quería decir es que tenemos un navegador que resolvió ese problema pero el ISP, si usted está con un ISP seguro que utiliza validación de DNSSEC con sus resolutores, utilizan ellos la tilde verde. Del lado suyo no va a haber nada. ¿Quieres agregar algo, Matt?

MATT LARSON: Es importante distinguir cada vez que hablamos de DNSSEC que hay que recordar que estamos hablando de dos cosas importantes. El lado de la firma, donde hay datos de DNS sobre los que tenemos responsabilidad, un nombre de dominio que está activo en la Internet, y para participar en DNSSEC hay que

firmar esos datos. Ese es el lado de la firma. Del otro lado es alguien que busca los datos. Es el lado de la validación. Si usa un ISP o la empresa tiene validación por DNSSEC, puede consumir los datos firmados en la zona y validar. Ambas cosas tienen que estar funcionando para aprovechar lo que es DNSSEC. Si se firman los datos y se ponen datos firmados disponibles pero nadie los busca y los valida, que es la mitad del camino, está a medias. Pero si hace validación y se va a dominios que no están firmados, no se completa. En el contexto de los registradores, estamos hablando de la capacidad, como dueño del dominio, de poner la información DNSSEC necesaria para que el dominio esté vinculado con la otra parte del mundo, con el lado de la firma. Está entonces el lado de la firma y de la validación. Hay todavía un lado en que los registradores en general no están involucrados sino los ISP y las grandes empresas.

CRISTIAN HESSELMAN: Iba a decir algo similar.

WES HARDAKER: Tenemos otra pregunta.

WARREN KUMARI: Creo que usted dijo Ucrania. Acabo de chequear el ccTLD de Ucrania y este está firmado. Quizá ya esté en DNSSEC.

CLAIRE CRAIG: Buenas tardes. Soy Claire Craig. Soy de Trinidad y Tobago. Pertenezco al campo de la investigación. Cuando surgen estos temas, lo considero siempre desde el punto de vista del usuario porque estamos haciendo muchas cosas para que los no conectados se conecten. Muchas veces el usuario final se conecta y hace cosas tontas en la Internet porque no saben. Como usuario final, yo no quiero enterarme de qué es DNSSEC. De hecho, no sé nada sobre DNSSEC. ¿Cómo opero segura en Internet yo? ¿Qué rol tengo que cumplir? ¿Cómo obtengo información para actuar frente a mi ISP o mi gobierno? ¿Qué necesito saber como usuario final para estar segura en Internet? Parte de lo que hacemos es enseñar a la gente cómo ser seguros en las redes sociales. De igual modo, tenemos que hacer algo, tener algún tipo de iniciativa para los usuarios finales. Gracias.

WARREN KUMARI: Seguramente hay muchas respuestas pero usted, como usuario final, asumiendo que el ISP tiene habilitado DNSSEC, usted como usuario final no tiene que hacer ni saber nada. Si hay un problema con el DNSSEC, usted simplemente no podrá ir al sitio web. Habrá un ataque en el DNS y usted no podrá llegar al sitio web. Habrá un fallo. Si puede llegar al sitio o si puede hacer lobbying con el ISP, debo señalar que esto no la va a mantener

segura, totalmente segura en línea. Solo una parte. Al igual que hay que verificar cómo se funciona en las redes sociales.

CLAIRE CRAIG: Lo que quería decir es que no sé nada sobre DNSSEC. No puedo exigirle nada al ISP. El ISP me va a decir: "No lo podemos pagar. Tenemos que cambiar la infraestructura. No nos interesa hacer eso en este momento". ¿Qué podemos hacer los usuarios para asegurarnos de que la Internet sea segura?

MATT LARSON: Warren, quizá pueda responder mejor pero yo diré que usted puede usar un servidor de nombres recursivos que hace DNSSEC. El más grande es el DNS público de Google pero también VeriSign tiene uno. Seguramente hay otros. No los recuerdo ahora. Es lo más significativo que pueden hacer los usuarios. Requiere cierto nivel de sofisticación del usuario para ir a la configuración, cambiar los valores por omisión. La manera más sencilla es conseguir que el ISP haga validación. Los usuarios tienen que encontrar una manera de pasar a servidores recursivos habilitados por DNSSEC.

WES HARDAKER: Yo diría que se podría usar un resolutor alternativo pero está en las configuraciones avanzadas.

WARREN KUMARI: He buscado en el sitio de Geoff Houston, quien recaba estadísticas, y dice que el 3,3% de las personas en Trinidad y Tobago ya hacen validación del DNSSEC. Algunos ISP ya dan soporte.

WES HARDAKER: ¿Alguien levantó la mano? Tome la palabra. Tenemos otra más por aquí.

SIMON SOHEL BAROI: Soy Simon. Vengo de Bangladesh. Quizá mi pregunta sea tonta pero este año América cambió de presidente. El presidente Trump. Usted dijo que tienen esas llaves en distintos lugares dentro de los Estados Unidos. ¿Por qué no en distintos países? Esa es mi primera pregunta. Mi segunda pregunta es otra pregunta tonta. Yo vengo de un país menos desarrollado. En países como estos, un proyecto como el DNSSEC, IPv6, RPKI, todos estos proyectos no funcionan muy bien. El DNSSEC empezó hace unos 10 años. RPKI comenzó hace cinco. IPv6 antes de que empezara la Internet. ¿Por qué estos proyectos no salen a la luz? Geoff dijo que el 17% del mundo tiene resolutores con DNSSEC. ¿Por qué? Son dos preguntas.

MATT LARSON: Creo que responderé a la primera pregunta. Cuando firmamos la raíz en el 2010, ahí fue cuando la ICANN todavía tenía la validación con el departamento de Comercio estadounidense. El requerimiento para firmar la raíz era que el material de la llave quedara dentro de los Estados Unidos. Por eso tenemos las instalaciones en la costa este y la costa oeste con la mayor distancia posible entre ambas localizaciones. Usted ha planteado una pregunta que se hicieron muchos antes de la transición y durante. ¿Por qué no fuera de los Estados Unidos? En mi opinión es muy razonable esta pregunta. Habría más oportunidades de evitar problemas con la llave. Sería una acción muy importante y muy costosa que ICANN mudara estas instalaciones. Sería muy complicado porque imagino que serían muchos los países interesados en alojar la llave.

Habiendo dicho esto, es algo que la ICANN como organización tiene que liderar en ICANN comunidad. Si la comunidad dice claramente que esto es una prioridad, que debiera haber instalaciones de gestión de la llave fuera de los Estados Unidos, esto debiera ser un aporte, una contribución al desarrollo de políticas y priorizarse respecto de otras cosas que requiere la comunidad que hagamos y destinemos fondos.

JACQUES LATOUR: Voy a responder a la segunda parte, si me permite.

WARREN KUMARI: Voy a responder a la primera pregunta un poco más. Sí, las llaves están en los Estados Unidos pero para usar las llaves se requiere la participación de representantes de comunidades confiables que vienen de distintos países. Cuando las llaves se usan, hay personas que vuelan de otros países y hacen cosas. Las llaves están en los Estados Unidos pero están conservadas o se mantienen en enclaves. Si alguien trata de abrirlas, salen alarmas y pasan cosas muy malas. Sí, es algo que asusta pero es menos problemático de lo que parece.

JACQUES LATOUR: Con respecto a la segunda pregunta, IPv4 hace 45 años que funciona. Creo que me parece que ya es hora de que empecemos a jubilarlo. El DNSSEC hace tiempo que existe también. La razón principal es que los seres humanos resisten el cambio. Por algún motivo nos encanta el IPv4 e intentamos maneras de hacer que dure más, cada vez más. Yo soy un defensor de cerrar IPv4 y pasar al IPv6. Cuando hablo de esto con algunas personas me preguntan por qué parar el IPv4 y me dicen que no se puede hacer. Hay que cambiar. Manejar el cambio sobre una base global es algo muy difícil. Por eso en la Internet tenemos que enfrentar estas cosas.

CRISTIAN HESSELMAN: El cambio se daría más rápido si hubiera una demanda de los clientes que no existen. En este caso es una actualización de la infraestructura que tenemos que realizar como comunidad. Además, quería decir otra cosa pero me olvidé.

WES HARDAKER: Hay mucha tecnología que tiene un costo asociado. La nueva tecnología tiene un costo asociado. Siempre hay que tener en cuenta todo lo que se quiera seguir, el costo asociado. Lamentablemente, a veces la seguridad va más hacia abajo en las prioridades porque no tiene un componente inmediatamente visible hasta que alguien recibe un ataque. Tanto el RPKI como el DNSSEC e IPv6, hay un costo enorme asociado a todos ellos. Lleva tiempo.

JAD EL CHAM: Hola. Soy Jad El Cham. Soy un becario por primera vez. Yo tengo una formación puramente técnica. Por lo tanto, mi pregunta es puramente técnica. Hemos visto recientemente, en los últimos dos años, cada vez más proveedores que ofrecen seguridad a través de DNS en términos de hacer el relay, de consulta al DNS a proveedores de DNS en la nube y en general tienen algunos centros de scrubbing. Identifican la consulta de DNS y nos dan una respuesta a nosotros. Una de las soluciones es, por ejemplo, el VPN abierto requerido por Cisco. También he visto antivirus o

software antimalware que cuando se instala en las PC, piden permiso para reenrutar y cambiar los servidores de DNS que usaría cualquier PC. Mi pregunta tiene dos partes. Por un lado, ¿esta clase de soluciones son una alternativa para DNSSEC? Porque si vemos por ejemplo el VPN abierto solo tiene un 2% de todo el tráfico de DNS o de las consultas, por lo menos. La segunda pregunta es ¿pueden avanzar? ¿Funcionan?

ERWIN LANSING: Yo diría que avanzan en cuanto a que esos servicios de confianza le dan parte de la respuesta y el DNS formaría parte de eso porque le garantizaría la respuesta correcta. También se utilizan otras cosas como listas negras conocidas de virus o malware. DNSSEC definitivamente es parte de lo que tendrían que hacer antes de darle una respuesta.

WES HARDAKER: ¿Alguien más? Muchas gracias. Voy salteando a las personas porque no los veo.

RACHEL POLLACK: No hay ningún problema. Estaba cerca y me acerqué al micrófono. Soy Rachel Pollack. Soy embajadora de NextGen. Trabajo en la UNESCO sobre libertad de expresión. Mi pregunta proviene también de una formación no técnica. Hoy es el día

mundial contra la censura en el ciberespacio. Yo creo que una forma de censura podría ser redireccionamiento de DNS. Me pregunto si DNSSEC podría desempeñar algún papel en cuanto a que los usuarios lleguen al lugar correcto. Si fuera así, quisiera saber si hubo alguna clase de resistencia política o de otro tipo en este sentido. Gracias.

WARREN KUMARI: Hay dos respuestas. Por un lado, sí, DNSSEC puede por lo menos ayudar a evitar la censura a través del DNS o por lo menos dejar en claro que está ocurriendo. Quizá no pueda detener la censura pero por lo menos podemos identificar que hay alguien que está alterando las consultas de DNS, lo cual ayuda a exponer la censura. Gran parte de la censura se hace con el DNS. Muchos ISP o países tratan de identificar consultas determinadas y las detienen. Esto es algo que el IETF se ha tomado muy en serio. De hecho, yo dirijo un grupo de trabajo que se llama Deprive. Estamos tratando de privar a los atacantes de la información de DNS. Se encriptan los datos de DNS de la máquina cliente. De esa forma, los sensores no pueden ver que usted está tratando de llegar a un sitio al que ellos no quieren que usted llegue. Esto es algo que se está empezando a implementar y debería avanzar mucho en términos de la censura y de evitarla.

MATT LARSON: Quisiera decir que en la mayoría de los casos, si alguien va a ejercer la censura a través del DNS, esto en general ocurre donde ocurre la validación de DNS, el servidor de nombres recursivos en el ISP. Mi teléfono está configurado para utilizar un servidor de nombres recursivos que está en algún lugar. En general es ahí donde se produce la validación o donde se produce la censura de contenidos. Diseñamos el protocolo de DNS de forma tal que mi teléfono pueda hacer validación de DNSSEC solo, sin tener que confiar en lo que está más arriba, por así decirlo. Uno de los miembros del panel habló acerca de la última milla. Nosotros lo llamamos la última milla. Tenemos que confiar entonces en lo que nos dice el servidor de nombres recursivo. Si hace validación de DNSSEC, mejor. Por distintos motivos como la antigüedad del software o las API, por muchas razones la validación de DNSSEC no llegó todavía a los dispositivos de los usuarios pero esta sería la forma en la que podríamos impedir que alguien altere los resultados que le llegan a usted.

WES HARDAKER: Creo que ese es el punto al que llegaremos en el largo plazo. Hablo acerca del teléfono. Podemos pensar en otros ejemplos. Es muy posible. DNSSEC no es tan especial que tenga que usarse solamente en grandes cosas. También puede implementarse fácilmente en pequeños dispositivos.

RACHEL POLLACK: Muchas gracias.

WES HARDAKER: Adelante.

ORADOR DESCONOCIDO: Trabajo para la Oficina de Intercambio de Internet de la India. También trabajo en el Foro de Gobernanza de Internet en la India. Una de mis funciones en mi trabajo es asesorar al gobierno de India acerca de las propuestas. Trabajamos con la Sociedad de Internet. Hay una propuesta. La Sociedad de Internet nos hizo algunas preguntas. ¿Por qué tenemos este tipo de centros en India? Yo empecé entonces un informe publicado por la ISOC que habla acerca de la implementación de DNSSEC. Yo asesoro en ese sentido. Dividí todo el proceso en dos fases. DNSSEC en India que lleva a cabo un estudio sobre información, hechos y datos sobre el proyecto, registros, registradores y dueños de sitios web que están implementando DNSSEC.

La segunda fase, después de la exitosa implementación de la primera fase, vamos a empezar a capacitar y a desarrollar programas de capacitación para ISP. Vamos a hacer que sean obligatorios para los sitios web gubernamentales. Que sea obligatorio implementar DNSSEC en India y también en todos los

sitios web que se registran y que se utilicen, así como en las nuevas aplicaciones. Quisiera saber qué papel puede desempeñar la ICANN en cuanto al apoyo que puede recibir esta sociedad técnica de la ICANN.

JACQUES LATOUR: ¿Está hablando acerca de implementar el Centro de Excelencia DNSSEC? La respuesta es sí. Hagan eso porque hay muchas innovaciones en torno a DNSSEC que van más allá de las consultas de DNS simplemente. Si asiste al taller que tendrá lugar el miércoles verá que se está desarrollando nueva tecnología por encima de DNSSEC que permite la encriptación de correo electrónico, la certificación. Hay nuevos protocolos que se están desarrollando en DNSSEC que pueden cambiar Internet. Sin duda podemos hacer eso y creo que la ICANN también tiene recursos para ayudarlos a brindar capacitación sobre este tema.

ORADOR DESCONOCIDO: Nosotros desarrollamos un taller con la ICANN en Mumbai también. Seguimos sin implementar DNSSEC en gran medida. La gente viene a la capacitación pero luego no lo implementa. Ese es el problema. Estamos pensando en principio hacer que sea obligatorio para todos los sitios web del gobierno. Después vamos a llegar a los otros sitios web. Primero queremos apoyo

técnico y capacitación técnica de la ICANN para poder desarrollar juntos un centro de excelencia de DNSSEC en mi país.

MATT LARSON: Sin duda, apoyo eso. Creo que es una muy buena idea. Alguna de mis colegas en la oficina del director de tecnología de la ICANN hace capacitación de DNSSEC. Como todas las organizaciones, tenemos algunos problemas con el ancho de banda. No sé cuánto podemos ayudarlos en términos de personal pero voy a ponerlo en contacto con nuestro colega Rick Lamb, que no está acá para defenderse. Le voy a dar su nombre. En serio, él ha sido un partidario incansable de la implementación de DNSSEC y ha brindado capacitación de DNSSEC en todo el mundo. Esta es una de las cosas que hace. Eso es lo primero que se me ocurre cuando escucho su solicitud de ayuda para la ICANN. También quisiera decirle que venga a las reuniones de la ICANN porque este es el lugar. En este tipo de salas donde hablamos sobre esto. El miércoles tenemos el taller de DNSSEC. Ahí tiene las fechas en pantalla. Ese es el lugar donde podrá reunirse con nuestros colegas de DNSSEC y con la industria. Quizá esto no sea ayuda de la ICANN como realización per se pero esperamos poder ayudarlo a facilitar el contacto con otras personas que están haciendo lo mismo.

WARREN KUMARI: Cuando usted dice que la gente no lo está implementando, resulta que la India tiene un grado de implementación un poco más alto que otros países.

ORADOR DESCONOCIDO: Sí. Eso se debe a que en la India hay muchos usuarios pero hay 400 millones de usuarios de Internet. Si comparamos los porcentajes, vemos que siguen siendo bajos y el riesgo es grande.

WARREN KUMARI: Incluso desde el punto de vista porcentual, en India hay un 17% de validación, lo cual es alto desde el punto de vista global. En cuanto a que los sitios del gobierno hagan la validación con DNSSEC, un movimiento inicial de DNSSEC lo está haciendo el gobierno de Estados Unidos que también dijo que todos los dominios gubernamentales van a tener que estar validados con DNSSEC. Ese es un gran avance en cuanto a lograr la implementación de DNSSEC y también es un gran avance en cuanto a lograr que la gente repare y actualice su infraestructura de DNSSEC. El gobierno está trabajando mucho mejor que antes.

WES HARDAKER: Ese esfuerzo del gobierno de Estados Unidos llevó a la creación de muchas herramientas que ahora utilizan otros porque fueron los primeros en adoptarlo. Hay otra pregunta allí al fondo.

ABDERRAHMAN AIT ALI: Hola. Soy Abderrahman. Soy becario de NextGen. Tengo una pregunta breve acerca del costo de transición. Quisiera saber cuán fácil o difícil es hacer la transición de DNS a DNSSEC. ¿Hay incentivos suficientes para aquellos responsables de hacer la transición? Eso es todo.

CRISTIAN HESSELMAN: En cuanto a los registradores, en Holanda nosotros tenemos un programa de incentivos. Les damos un descuento en los nombres de dominio que registran en nuestra empresa. Creo que hay programas similares en Suecia y en otros registros. Para bajar un poco el umbral en términos financieros, para que empiecen a firmar los nombres de dominio y después tenemos el otro extremo, tenemos los ISP. En el caso de ellos, por lo menos en mi país, no se trata tanto del costo de implementar la validación de DNSSEC lo que les preocupa sino las llamadas de soporte potencial que tienen miedo de recibir, por errores por ejemplo. Esto es algo a lo que le temen pero por lo menos los grandes ISP en Holanda, ahora decidieron pasar a DNSSEC de todas formas. Es una falta de entendimiento de la tecnología

también en este caso. Para estas organizaciones no se trata tanto del costo de la validación sino del costo de la implementación de los sistemas. Son dos costos diferentes, si entiende a lo que me refiero.

ABDERRAHMAN AIT ALI: Sí, pero todo puede reducirse a costo. Es decir, el tiempo es dinero. Creación de capacidades también.

CRISTIAN HESSELMAN: Si para los registradores usamos un programa incentivo, ¿por qué tenemos una relación de clientes con ellos? En el caso de los ISP, ellos deciden por su cuenta si empezar la validación o no. ¿Respondí su pregunta?

ABDERRAHMAN AIT ALI: Sí. Muchas gracias.

WES HARDAKER: Tenemos tiempo para una pregunta más o dos quizá. Adelante.

CHAWANA HUANGSUNTORNCHAI: Hola. Una pregunta breve. Yo soy Chawana. Formo parte del programa NextGen. ¿Hay alguna posibilidad o ha ocurrido

que DNSSEC haya verificado: “Está la tilde verde en la URL” pero a pesar de eso es un sitio web falso? ¿Ha ocurrido esto?

WES HARDAKER: Usted habló primero.

WARREN KUMARI: Bueno, por lo que sé, no hubo ningún problema técnico en relación con DNSSEC. No hubo ningún caso en donde DNSSEC haya mostrado esa tilde verde de manera incorrecta. Quiero explicarles qué significa esa tilde de verificación. Solo significa que los datos que vienen de DNS es la información que se ingresó en DNS. Si alguien tipea la dirección incorrecta al configurar el servidor DNS, DNS igual va a mostrar esa marca de validación, aun cuando la persona haya tipeado el nombre incorrectamente. Simplemente valida que surgió de allí la información correcta.

CHAWANA HUANGSUNTORNCHAI: Entonces si entra basura, sale basura.

WARREN KUMARI: Exacto. Pero no hubo ningún caso en donde el DNSSEC haya dicho que hay algo válido cuando no lo era.

WES HARDAKER: Yo hablé con muchos autores de los navegadores y hay mucho debate acerca de cuál es la forma adecuada de utilizarlo. Creo que la respuesta todavía no está allí. Julie tiene una pregunta remota.

JULIE HEDLUND: Gracias. Hay una pregunta de Alexandrine Gauvin. La pregunta es: "¿Cómo puedo verificar que un ISP tenga la validación de DNSSEC?"

WES HARDAKER: Es una muy buena pregunta. Ojalá tuviéramos una lista.

WARREN KUMARI: Creo que igual van a aparecer nombres inválidos de DNSSEC. Habría que ir a la página de phishing y ver si aparece ahí. Así es como yo haría esta validación.

WES HARDAKER: Hay algunos dominios a los que podemos ir y que nos dicen si el ISP está haciendo la validación. Creo que hay un término que es DNSSEC-ready. DNSSEC-deployment.org es uno de los sitios. Hay otro que tiene un pulgar hacia arriba o un pulgar hacia abajo. Es muy obvio. Llena toda la página.

CRISTIAN HESSELMAN: No tengo una respuesta específica. Hay un sitio web donde en general mostramos el porcentaje de tráfico que recibimos que pide material clave DNSSEC. Esto sugiere por lo menos que el origen del tráfico está habilitado para trabajar con DNSSEC. Si se fijan en nuestro sitio, podrán ver cuáles son los ISP que piden firmas en el DNS.

WES HARDAKER: En el Android Marketplace, yo creé una herramienta hace muchos años que hace una prueba extensiva del resolutor del ISP, no solamente DNSSEC y validación sino que da muchos puntos rojos y verdes en función de diferentes cosas. Es para expertos pero si ven mucho verde significa que está bien. ¿Alguien encontró el otro sitio web? Hay algunos sí, unos cuantos. Creo que queda tiempo para una última pregunta. ¿Alguien tiene una última pregunta?

ORADOR DESCONOCIDO: Hola. Quisiera hacer una pregunta acerca de los sistemas DNSSEC y cómo interactúa con Internet o con la seguridad de Internet. Si este problema de la seguridad de DNSSEC está resuelto o no, ¿hay alguna hipótesis con respecto a hacia dónde van los problemas de seguridad del DNS? si ataco el DNS y ustedes resuelven el problema del DNS, ¿dónde ataco en segundo lugar?

WES HARDAKER: Es una buena pregunta.

CRISTIAN HESSELMAN: Probablemente sea el Internet de las cosas, porque hay todo tipo de dispositivos que pueden hackearse fácilmente. Ese también es un desafío importante desde el punto de vista de la seguridad en Internet hoy en día.

WES HARDAKER: Usted planteó un punto fundamental. Internet empezó como algo muy pequeño que no era seguro y después tuvimos que ir incorporando estas soluciones. Parecería que siempre hay un próximo lugar. ¿Usted quiere hacer otro comentario? Habiendo dicho esto, quiero agradecerles a los miembros del panel por habernos ayudado a responder las preguntas. Un aplauso para ellos. Quisiera señalarles que hay otros recursos a los que pueden acceder. Esta semana van a escuchar que se habla de DNSSEC en varios lugares. Hay presentaciones el día técnico, el lunes. Hay toda una serie de material técnico. Si buscan información técnica, los vamos a saturar con más información de la que van a poder manejar. Casi siempre hay alguna presentación sobre DNSSEC. El miércoles tenemos todo un día dedicado a DNSSEC desde las 9:00 hasta las 3:00 de la tarde.

Habrá un taller que tendrá lugar durante todo el día. Ese es el lugar al que yo asistí en mi primera reunión. De hecho, yo voy a hacer el concurso de preguntas y respuestas de DNSSEC. Al venir, ustedes podrían responder correctamente. Si realmente prestan atención a lo que ponemos en las diapositivas. Julie.

JULIE HEDLUND: Quiero agradecerles por el aviso. Espero que asistan al taller y que también todos juntos le agradezcamos a Wes por haber hecho un muy buen trabajo. Realmente lo necesitamos acá. Muchas gracias.

WES HARDAKER: Gracias. No me dieron la oportunidad de agradecerles primero. Julie y Kathy manejaron todo. Lograron que tuviéramos las remeras, que la gente se pusiera las remeras. Tomamos nota de su esfuerzo. Muchas gracias por organizar esto año tras año. Muchas gracias a todos por haber venido. Que tengan muy buenas tardes.

[FIN DE LA TRANSCRIPCIÓN]