BARCELONA – DNSSEC para todos: guía para principiantes
Domingo, 21 de octubre de 2018 – 15:15 a 16:45 CEST
ICANN63 | Barcelona, España

WES HARDAKER: Vamos a explicar cómo DNSSEC hace que todo el mundo sea más seguro si se usa. Lo vamos a hacer a través de un cuento. Vamos a comenzar con los orígenes de DNSSEC que comenzó en el año 5000 a.C. Vamos a presentarles a Ugwina, que vive en los límites del Gran Cañón. Aquellos que no conocen el Gran Cañón, es un cañón enorme en el centro de los Estados Unidos. Aquí tenemos a Og. Él vive en una cueva en la otra punta del Gran Cañón. Viven muy lejos uno del otro. Por lo tanto, no se encuentran con frecuencia para charlas. Yo lo hice. Lleva dos o tres días ir de una punta a la otra y trepar.

Una de las veces que estuvieron de visita, ven que sale humo del fuego de Og. Pronto comienzan a charlar periódicamente y utilizando señales de humo a través de UDP hasta que un día el maldito hombre de las cavernas Kaminsky se muda al lado de Og y empieza a mandar señales de humo también. Para aquellos que no estuvieron por aquí hace 10 años, Kaminsky fue la persona que descubrió una vulnerabilidad muy importante en el DNS. Ahora, Ugwina está muy confundida. No sabe a qué señal de humo creer. No sabe cuál de las señales, sin binoculares, es la que debe leer.

Entonces Ugwina baja del cañón para tratar de resolver todo este lío. Ugwina y Og consultan a los sabios mayores del pueblo. El hombre de las cavernas piensa que tiene una idea astuta. Para aquellos que no

saben quién es Diffie, Diffie fue una de las personas que creó la encriptación de la clave pública que es la base de la criptografía de Internet de hoy en día. Rápidamente, Diffie salta dentro de la caverna de Og y en el fondo encuentra una pila de arena con un color extraño que no se encuentra en ningún otro lugar fuera de la caverna de Og. Rápidamente, sale y tira la arena mágica al fuego y el fuego genera humo de un color azul magnífico.

Ugwina y Og ya pueden volver a charla rápidamente y felizmente de nuevo porque saben que nadie puede interferir con su conversación, porque solo él tiene la arena mágica azul.

Esta es la introducción a DNSSEC. En un formato en diagrama bastante simple. Vamos a volver a hablar de DNS un poco porque funciona de una forma similar a las señales de humo. Hay una forma de estructura de árbol o de jerarquía en el DNS. Comienza con la raíz en la parte superior y por debajo tenemos todos los TLD. Los ccTLD, los gTLD, los nuevos TLD. Por debajo de cada uno de ellos tenemos los puntos de registración donde pasan varias cosas. Los voy a referir a la parte del medio. La raíz delega la información de .COM en los servidores de .COM y .COM delega bigbank en sus servidores.

Un resolutor, cuando trata de resolver una consulta para saber dónde está www.bigbank.com, por ejemplo, no conoce todo el árbol. Tiene que empezar desde arriba pero sí sabe dónde está la zona raíz y puede recorrer la jerarquía del DNS para encontrarlo. Como dije, cada nivel de esa jerarquía se deriva al siguiente nivel. El resolutor entonces sigue la cadena hasta abajo hasta que se responde la pregunta. El resolutor

almacena toda esa información para su uso futuro. La próxima vez que hagan esa pregunta la van a poder responder más rápidamente porque esa información queda guardada en la memoria caché.

Hay un problema con el sistema de DNS sin embargo y es que no fue diseñado con ningún tipo de seguridad así como las señales de humo tampoco tenían seguridad. El DNS supone ingenuamente que todo es correcto. Por lo tanto, es fácil hacer suplantación de nombre y esa información que se guarda en la memoria caché también se puede ver contaminada. Como no alcanzaba con ese diagrama tan simplista ahora vamos a hacer una obra. ¿Cuántos de ustedes ya vieron esta obra? ¿Un par de ustedes? ¿Y el resto? Los que lo vieron antes van a tener que sufrir y volver a verlo. El resto se va a divertir.

Quiero actores voluntarios. Por favor, pónganse de pie los actores voluntarios. Aquí están. Tenemos algunos actores. El usuario promedio. Él va a ser el usuario. Tiene que hacer una transacción bancaria hoy. Tenemos un representante de la raíz. Él representa la raíz en el árbol DNS. Tenemos un ISP que sabe dónde está la raíz. Tenemos .COM y tenemos bigbank.com. Me parece que es mejor que se coloque aquí. Ahora ellos van a continuar. Vamos, adelante. Hola, hola. Muy bien. Ambos funcionan.

TIM: Bueno, tengo todo este dinero. Tengo que hacer un depósito. Tengo que ir a www.bigbank.com para depositar mi dinero.

ORADOR DESCONOCIDO: Bueno, no sé dónde queda así que lo voy a averiguar para que usted lo sepa. Señor Raíz, ¿sabe dónde está bigbank.com?

WES HARDAKER: Hola. No tengo ni idea. Sin embargo, lo puedo ayudar con lo siguiente. Usted podría preguntar a .COM. Quizá él sepa. Está en 1.1.1.

TIM: Perfecto. Lo voy a intentar. Me dijeron que le pregunte a usted si sabe dónde está www.bigbank.com.

ORADOR DESCONOCIDO: Muy buena pregunta. Yo soy .COM. Estoy 1.1.1. Gracias por visitarme. Yo puedo decirle dónde está bigbank. Aquí está. Bigbank está en 2.2.2. ¿Quiere ir allí?

TIM: Gracias. Necesito saber dónde está www.bigbank.com.

RUSS MUNDY: Gracias por preguntarme, señor ISP. De hecho, yo puedo decirle exactamente dónde está bigbank.com. Es 2.2.2.3.

TIM: Gracias. Bigbank.com es 2.2.2.3. Increíble. Ahora puedo ir y depositar mi dinero. Muchas gracias, Bigbank.

WES HARDAKER: En realidad él debería agradecerle a usted. Muy bien. Gracias, gente. Quédense aquí porque los vamos a volver a necesitar en un momento. Esto es lo que hacen. De esto trabajan. Ugwina, el resolutor, cuando chatea con Og, el servidor, hace algo parecido a lo que ustedes acaban de ver. Se comunicaban por señales de humo. No había problema. Nadie interfería. Ahora vamos a ver qué pasa cuando quizá hay algo que sale mal. ¿Podrían repetir por favor la actuación?

TIM: Ahora tengo un millón de dólares que tengo que depositar. Tengo que ir a www.bigbank.com. Voy a ir a mi ISP y le voy a preguntar cómo llego a bigbank.com.

ORADOR DESCONOCIDO: No tengo ni idea pero lo voy a intentar. Hola. ¿Usted sabe dónde queda bigbank.com?

WES HARDAKER: Yo soy la raíz. La verdad, no sé estas cosas. Podría preguntar a .COM. Quizá él sepa. Está en 1.1.1.1.

TIM: Bueno, muy bien. Gracias. Hola, .COM ¿Usted sabe dónde está bigbank.com?

ORADOR DESCONOCIDO: Bienvenido. Yo soy .COM. Le voy a decir dónde está. Bigbank.com está en 2.2.2.

ORADOR DESCONOCIDO: .2.

TIM: Gracias. Hola. ¿Usted sabe dónde queda bigbank.com?

ORADOR DESCONOCIDO: Por supuesto que sí. Es 6.6.6.6.

TIM: Perfecto. Gracias.

ORADOR DESCONOCIDO: Bigbank.com queda 6.6.6.6.

ORADOR DESCONOCIDO: Perfecto, gracias. Voy a depositar mi dinero.

ORADOR DESCONOCIDO: Gracias.

WES HARDAKER: Muy bien. Gracias de nuevo. La pregunta real es cómo salimos de esta sesión horrible con el Sr. Mal frente a todos los grandes bancos.

Ugwina, el resolutor, está confundida. No sabe a qué señal creer porque hay dos y el DNS, el que devuelve la primera respuesta es el primero al que se cree, al menos hasta que surgió DNSSEC. Una vez más, volviendo al mismo gráfico, si dos servidores diferentes nos dan dos respuestas diferentes, quizá tengamos respuestas de bigbank.com de dos fuentes diferentes y no sabremos a cuál creer. Aquí en este diagrama tenemos uno rojo y uno azul. Hay que adivinar cuál es la respuesta correcta.

DNSSEC, de hecho, le suma seguridad al DNS. Utiliza firmas digitales para hacerlo. Básicamente, garantiza dos cosas, que la información no fue alterada y que se originó en el lugar correcto. No importa en cuántos lugares se haya almacenado, cuántas memorias caché lo tengan. Es información que no fue alterada. Sabemos de dónde viene. Las claves y firmas se almacenan en el DNS también y como el DNS es un sistema de búsqueda, se pueden buscar las claves y las firmas al igual que cualquier otro dato.

El concepto general de DNSSEC es que el resolutor sabe no solamente dónde está el servidor raíz sino también dónde está la llave de la raíz. Siempre y cuando sepa esto, esa es la información inicial y puede continuar recorriendo el resto del árbol. Lo puede hacer generando una cadena de confianza. Cada nivel firma el siguiente nivel hasta que se completa toda la cadena y se llega a la respuesta que uno busca. De esa forma, finalmente el resolutor o el ISP puede determinar cuál de esos dos registros de bigbank es el correcto. El azul es el correcto y el colorado es el incorrecto.

Veamos entonces qué pasó con DNSSEC en la obrita. Hay un par de cosas que vamos a ver hoy. Ustedes podrán ver que ahora tenemos estas medallas que indican las firmas digitales. Cada uno de estos tres servidores de DNS tendrá una medalla y el ISP tendrá una medalla que hace juego para poder verificar que está hablando con la persona correcta.

TIM: Tengo otro depósito para hacer. Tengo que ir a www.bigbank.com para hacer este depósito.

ORADOR DESCONOCIDO: Muy bien. Se lo busco. Hola, raíz. ¿Podría decirme dónde queda bigbank.com?

WES HARDAKER: Yo soy la raíz y puedo demostrar la autenticidad de lo que digo pero no tengo ni idea de dónde está bigbank. Pregunte a .COM, que está 1.1.1.1.

TIM: Muchas gracias. Hola, .COM. ¿Podría decirme dónde queda bigbank.com?

ORADOR DESCONOCIDO: Hola, ISP. Yo soy .COM. Fíjese, soy .COM. ¡Muy bien! ¡Sí! Perfecto. Le voy a decir dónde está bigbank. Bigbank está en 2.2.2.

ORADOR DESCONOCIDO: .2.

ORADOR DESCONOCIDO: Hola, bigbank. ¿Podría decirme dónde queda bigbank.com?

ORADOR DESCONOCIDO: Claro, pero no tengo firma así que usted debería rechazarme.

ORADOR DESCONOCIDO: Oh, no. Adiós. Hola, bigbank, ¿podría decirme dónde queda bigbank.com?

RUSS MUNDY: De hecho, www.bigbank.com queda en 2.2.2.3.

TIM: Gracias. ¿Puedo verificar su firma?

ORADOR DESCONOCIDO: bigbank.com queda en 2.2.2.3 y está firmado.

TIM: Excelente. Ahora puedo depositar mi dinero con seguridad.

ORADOR DESCONOCIDO: Dinero.

WES HARDAKER: Muy bien. Vamos a darles un aplauso a los actores que terminaron la tercera escena de esta obra. Quiero que reconozcan que hacían un ruidito las medallas cuando se chocaban entre sí para verificar la autenticidad. Parece tonto pero esto es lo que ocurre en el sistema de DNS y esto es lo que pasa con DNSSEC. Por supuesto que es un poco más complejo que esto pero en realidad los resolutores sí recorren toda la cadena y pasan por múltiples niveles hasta que llegan a la respuesta final. Esos distintos niveles pueden ser bastante profundos, siempre y cuando DNSSEC proteja a toda la cadena, ustedes van a obtener una respuesta segura a su consulta, al igual que el humo azul protege al resolutor y le permite verificar que Og es el que mandó el mensaje real. Ahora le voy a dar la palabra a Russ Mundy. Debería haberme presentado yo primero. Yo soy Wes, de la Universidad de California. Russ Mundy va a hablar acerca de por qué necesitamos DNSSEC.

RUSS MUNDY: Gracias, Wes. Muchas gracias a los actores de hoy. Fue muy divertido hacerlo con nuevos actores porque este es un elenco nuevo. Muchas gracias a todos los que participaron. Muchas gracias. Se lo agradecemos. Este es el aspecto de la sesión de DNSSEC para todos que apunta a ayudar a todos a pensar en las razones que explican por qué todos, ya sean usuarios finales o ISP o servidores autorizados, por qué todos querrían hacer la validación con DNSSEC para evitar que el Dr. Mal se introduzca en el medio. Para eso está diseñado DNSSEC.

Cuando pensamos en este tema, antes hablábamos acerca del DNS y en términos de DNS, DNS no transfiere dinero entre el usuario y el banco. Hay aplicaciones que se utilizan para hacer esa transferencia. Cuando la gente ataca el DNS y remplaza información, en casi todos los casos lo que hacen es tratar de hacerlo mediante otras aplicaciones y otras funcionalidades.

Si el DNS no funciona correctamente, ya sea un navegador web, un servidor de email o un motor de chat, no van a funcionar bien tampoco y no van a lograr llegar a donde necesitan llegar, a donde quieren llegar o a donde esperan llegar. Ese es el tema fundamental que explica por qué necesitamos que el DNS sea correcto. Tiene que ser correcto para que el resto de las aplicaciones también puedan funcionar correctamente.

Nuestra obra trataba de demostrar este secuestro para que ustedes entiendan cómo funciona este software y cómo sabe el usuario que está hablando con alguien con quien no debería hablar. A lo largo del tiempo ha habido una serie de aplicaciones que han sido atacadas y el ataque comenzó con el DNS. Algunos de los ataques que comenzaron en el DNS terminaron siendo usos explotados de tres o cuatro protocolos adicionales pero comenzaron en el DNS, obteniendo información de DNS que los delincuentes necesitan para llegar a otro lugar y aprovecharse de las personas de las que están tratando de aprovecharse.

En algún momento, creo que en los últimos dos años no lo vi pero en un momento había un curso universitario en dos universidades

diferentes que exigía que los estudiantes desarrollen una herramienta de ataque al DNS. Esto demuestra cuán fácil es relativamente hacerlo. Hay software disponible en Internet para hacerlo. Es un software de ataque al DNS pero el problema es que hay información online pero en esta información no había nada acerca del aspecto de la ética, acerca de que esto es algo que no habría que hacer en realidad, aun cuando el profesor pida que los alumnos lo hagan como parte de la materia.

No queda muy claro cuánto software de secuestro existe pero existe y se puede acceder fácilmente. Es fácil también que lo escriban aquellos que están interesados en crear software. Cuando los usuarios utilizan DNSSEC, como Wes dijo antes y como vimos en la obrita de teatro, la idea es tener información criptográfica en la estructura normal del DNS porque DNSSEC es una parte del DNS. Está totalmente integrado con el DNS estándar. Cuando el receptor de una respuesta recibe una respuesta firmada por DNSSEC, ya sea que la validación tenga lugar en un resolutor de validación local o en la aplicación propiamente dicha, la idea básica es que el usuario que envió la consulta y que pidió la información pueda tener la garantía criptográfica de que proviene de donde debe prevenir y de que no fue alterada en el camino.

Lo que hace esto en realidad es que ustedes puedan estar seguros de que de hecho las respuestas que ustedes obtuvieron son la información que deberían usar, ya sea que estén haciendo una consulta en la web o ya sea que se trate de un servidor de mail comunicándose con otro o una sesión de Twitter o algo así.

Un ejemplo simplificado de cómo funciona un intercambio de DNS lo vemos aquí. Aquí vemos un usuario que hace una consulta. Joe es el usuario. Joe, el usuario, envía una consulta a su ISP. El servidor de nombres recursivo a su vez envía una consulta al servidor de nombres autorizado. Le dice cómo tiene que llegar. Recibe una respuesta del servidor de nombres autorizado que llega al servidor de nombres recursivo y esa respuesta le llega a Joe, el usuario. Esta es la primera situación que ustedes vieron en la obra.

Una vez que vuelve la respuesta es cuando la información va entre las aplicaciones. El usuario Joe habla con el servidor web y hace su actividad. Cuando tenemos una serie de zonas firmadas por DNSSEC y resolutores validantes, podemos ver a través de los sitios web que se está intercambiando la información adecuada. La mayoría de los sitios web que utilizan DNSSEC no tienen un indicador como este pero esto es algo que hicimos hace varios años para que se pudiera ver fácilmente que se está utilizando una cadena DNSSEC para mandar y recibir información.

Si no ven esta señal DNSSEC, la indicación sería diferente. Parte de la adaptación de un sitio web o de la preparación de un sitio web consistió en insertar un indicador de ataques. Ese ataque es el mismo que realizó el Dr. Mal que presta atención cuando se manda una consulta. El servidor recursivo le pregunta algo al servidor autoritativo pero antes que el resolutor autoritativo reciba la respuesta el Dr. Mal ya responde al usuario Joe. El usuario Joe va al lugar incorrecto. Va al sitio del Dr. Mal. Mientras tanto, las consultas estándar de DNS tienen lugar en la red pero el equipo del usuario Joe ya tiene una respuesta.

Ignora la respuesta correcta y envía la aplicación para que se conecte con el sitio web del Dr. Mal. Nunca recibe la información hasta que DNSSEC empieza a jugar un papel. Cuando el DNSSEC aparece, el usuario Joe rechaza la respuesta incorrecta que vieron en la obrita de teatro y va al sitio correcto.

En este caso, el sitio web tiene información correcta y a pesar de que lo hicimos en el sitio web, lo implementamos de modo que podamos mostrar cuándo se está yendo a un sitio web incorrecto. Esto es lo que obtiene a través de un resolutor de validación. Esto es lo que se hace con DNSSEC con los ISP. Un resolutor no validante, Steve Crocker diría que DNSSEC no resuelve el hambre del mundo. Esa sería la primera frase. Ven que abajo de eso dice que .ORG comparte asesoramiento DNSSEC de Comcast para ISP. Es decir, se insertó información en el sitio web de un modo que el usuario sin ver ese triángulo arriba no sabría que es información errónea, no sabría que el sitio web sufrió un ataque de sustitución de contenido o de secuestro de sitio web.

Quizá digan ustedes: “No hay mucha resolución de DNS, ¿no?” Esta es una imagen de hace 10 años, cuando medimos lo que pasaba con el sitio web de CNN. Esto fue hace cinco años, de una sola página de contenido de cnn.org. Esta es la cantidad de consultas de DNS que pasaron por allí. Hay muchísimas consultas. La información importante acerca del DNS y DNSSEC son los elementos críticos en los datos de la zona. Eso es lo más importante. Aquí es otro ejemplo donde vemos cómo funciona el proceso y dónde deben darse los cambios. Aquí pueden ver a la izquierda la información de zona que se pone en los servidores autoritativos. Allí está disponible en el DNS. Los

servidores recursivos que ven en el medio se comunican con los autoritativos respondiendo a preguntas que reciben de los clientes. El cliente, como pueden ver, la primera flecha, la número 1, número 2, el recursivo le pregunta al autoritativo, número 3, el autoritativo responde al recursivo. Después el recursivo responde al cliente.

Cuando se hace la implementación de DNSSEC, hay algunos pasos que se deben seguir, agregando datos adicionales y funcionalidades adicionales. Si la implementación en su parte del DNS, la parte por la cual son responsables en cuanto a operación o gestión, esto depende de dónde están ustedes en la estructura de DNS. Según el lugar donde están dependerá lo que hagan. Hay unas actividades que tienen mucho que ver con DNS. Quizá deban ustedes hacer todas estas cosas porque algunas empresas ya tienen personal que se ocupa de lo que tenga que ver con DNS. Si el tamaño y la complejidad de sus operaciones son importantes, pueden ver aquí algunos ejemplos de los que pueden realizar esto: los registros, las empresas muy grandes. Las zonas DNS no crítica son fáciles de administrar, son pequeñas, fáciles de manejar. Recuerden que proteger los datos de la zona DNS es lo más importante.

Aquí vemos que la información de zona debe agregarse para que esto sea una función firmada y validada por DNS. Es la información firmada que se ingresa al sistema, la ingresa el propietario del servidor autoritativo y después está disponible para ser incluida en respuestas y después el servidor recursivo de validación que vemos abajo es el que hace la validación y dice: “Sí. Esto es correcto desde el punto de vista criptográfico”.

Si la organización en la que están trabajando o con la que quieren trabajar tiene mucha actividad de DNS, mucha funcionalidad DNS y utiliza mucho el DNS, seguramente podrán hacer DNSSEC internamente. Si la actividad de la organización utiliza muy poco DNS en cuanto a la funcionalidad central, probablemente tenga un departamento de tecnología la empresa o quizá tercericen estas actividades o funciones. Cualquier proveedor, ya sea el departamento interno de tecnología o el proveedor externo, si pueden hacer DNSSEC, les ayudarán. Si no, ustedes tienen que decirles: "Aprenda a hacer DNSSEC. Si no, voy a buscar otro proveedor". Hay muchas personas en el negocio DNSSEC pueden hacer esto. Ustedes podrán contratar a alguien que conozca esto. Podrán contratar otro proveedor que sepa cómo manejarse con DNSSEC.

Este es el fin de la presentación principal. La idea es que esto sea una parte de la sesión muy abierta, con preguntas y respuestas. Ahora le voy a dar la palabra a Wes. Voy a dejar que él sea el que señale a las personas, porque tenemos muchos actores y personas que trabajan con DNSSEC aquí, personas que saben mucho sobre DNSSEC. Por favor, hagan cualquier pregunta que les surja. Estamos plenamente dispuestos a responderlas.

WES HARDAKER: Ahora sí. Ahora tenemos dos micrófonos. Puedo usar los dos. DNSSEC no es simple. Hay mucha complejidad en esto. Les garantizamos que va a haber preguntas aquí. Tenemos mucho tiempo para esta sesión. Hemos dedicado mucho tiempo para responder preguntas. Tenemos

muchos expertos aquí que ayudan a crear DNSSEC. Si tienen una pregunta, se la podemos responder. ¿Alguien tiene alguna pregunta? Levanten la mano si tienen alguna pregunta y les vamos a acercar el micrófono.

THANH NGUYEN: Hola. Soy Thanh Nguyen, de Vietnam. He visto esta representación y vi que hay mucha información y muchas formas de garantizar la seguridad del DNS. He visto mucho material sobre el DNSSEC cuando implementamos el ccTLD pero quisiera ver cómo se implementa esto. Aquí habría que pensar seguramente que hay algunos desafíos como, por ejemplo, hay que conocer bien lo que es DNSSEC, hay que firmar el DNS, hay que firmar la raíz y algún otro paso que me olvidé. En base a estos pasos, creo que algún secuestrador puede utilizar un ataque DDoS aprovechando las debilidades de DNSSEC. Quizá puedan atacar el tema de la sincronización. Por ejemplo, en una diapositiva usted mencionó algunos otros temas adicionales del sistema de DNS. Un secuestrador puede aprovechar esta debilidad que tiene que ver con los tiempos. ¿Tiene alguna solución para este problema que tiene que ver con los tiempos?

WES HARDAKER: Creo que hizo una pregunta que implica varios puntos. En primer lugar, está preguntando si hay una mayor demora para recibir los datos. Como se deben pedir más datos, esto hace más lenta la búsqueda en el DNS. Los usuarios a los que más les importa eso son los que usan aplicaciones instantáneas que tienen que hacer muchas

búsquedas en DNS. En general, se trata de los navegadores. Recuerden que como se utiliza la caché, solo se enlentece una búsqueda. Las demás incluso son más rápidas porque todo, incluso los registros de seguridad, están en la caché. Quizá sea más lenta por unos milisegundos una búsqueda pero después está en la caché. La demora la ve solo un usuario y un ISP una vez.

Creo que también está preguntando acerca de que los registros DNS son muy grandes y que se pueden utilizar en un ataque de amplificación. Si usted hace una pregunta a un servidor DNS y nos da una respuesta muy grande, si falsificamos el lugar de origen, la respuesta puede ir a la persona incorrecta. Hoy en día se utiliza una limitación de frecuencia de respuesta, velocidad de respuesta, limitación de cantidad de solicitudes procesadas por WHOIS. Si hacen algo que no es correcto, se dejan de enviar respuestas. Esa es la solución que se utiliza hoy en día. Yo estoy a cargo de uno de los servidores raíz y el momento en que activamos esto repentinamente recibimos muchos menos pedidos de ese tipo. Eso fue hace muchos años. Es un problema que casi no existe en la actualidad. Creo que hay una pregunta allá.

ANDREW FRASER: Warren, ¿quería agregar algo?

WARREN KUMARI: No.

WES HARDAKER: Todos los expertos que están en la sala pueden acercarse aquí delante.

EBERHARD BLOCHER: Soy Eberhard Blocher, de Alemania. No soy experto. Soy totalmente lego en este tema. Tengo una pregunta. Yendo hacia atrás en la historia, sé que DNSSEC existe hace varios años, hace como 10 años. Me dijeron que Steve Crocker básicamente lo creó o fue parte del grupo que lo creó. Entiendo que ya pasó mucho tiempo y ahora tenemos un nuevo escenario. Este año todos mis clientes finales, yo presto servicios de dominio, todos mis clientes están pidiendo encriptado SSL. Tenemos Let's Encrypt. Esta es otra forma de proteger los sitios web. Tengo entendido que el certificado SSL tiene que estar relacionado con un nombre de dominio únicamente. La pregunta es la siguiente: ¿Seguimos necesitando DNSSEC o cuál es la diferencia entre DNSSEC y un sitio web encriptado con SSL? Si yo encripto mi sitio web utilizando un certificado SSL, ¿por qué sigo necesitando DNSSEC?

Además, tengo una segunda pregunta. He estudiado las estadísticas y sé que muchos registros brindan datos acerca de la cantidad de dominios que utilizan encriptado DNSSEC. Algunos registros tienen una penetración muy baja. ¿Por qué se da esto? Esa es mi pregunta. Después la misma pregunta. ¿Seguimos necesitando DNSSEC?

WES HARDAKER: Uno de los temas más difíciles con respecto a la seguridad de Internet es que no se puede resolver un problema porque de hecho todo funciona por capas. Por ejemplo, si hacemos una búsqueda de DNS,

supongamos que van a un sitio protegido con SSL. Ustedes saben que llegan al sitio web adecuado si es que pueden llegar. El tema es que DNS entra a jugar mucho antes de esto y nos puede redirigir al sitio web incorrecto. Aquí hay una serie de temas. Puede enviarlos al sitio incorrecto y nunca van a llegar al sitio al que querían llegar. Si no protegemos la capa de enrutado en la infraestructura de enrutamiento, tampoco va a funcionar. Internet es una pila con muchas capas. Cada capa debe estar protegida. DNS entonces sigue siendo necesario. ¿Quiere usted hablar sobre la historia y Steve Crocker? Hay muchas personas que trabajaron en DNSSEC. Steve Crocker sí contribuyó mucho a esto.

RUSS MUNDY: DNSSEC tiene una historia muy larga. Se tardó mucho en diseñarlo e implementarlo. Como dije Wes, tiene por objetivo asegurarnos de que el uso de DNS reciba la respuesta correcta y la mande al usuario. ¿Qué aplicación lo utiliza? Eso es bastante independiente. De hecho, en 1993 se empezó a trabajar fundamentalmente en el desarrollo de DNSSEC y en el diseño y su implementación. Hubo muchas llamadas, muchas consultas. Steve Crocker fue una de las personas que participó en esto. Yo también trabajé en esto. Hubo muchos rediseños porque es la primera vez que se trabajó para insertar una funcionalidad de seguridad en un protocolo que ya estaba funcionando. Había dos diseños que presentaban problemas. En el tercer caso se hizo bien. En el año 2010 se firmó la zona raíz. Antes ya se habían firmado algunos TLD. Sí, hay muchas personas que hicieron aportes importantes, muchas organizaciones también que trabajaron mucho en esto. Como

hemos dicho, esto tiene por objetivo impedir que pase lo que vemos en esta diapositiva porque ya sea que estemos utilizando un certificado de SSL o no, hubo muchos problemas y desafíos con las autoridades de certificación. A veces se emiten certificados incorrectos o erróneos y a veces pasa lo que vemos en la diapositiva y tenemos un problema. El usuario recibe igual un sitio web firmado por SSL que no es el correcto.

WES HARDAKER: Quiero decirles que la web no es lo único que hay que proteger en el caso de búsqueda. El correo electrónico también es un ejemplo de algo que no se puede resolver con los sistemas tradicionales de certificado. El miércoles voy a hablar de esto en el taller de DNSSEC y todos pueden participar de ese taller. Es un taller de todo el día sobre DNSSEC. Yo voy a hablar sobre cómo DNSSEC es la única solución disponible para proteger los servidores web, para evitar que se roben los correos electrónicos y se lleven al lugar inadecuado. Los certificados tradicionales no nos pueden ayudar allí. Se lo voy a explicar bien el miércoles porque es un tema complejo. Andrew.

AHMAD ALSADEH: Soy Ahmad Alsadeh. Soy becario. ¿Por qué no está implementado en todos lados DNSSEC como pasa con DNS? ¿Por qué no todo el mundo utiliza DNSSEC? Esa es la pregunta uno. La pregunta dos sería: ¿Creen ustedes que las nuevas tecnologías como blockchain podrían ser una posible solución para brindar seguridad al DNS?

WES HARDAKER: Son dos preguntas. La otra persona preguntó por qué algunos registros tenían mayores implementaciones y otros no. Todas las regiones del mundo tienen diferentes tasas de implementación desplegadas. Algunos TLD, especialmente Suecia, República Checa y algunos otros, de hecho ofrecían incentivos financieros para que se firmara la zona. También hay otros incentivos por los cuales se trata de impulsar a las empresas para que utilicen esta tecnología. La tasa de adopción en general ha sido bastante baja pero en este momento, si vienen el miércoles les voy a dar las estadísticas correctas, hay millones de zonas firmadas. Aunque el porcentaje es bajo porque hay tantos dominios en el mundo, ya tenemos millones de implementaciones. Tenemos un 85% de los TLD que ya firmaron. Estamos llegando al final pero es un proceso muy largo este de lograr que todo el mundo pase a utilizarlo.

RUSS MUNDY: Además, si puedo agregar algo, quisiera decir que no son solamente los TLD y los dominios de segundo nivel. Los usuarios finales, las empresas tradicionalmente no han demandado en forma activa DNSSEC porque la mayoría de las veces no se dan cuenta de la importancia de esto. En los últimos cinco años, el gobierno de los Estados Unidos junto con lo que hicieron en cuanto a crear el requerimiento de que se firmaran todos los dominios .GOV, otros gobiernos después siguieron estos mismos pasos. Hablo de los Estados Unidos porque es el caso que más conozco. Muchos gobiernos

piden que se validen todos los dominios del gobierno, de la administración pública. Esto está obligando a las empresas y a algunas organizaciones a hacer lo mismo. Por ejemplo, la empresa para la cual yo trabajo, Parsons, parsons.com es un dominio firmado y se opera de esa manera. Se trata de seguir educando y capacitando, incentivando a los usuarios a que pidan esto. Por eso verán en varios lugares que les decimos: "Pidan al proveedor o al ISP, a quien sea que les ofrezca el servicio DNS, que les ofrezca las funcionalidades de DNSSEC".

WES HARDAKER: Muchos registros y registradores ya ofrecen esto. Si ustedes trabajan con estos registradores, simplemente tienen que presionar la tecla y ya van a tener el DNSSEC implementado. Los que manejan sus propios sistemas y servicios, no lo van a tener porque no lo pueden hacer en forma personal pero hay muchas herramientas sin embargo que facilitan esto. Hace 10 años no era así. Era mucho más difícil. ¿Hay alguna otra pregunta?

ORADOR DESCONOCIDO: Hola. Mi pregunta es acerca del comentario sobre el último traspaso de la llave. La otra pregunta es si hay planes de agregar algo al navegador para que pueda detectar esta firma.

WES HARDAKER: El traspaso de la KSK tuvo lugar la semana pasada. Fue la primera vez. Funcionó muy bien. John, ¿quisiera hablar sobre eso? El traspaso de la KSK funcionó muy bien. Hubo algunos ISP que no cambiaron esa clave

pero son los ISP como vieron antes. El usuario con el navegador web no tenía que hacer mucho. Ni siquiera hacía falta que supiera que estaba teniendo lugar el DNSSEC. Está todo el tema de lo que pasa si uno está en un barco usando wifi. En general, el ISP solo tiene que saber lo que pasa con las nuevas clave.

En cuanto al proceso futuro de la ICANN, cuándo se va a hacer otro traspaso, esto es algo que se va a debatir a lo largo de esta semana y a lo largo del año próximo probablemente se decidirá con qué frecuencia se va a hacer este traspaso. ¿Cuál es el mecanismo para hacer el traspaso de la llave de la KSK? Esto se basará en las lecciones aprendidas.

RUSS MUNDY: La comunidad sin duda realizará un aporte en cuanto a decidir cuándo tendrá lugar el próximo traspaso de la KSK. Esto es algo en lo que la organización, la ICANN o el director de Tecnología de la ICANN está muy interesado. El director de Tecnología quiere recibir aportes, contribuciones, ideas. Sin duda quiere escuchar esas ideas. Hay múltiples mecanismos para buscar estos aportes pero piénsenlo y hagan sus contribuciones.

WES HARDAKER: Habrá una presentación sobre el traspaso de la clave para la firma de la llave el miércoles.

JOHN LEVINE: Soy John Levine y quiero hacer la misma pregunta que hago siempre y que es la siguiente. Yo tengo DNS para 300 zonas, para mis usuarios. En la mitad de las zonas yo soy el revendedor o distribuir de registradores. Tengo acceso al registrador y tengo que asegurarme de que las firmas funcionen. Para la otra mitad yo soy un tercero proveedor de DNS. Para todos estos usuarios, la única persona que puede hacer que DNSSEC funcione es el registratario, la persona con las credenciales de registratario. Tengo que llevar a mis usuarios y hacerlos pasar por el proceso de instalar un registro de DNS, lo cual es fácil para ustedes pero no necesariamente para el resto de las personas o necesito las credenciales, que es algo que no quiero. Eso es algo que puede resolverse a nivel de registrador, agregando alguna forma de que se pueda actualizar el contacto del DNS o algo que pueda hacer el IETF. Creo que en ninguno de los dos casos se está avanzando mucho. Yo sé que no soy el caso más común pero creo que los proveedores independientes de DNS no son conscientes de esto y es algo que tenemos que resolver.

WES HARDAKER: Es cierto que hay que resolver esto. Yo hice todo mi trabajo manualmente porque también tenía algunos. Eso ha mejorado. Hay algunas cosas que le puedo decir y que surgieron en los últimos dos años. Por un lado, algunos proveedores que están creando una tecla para que si usted publica su registro DS pueda hacer clic en la tecla que diga: “Este es el correcto” y ya no va a tener que hacer todo. El sistema lo hace directamente. Por otra parte, tendría que hablar con [Oliver] en algún momento. Ellos crearon el registro CDS que es una

forma de actualizar automáticamente las claves en el DNS entre la zona raíz y el registrador.

JOHN LEVINE: Esto solo lo actualiza.

WES HARDAKER: Se está hablando de hacer el salto de la verificación de fe. De hecho, el mes pasado se estuvo hablando de esto. La gente ahora está hablando acerca de pasar eso a producción. Estamos viendo tráfico. Estamos escuchando hablar de quién lo implementa y recientemente se ha estado hablando mucho de esto.

ORADOR DESCONOCIDO: Quería comentar que hay dos o tres países hoy en día que están trabajando con estos registros. Suiza, Liechtenstein, estos países tienen el dominio y muestran el CDS en la zona. Esto lo toma el registro y hay otros donde esto está comenzando y esto será una iniciativa global que está comenzando y podemos aprender de esto. Tenemos una presentación sobre este tema esta semana. Los invisto a participar y escuchar la presentación.

WES HARDAKER: Hay trabajo por hacer pero la buena noticia es que creo que hay bastante impulso para hacerlo en este momento. Hay un panel el miércoles sobre este tema.

RUDOLPH DANIEL: Hola. Soy Rudolph Daniel. Buen día. Soy becario de la ICANN. No sé si corresponde pero el traspaso de la KSK se acaba de mencionar. Yo quisiera saber lo siguiente. Ha tenido éxito hasta el momento. ¿Se han borrado todas las claves antiguas?

WES HARDAKER: Dos cosas. Ha tenido éxito hasta el momento. Los TTL en los datos, el tiempo con el que contamos eran dos días. Ya pasaron 10 días, creo. Sí, 10 días. Ya pasaron 10 días desde el traspaso de la KSK, lo cual significa que ningún resolutor de DNS en el planeta debería haber tardado tanto tiempo. Ya tienen que haber actualizado la información y ya tienen que haber observado una falla, al menos que algo esté muy mal. Ya pasamos el punto. Si había una falla, seguramente ya se detectó. En cuanto a eliminar la clave anterior, hay dos aspectos. Por un lado, todavía tenemos la clave en la zona raíz pero no se la está utilizando. Está allí todavía pero no se está utilizando.

El 11 de enero habrá un cambio, una advertencia que dirá, ahora es momento de dejar de confiar. Va a ser la revocación de confianza. Eso se va a publicar durante tres meses más y después el 11 de abril directamente se eliminará de la zona raíz. El proceso de traspaso continúa. Por el momento no pensamos que vamos a volver a utilizar la clave anterior porque parecería que el traspaso ha tenido éxito. Es una muy buena pregunta. Gracias.

ORADOR DESCONOCIDO: ¿Hay algún plan para notificar a los usuarios de los navegadores acerca de este certificado, si estamos utilizando un sitio que utiliza DNSSEC? Por otra parte, quisiera proponerles a mis clientes que utilicen .COM y no un TLD genérico porque no están firmando los certificados. Es una cuestión de promoción de marketing también. Esto va a hacer que algunos implementen DNSSEC más rápidamente. Mi pregunta es la siguiente. ¿Hay algún plan para mostrar que alguien está implementando el sitio correcto? para que el usuario pueda decir: "Yo veo la firma". En la diapositiva vi una notificación en el navegador y también vi una imagen del navegador, una extensión web integrada. Algo así.

WES HARDAKER: ¿Quiere responder usted? No. De acuerdo. Hay una extensión del navegador que pueden instalar que se llama DNSSEC. No me acuerdo del nombre. Si buscan la extensión del navegador de Firefox y de Chrome van a ver que hay una extensión. Los proveedores de navegadores no están muy interesados en hacer DNSSEC directamente en el navegador por su cuenta. Hay una larga historia. Pueden contactarse con ellos y quejarse. El validador de DNSSEC, pueden buscarlo e instalarlo. Russ y yo hace muchos años trabajamos en un navegador que hacía DNSSEC en la biblioteca básica. Se llamaba Bloodhound. Creo que no fue actualizado. Por tanto, no tiene la nueva clave.

RUSS MUNDY: Sí. Tenemos que investigarlo.

WES HARDAKER: Esto estaba modificando Firefox en particular para que haga DNSSEC directamente en el fondo del navegador. Hay más uso en aplicaciones de email y otras cosas. El miércoles voy a hablar sobre este tema y van a ver un gráfico con las tendencias y van a ver que el email cada vez lo utiliza más.

BARRY LEIBA: Al hablar a los usuarios sobre esto tenemos que decir que hay muchas evidencias de que no se entiende lo que se está haciendo. A veces les decimos a los usuarios cosas sobre DNSSEC y no tienen idea de qué se trata.

WES HARDAKER: En otras palabras, la gente ahora está pensando en hacerlo diciendo: "Usted va a tener un mensaje de error". Si obtiene un mensaje de error, no continúe. Hay muchas evidencias que indican en términos generales que los usuarios finales no tienen el conocimiento suficiente como para tomar decisiones de seguridad. No tenemos que permitir que tomen decisiones de seguridad. Hay que denegar ese acceso. Hay una pregunta al fondo.

ORADOR DESCONOCIDO: Quiero hacer un comentario. Eso no significa que no debamos decirles a los usuarios finales lo que está pasando, explicarles por qué aparece ese mensaje. Podríamos poner un banner, un mensaje aclaratorio,

porque si ocurre la primera vez, es algo nuevo, uno no sabe qué es. Si el mensaje es claro, entonces podría ser una buena forma de que la próxima vez que aparezca, el usuario lo entienda.

WES HARDAKER: Sí. Este es un debate de seguridad genérico muy largo. Dejar que los usuarios lo hagan o no. Yo personalmente, que soy un especialista técnico, siempre prefiero que me den la opción de tener el mayor detalle posible pero yo tengo parientes que no entienden este tema y me llaman a mí para que se lo explique. ¿Alguien más tiene alguna pregunta?

ORADOR DESCONOCIDO: ¿Qué pasa cuando hay problemas en el host local? A veces tenemos una notificación en el navegador y no sabemos qué pasa, no sabemos cuáles son los beneficios de la firma. Es muy importante explicárselo al usuario y ver qué pasa con los problemas de seguridad.

WES HARDAKER: Hoy estamos hablando solamente de nombres. Si el proxy está utilizando también el resolutor del ISP, entonces es otra cosa. Pero es cierto que hay múltiples capas y múltiples memorias caché, en mail, en los navegadores y las búsquedas de DNS hay que validarlas para que funcione toda la cadena de seguridad. ¿Hay una pregunta allí al fondo? Siempre es alguien que está detrás de usted.

JOSE ALBERTO: Hola. Soy Jose Alberto. Soy un becario, miembro del programa de becarios de la ICANN. Mi pregunta está relacionada con Tor. Cuando usamos Tor, por ejemplo, la seguridad de DNS aplicada a Tor, ¿es posible esto o utilizan otro tipo de seguridad en el DNS?

WES HARDAKER: Es una buena pregunta. Me recuerda que no respondí antes la pregunta de blockchain. Hay sistemas de nombres alternativos en Internet. El más conocido es Tor. Hay otro que se llama Namecoin, basado en blockchain. No son compatibles con el DNS. DNSSEC protege solamente a la resolución de nombres comunes. No evita que estos otros mecanismos sean utilizados. Tampoco evita que tengan su propio sistema de seguridad pero creo que DNSSEC no se aplica a Tor. Quizá en teoría podría porque actúa como el DNS pero yo no soy un experto en Tor, lamentablemente. No sé si alguien puede responder esta pregunta. No. Yo supongo que probablemente la respuesta a esa pregunta sea no pero tendría que preguntar a alguien que tenga un poco más de información sobre esto. Lamentablemente no hay expertos en Tor aquí. No va a funcionar. Aquí tenemos una respuesta. No, no funciona.

FAN CHIEH LIN: Hola. Soy Fan-Chieh Lin. Soy Jason, de nuevo. DNS está diseñado para proteger las transacciones de DNS. Yo leí un artículo que sostenía que las cookies de DNS son introducidas por [RFC, MTA, MT3]. ¿Hay un método más liviano para hacerlo? ¿Podría hablar sobre esto? Espero no estar desviándome del tema.

WES HARDAKER: No, no hay ningún problema. Las cookies de DNS resuelven un problema totalmente diferente. Voy a corregir lo primero que usted dijo, que tenía un pequeño error. Usted dijo que protege las transacciones. DNSSEC no protege las transacciones, protege los datos. Le voy a dar un ejemplo. Si yo necesito enviar información de DNS a Russ digo: "Olvídense de lo que pasa fuera de DNS. Mi número host es 1.1.1.1 y esta es mi firma". Él se la puede dar a todos ustedes y pueden hacer toda la verificación. Son los datos. No me importa cómo se transporta. Puede ser a través de DNS, a través de una paloma mensajera, no importa, eso no importa. Lo que se protege son los datos, no la transacción. Esto es importante debido al caché porque debido al DNS se pueden dar varios saltos. Se utiliza Google, el resolutor de Google 8.8.8.8. Ellos tienen muchos hosts que conforman ese sistema con un caché compartido. No importa quién lo pregunte o quién lo responda siempre y cuando se pueda verificar los datos en última instancia no importa cómo se tiene. El mecanismo de cookies fue diseñado para proteger una única transacción de cosas que a veces son demasiado grandes para poder obtener respuestas más grandes del servidor a fin de evitar cosas como la denegación de servicio, para no recibir un TCP o algo así. No protege los datos que están dentro de la transacción del DNS.

ORADOR DESCONOCIDO: Según yo entiendo, con respecto a los datos del DNS tenemos dos clases de mecanismos. En primer lugar tenemos DNSSEC y en segundo

lugar tenemos DNS sobre TLS. DNSSEC es muy popular. Más popular que DNS sobre TLS. ¿Podría hacer una comparación entre las dos clases de mecanismos? ¿Cuáles son las características de DNSSEC en comparación con el otro sistema?

WES HARDAKER: También tienen dos objetivos diferentes. DNSSEC, una vez más, protege los datos. No importa si es TLS o no. No importa cómo lo obtuvieron. DNSSEC sobre TLS apunta a proteger la transacción entre una persona que hace la pregunta y el lugar de donde obtienen la respuesta. Lo que no sabemos es si su navegador le pide al resolutor que llegue al ISP, establece la conexión para asegurarse de que nadie más que está ahí en el bar pueda ver la respuesta. El resolutor puede preguntar a la raíz, a .COM o a bigbank.com a través de TLS. DNSSEC protege la integridad, ya sea que usted tenga la respuesta correcta o no. DNS sobre TLS apunta a proteger la privacidad para asegurarse de que nadie vea lo que usted está pidiendo y cuál es la respuesta que obtiene. Quizá algún día el TLS se utilice en todas partes pero a pesar de que hay múltiples saltos no vamos a saber si como llegamos del punto A al B al C al De fue de una forma segura. DNSSEC nos da la seguridad independientemente de cuántos pasos se den, sabemos que lo que vamos a obtener es correcto.

KEN HERMAN: Buenas tardes. Ken Herman, consultor independiente. Estoy convencido del valor de DNSSEC. Usted habló acerca del nivel de penetración, cuántas personas lo utilizan, cómo las organizaciones o

las personas incluso pueden saber que se estableció esta cadena de confianza mediante DNSSEC. En tercer lugar, ¿podrían hablar acerca del costo de la implementación para las organizaciones? Quizá no sea mucho para una pequeña empresa, depende de cuántos ISP tengan. Quizá para las grandes empresas sí sea mucho.

WES HARDAKER: Venga al taller del DNSSEC. La primera presentación de todos los talleres sobre DNSSEC que tendrá lugar el miércoles esta vez es una serie de mapas y una serie de datos acerca de dónde está la penetración, cuáles son las partes del mundo que más lo están usando y ese tipo de cosas, incluyendo la presentación sobre dominios y sobre la implementación de DANE. Creo que se me está quedando sin batería.

¿Cuál fue la segunda mitad de la pregunta? El costo. Antes era más difícil. Si ustedes quieren activar la validación de DNSSEC, probablemente las empresas no lo hagan hasta que la gente lo pida y lo van a hacer cuando la gente lo pida. Es una cuestión de que hoy en día se necesita muy poca configuración para hacerla por lo tanto no tienen muchas excusas para no hacerlo. Solo necesitan saber cómo quitar los bugs cuando hay una falla, qué hacer cuando hay un traspaso. La mayor parte de las cosas hoy están automatizadas. Antes había que saber mucho más. Hoy en día es muy obvio. Antes había que asignar las zonas. Si uno lo iba a hacer por su cuenta tenía que hacer el host en el DNS, hacer la firma por su cuenta. Hacían falta como 12

comandos. Lo documentamos en una guía de implementación inicial. Era muy tedioso. Llevaba mucho tiempo.

Russ y yo trabajamos juntos. Un colega nuestro desarrolló una herramienta que permite hacerlo de una sola forma y publicar el resultado. Las herramientas han mejorado mucho. El costo es menor pero no existe una seguridad a costo cero. Lo que también tienen que saber con respecto a DNSSEC es que si lo van a hacer ustedes, antes DNS era algo que uno publicaba y se olvidaba, no había que modificar la zona. Uno publicaba una vez y lo dejaba durante tres años y los datos seguían estando bien. Con DNSSEC, debido a que tiene una limitación de tiempo, hay que volver a firmar una vez por mes o depende de los parámetros que uno elija. Un mes es lo más común. Yo en mis zonas firmo cada dos semanas.

ORADOR DESCONOCIDO: ¿Puedo hacer un comentario respecto de lo que usted dijo? Por ejemplo, en el caso de los resolutores que hacen la firma de última instancia, si hay un sistema para publicar los registros CDS es como se hacía antes. Se publicaba una vez y listo. Todos los mecanismos automatizados se ocupaban de la seguridad. Entonces el costo era mínimo.

WES HARDAKER: Menciona algo muy importante. Si ustedes le dicen al resolutor, la mayoría de los resolutores autoritativos tienen una firma automática, la van a seguir firmando una y otra vez. Hay algunas herramientas que

automatizan todo. Yo soy paranoico con respecto a esto así que sigo haciéndolo en forma manual. Todas han sido preguntas maravillosas hasta ahora. Muchas gracias. ¿Hay alguna otra pregunta?

THANH NGUYEN: Yo tengo otra pregunta. No es una pregunta técnica. Para los países, por ejemplo, en el caso de Vietnam, para el sistema del gobierno, para el DNS en mi gobierno el sistema DNS no es seguro y queremos cambiar todos los sistemas DNS y pasarlos a DNSSEC. ¿Cuál sería el costo de pasar DNS a DNSSEC y cuánto tiempo nos llevaría? ¿Podría darme un estimado de plazos y costos?

WES HARDAKER: Es difícil dar un estimado de esto. No estoy seguro de que pueda hacerlo.

RUSS MUNDY: Voy a hacer unos comentarios sobre esto. No le voy a dar una respuesta específica pero puedo darle una idea. Uno de los puntos que se identificaron por las personas que empezaron a hacer DNSSEC y a utilizarlo, muchas veces vieron que el software de DNS no había sido actualizado correctamente. Quizá hayan estado utilizando los servidores autoritativos o si también están operando los ISP y usando los servidores recursivos, quizá estarían utilizando software desactualizado por 3, 5, 10 años. En el primer caso, lo que tenían que hacer es analizar la infraestructura de DNS que tiene. Si está actualizada y el software es el actual, como dijimos antes, la dificultad

o los desafíos relacionados con el paso a DNSSEC a veces pueden ser muy simples. Se trataría de cambiar solamente una o dos configuraciones en el archivo de configuración que es el que hace la distribución hacia los servidores autoritativos. Quizá también pueda hacer algo más complejo si queremos establecer o configurar un mecanismo criptográfico offline independiente. Esto varía pero lo más importante es analizar la infraestructura que tienen hoy en día para DNS. A partir de allí, hay mucha información disponible en línea y la comunidad de DNSSEC ha compartido muchísima información, ha trabajado muy bien y hay muchísima información disponible online que explica lo que se hizo en diversos países.

WES HARDAKER: El sitio web que vimos antes, que es DNSSEC-Deployment, que tenía la foto de Steve Crocker, es un buen lugar para empezar a buscar recursos DNSSEC que les puedan ayudar a avanzar por este recorrido. Es un sitio web muy bueno que tiene mucha información. Yo tengo un sitio web que se llama DNSSEC-Tools, que está más orientado a los técnicos. Pueden hablar también con los registradores. Muchos de ellos ya tienen herramientas. Si ellos le dan el hosting de sus datos, ellos pueden ayudarles con el DNSSEC. El costo depende de lo que quieran hacer. Tienen que hacer primero esa evaluación que mencionó Russ. Deben empezar viendo lo que tienen en la actualidad y después, a partir de allí, definir el costo del cambio.

RUDOLPH DANIEL: Soy Rudy, una vez más, becario de la ICANN. Estoy recordando que vi algo llamado EDNSSEC. ¿Hay algo así?

WES HARDAKER: Creo que está confundiendo dos cosas. EDNS, sin el SEC, es una extensión en el mecanismo de DNS para agregar información adicional cuando se está pidiendo información. De hecho, ahí es donde decimos: "Yo utilizo DNSSEC. Denme todas las firmas, etc." Es un mecanismo de extensiones dentro de DNS. DNSSEC cumple con esto o es compatible con esto.

WES HARDAKER: ¿Hay alguna otra pregunta? ¿Últimas preguntas?

BARRY LEIBA: Quisiera reformular mi pregunta anterior con respecto a DNSSEC y HTTPS. Inicialmente, uno no visitaba los sitios web que tenían HTTPS. Íbamos a HTTP y nos redireccionaba. Un atacante podría llevarnos a otro lugar para que no llegáramos a HTTPS. Hacía falta una verificación allí. Después desarrollamos algo que se llama seguridad de transporte. El sitio web: "Utilice HTTPS y solo utilice HTTPS y nunca acepte una conexión que no lo lleve a ese lugar". Aquí hablamos de la confianza, suponiendo que los atacantes interceptan el primer pedido. Para resolver esto, ahora se está utilizando una lista de transporte de seguridad en los navegadores, para que no haya confiar en el primer uso, para que nunca lleguemos a ese sitio web. Allí tenemos lo que mencionó Russ. Si vemos un certificado, podemos ver en cuántos

certificados de raíz confía el navegador. Si alguno de ellos está comprometido o atacado, por ejemplo el de Bigbank sabemos que está comprometido. Después tenemos DANE donde el banco publica sus propios registros en el DNS para decir: "Estos son los certificados que yo quiero que usted utilice". Eso resuelve este problema pero piensen qué exige DANE. Exige DNSSEC porque los certificados vienen de DNS. Sí, es cíclico. Tiene que ver con lo que dijo Wes acerca de que todo está en capas. Hay que proteger todos los elementos.

WES HARDAKER: En realidad, si el usuario lo primero que pone en un campo es el nombre, ese nombre es buscado y esa es la primera vulnerabilidad. Hay otras formas de resolver todos esos problemas. En todos los casos hay problemas pero si tenemos seguridad en el nombre de dominio, los problemas empiezan a desaparecer. Esto no significa que no haya que realizar HTTPS porque eso resuelve un problema diferente. ¿Hay alguna otra pregunta?

AHMAD ALSADEH: Soy Ahmad Alsadeh nuevamente, becario de ICANN. Cuando vi ese diagrama todos en la cadena deben tener un certificado o deben firmar. Si un certificado no está o algo no está implementado, DNSSEC va a fallar. ¿Contesté bien?

WES HARDAKER: Casi. No es que ha fallado pero usted sabe con seguridad que no está entrando en un sitio que esté firmado con DNSSEC. Tiene que seguir

avanzando pero allí perdió la confianza. Hay partes de la estructura DNS que no están firmadas y el servidor web va a seguir funcionando porque DNSSEC le da una respuesta y dice: “Mire, tiene que ir a bigbank.com pero ellos no tienen DNSSEC. No tiene opción. Deberá seguir utilizando el DNS común”. Hay un mecanismo donde los resolutores van bajando por la cadena, llegan a un punto, dicen: “Bueno, no puedo dar seguridad después de esto pero quizá esta sea la respuesta igual”. Aquí estamos hoy en día. Hay muchos que están firmados, muchos que no están firmados. Los usuarios no conocen esto demasiado. Tenemos tiempo para una pregunta más. Si alguien quiere hacer una última pregunta.

ORADOR DESCONOCIDO: La pregunta es si recibimos mensajes de error en ese caso.

WES HARDAKER: Sí. No recibimos mensajes de error cuando pasamos a la parte no segura porque el resolutor sigue dándonos una respuesta pero el resolutor le dice a la aplicación si la respuesta es segura o no. En este momento, los navegadores y otras aplicaciones no consideran esa información porque no se sabe si es correcto o adecuado presentarlo al usuario o no. No se sabe tampoco si es útil para los usuarios finales pero sí si el DNSSEC falla en algún punto. Si el Dr. Mal se interpone, vamos a recibir un mensaje de sitio web caído. El mensaje será: “No pudimos encontrar ese nombre” porque el resolutor trató de encontrar el nombre y si no recibió una buena respuesta porque las respuestas que recibió son incorrectas una y otra vez, si entran a un

nombre caído, el servidor les va a decir: “No encuentro el nombre de ese servidor”. No van a saber que DNSSEC los está protegiendo. Solamente van a ver que no pueden llegar a esa página web. Con esto terminamos. ¿Quiere usted agregar algo sobre el miércoles?

RUSS MUNDY: Ya promocionamos esta actividad varias veces en forma no intencional, pero esta es una buena publicidad para el miércoles. Tenemos varios paneles. Uno tendrá que ver con DANE. Tenemos una parte introductoria que se refiere a los mapas que se crean, que muestran la cantidad y el tipo de despliegue de DNSSEC en diferentes partes del mundo. Invito a todos a que vengan el miércoles a estas sesiones. Empiezan a las 9:00 hasta las 14:30. ¿Es correcto esto, Kathy?

KATHY SCHNITT: Hasta las 3:00.

RUSS MUNDY: Hasta las 3:00 de la tarde. Por favor, piensen en esto y muchas gracias a todos por venir. Espero que hayamos respondido sus preguntas. Si quieren acercarse a cualquiera de nosotros los que estamos aquí o a los actores con preguntas sobre DNSSEC, con mucho gusto se las vamos a responder. También podremos hablar en forma personalizada en los pasillos.

WES HARDAKER: Mañana en el TechDay también se hablará mucho de DNSSEC y temas relacionados con DNSSEC. No me acuerdo de cuál es la agenda pero en general las presentaciones tienen que ver con TLD que están implementando DNSSEC.

RUSS MUNDY: Esto empieza después de la ceremonia de apertura.

WES HARDAKER: Gracias por venir. Espero que hayan obtenido información interesante y útil.

[FIN DE LA TRANSCRIPCIÓN]