JOHANNESBURGO – Sesión del GAC sobre el traspaso de la KSK
Jueves, 29 de junio de 2017 – 12:00 a 12:30 JNB
ICANN59 | Johannesburgo, Sudáfrica

DAVID CONRAD: Es la manera en que el DNSSEC se implementa. En el 2010, cuando firmamos la raíz por primera vez, le dijimos a la comunidad que después de cinco años íbamos a cambiar la clave. Esto es lo que se conoce como traspaso de la clave, traspasar la clave. Estamos en el 2017 y estamos en el proceso precisamente de hacer este traspaso, este cambio. En cuanto Adobe decida cooperar, tengo algunas diapositivas que mostrarles.

Mi presentación está diseñada para ser de un nivel muy general, para dar una herramienta o para comprender. Enviamos una carta a las entidades reguladores en 180 países y a otros representantes del GAC. En esa carta la intención era comunicar que se acercaba el traspaso de la clave para que se averiguara entre los operadores si estaban preparados para el cambio. Una reseña entonces.

La clave para la firma de la llave de DNSSEC en la zona raíz es la clave criptográfica más superior que asegura los datos en el DNS. Comprende una parte pública y una parte privada. La parte privada se mantiene en lo que se llaman las instalaciones de

Nota: El contenido de este documento es producto resultante de la transcripción de un archivo de audio a un archivo de texto. Si bien la transcripción es fiel al audio en su mayor proporción, en algunos casos puede hallarse incompleta o inexacta por falta de fidelidad del audio, como también puede haber sido corregida gramaticalmente para mejorar la calidad y comprensión del texto. Esta transcripción es proporcionada como material adicional al archive, pero no debe ser considerada como registro autoritativo.

gestión de la clave. Una está en la costa oeste de los Estados Unidos y la otra en la costa este, que se establecieron en 2009 cuando teníamos el contrato con el departamento de comercio estadounidense. En estas instalaciones hay un nivel de seguridad bastante alto. Hay una sala segura donde hay una jaula que tiene una caja de seguridad que tiene, a su vez, lo que se llama módulos de seguridad de hardware que son dispositivos especializados que contienen la información criptográfica. La clave privada para la zona raíz se mantiene dentro de estos módulos de hardware. Está dentro de la sala segura, dentro de instalaciones de co-localización que permiten el control.

La parte pública de este par público-privado está copiada en todos los resolutores de DNS que hacen validación de DNSSEC en el mundo. Estimamos que hay aproximadamente unos 100 millones de resolutores en el mundo y solo un porcentaje menor hace validación DNSSEC. No obstante, aun así, son millones de resolutores que tienen esta información de configuración.

La clave se usa en DNSSEC para crear la cadena de confianza desde la raíz del DNS hasta el extremo, la última hoja del árbol en la búsqueda y esto garantiza que los datos que han sido firmados en DNSSEC por el dueño de la zona no puedan ser modificados en el traslado, que en la trayectoria no sea sujeto de phishing o ataques intermedios y ese tipo de cosas.

Mientras hacemos el traspaso de la clave una práctica de seguridad común es que si se tiene una contraseña, hay que cambiarla cada tanto para impedir situaciones de que la clave sea comprometida sin conocimiento. Para garantizar que la infraestructura necesaria para cambiar la contraseña funcione en caso de que se vea uno forzado a cambiar la contraseña por cualquier razón, esto suceda. Lo mismo pasa con DNSSEC. Podemos pensar que la KSK es como una contraseña del DNSSEC. Como resultado, tenemos que asegurarnos de que la infraestructura que se usa para cambiar la clave funcione bien si en algún momento nos vemos forzados a cambiar la clave.

Puede ser que haya una violación de la tecnología que permita la factorización de la información criptográfica o alguna indicación de que la clave se ha visto comprometida de uno u otro modo. El problema es que dado el número de dispositivos existentes por ahí que tenemos que actualizar, lo tenemos que hacer con sumo cuidado, muy lentamente y además preferiríamos no parar la Internet mientras lo hacemos.

El tema es que si cometemos algún error durante el traspaso, los resolutores, esas máquinas, los servidores en los que los usuarios finales consultan cualquier búsqueda en Internet, de manera espontánea van a dejar de funcionar en cualquier zona firmada. Como es la zona raíz la que está firmada, va a ser un día muy malo para todos en la Internet. Preferimos no hacer tal

cosa. Por eso estamos abordando con mucho cuidado, de una manera deliberadamente cuidadosa todas las pruebas para que no haya riesgos significativos que generen problemas en la validación DNSSEC en Internet. Es un proceso de más o menos dos años y medio. La siguiente.

Aquí está. Estas son algunas de las fechas significativas del proceso del traspaso. El 19 de septiembre, el tamaño de la clave se incrementó porque tuvimos que insertar la nueva clave en el DNS para que se usar después en lo que se llaman las ceremonias de la clave, que es cuando se lleva la clave privada a la sala segura y se firma la clave de la zona de VeriSign, para que VeriSign pueda firmar la zona raíz. Lo hacemos cada trimestre. Esto significa que para todas estas actividades hay un reloj. En la última ceremonia fue el 19 de septiembre de 2017 se aumentará el tamaño de la clave porque agregaremos una nueva clave. El 11 de octubre de este año vamos a usar esa clave por primera vez.

Es, de algún modo, la fecha más probable en que algo raro podría ocurrir. Raro podría ser que aquellos que no cambiaron la clave antes del 11 de octubre, los resolutores, no van a poder validar. Cualquier nombre de dominio que se busque va a dar como resultado “Host not found”, “No se encuentra el host” o algo similar. El 11 de enero le vamos a poner un bit nuevo a la clave anterior para que deje de funcionar. El 22 de marzo la sacaremos de la zona raíz. En agosto vamos a destruir la clave

antigua para estar absolutamente seguros de que todo es seguro.

¿Quién va a recibir el impacto de esto? Los distribuidores y desarrolladores de software de DNS deben tener la clave implementada en su software. Los integradores de sistemas que son las personas que implementan los programas, los software, deben asegurarse de tener la última versión de la clave. Los operadores de red son las personas que administran los resolutores y tienen que asegurarse de que sus sistemas puedan soportar este cambio de clave. Los operadores de servidores raíz que trabajan de cerca con los anteriores, porque probablemente experimenten problemas si la gente no cambia la clave. Lo que generalmente sucede es que el resolutor va a tratar en varias oportunidades de resolver algo y la validación de la DNSSEC va a fallar.

Los proveedores de servicio de Internet que son quienes van a recibir las llamadas telefónicas si hay algún problema. Si los operadores de red no actualizan la clave, los ISP van a ser quienes van a recibir las primeras llamadas y los usuarios finales también van a recibir un impacto si el operador de red no actualiza la clave porque no van a poder llegar a ningún sitio en Internet. Siguiente diapositiva.

Obviamente tenemos que prepararnos para esto. Les hemos pedido a los operadores de red que vean si han podido habilitar la validación de la DNSSEC. Es necesario que se aseguren de que puedan actualizar esa clave. Históricamente, los resolutores comienzan a funcionar y no hay que pensar en eso. La gente los implementa en sistemas de archivo de solo lectura. Siguiente diapositiva.

¿Qué necesitan hacer los operadores de los resolutores? Estar al tanto y ver si la DNSSEC está habilitada en sus servidores. Estar al tanto de cuán confiable son las evaluaciones de sus sistemas. Tratar de verificar las actualizaciones y si hubo cambios en la clave, ver si la configuración es la correcta y si la validación de la DNSSEC está habilitada o está planeada en el sistema. Luego tener un plan para participar en el traspaso de la llave. Por ejemplo, observar conductas el día 11 de octubre y también saber qué harán si hay algo que falla. Básicamente si el resolutor no ha sido actualizado con la llave va a comenzar a responder con errores. Siguiente diapositiva.

El recuadro azul que ven en realidad es una imagen de la carta que enviamos. Enviamos una carta a los reguladores con copia a los representantes del GAC y a los operadores de red para que estuvieran al tanto del traspaso de la llave. Siguiente diapositiva. Eso sería todo. Con gusto ahora voy a responder las preguntas que tengan. Voy a brindar información que pueda para ayudarlos

a debatir este tema con sus operadores de red. Yo soy David Conrad. Mi correo electrónico es david.conrad@icann.org. Gracias. Le doy ahora la palabra al presidente.

THOMAS SCHNEIDER: Muchas gracias. Mi primera pregunta es si hay alguna línea telefónica análoga en caso de que toda la Internet se termine destruyendo y si va a operar las 24 horas, los 7 días de la semana.

DAVID CONRAD: Tenemos un centro de soporte global para que tengan en cuenta.

ESTADOS UNIDOS: Gracias, David, por la presentación. Esta es una cuestión que me toca de cerca. Nosotros recibimos la carta de Göran. Muchas gracias. Para ser honestos, mi reacción inicial fue que era necesario trabajar con nuestros ISP. En cuanto a brindar pautas para nosotros, ¿hay algo que nosotros podamos hacer como gobiernos además de garantizar que los ISP cumplan? ¿Hay algo más que nosotros podamos hacer que ustedes recomienden para que nuestras operaciones continúen?

DAVID CONRAD: Dentro de toda red, ya sea una red de gobierno interna o una red de ISP, tiene que haber un resolutor en algún lado. Quizá sea externo. Por ejemplo, Google tiene su propio servicio de DNS público que es 8.8.8.8. Muchos colegas utilizan ese servicio. Hay que asegurarse de que puedan lidiar con este traspaso de la llave raíz. Google definitivamente lo va a poder hacer. Eso es lo que me dijeron. No tengo duda. En cuanto a otros ISP, a otros operadores de red o empresas privadas, hay que preguntar para ver si realmente están al tanto del cambio de la clave. Primero hay que verificar si tienen el DNSSEC habilitado y si no, instarlos a que lo habiliten. Además saber si están al tanto de este cambio de la clave y también sugerirles que participen, en caso de que no estén al tanto, de los esfuerzos de traspaso de la llave que la ICANN ha estado publicando.

Nosotros lo estamos haciendo en muchos lugares para poder incrementar el conocimiento sobre este tema pero obviamente no vamos a llegar a todo el mundo. Pedimos que ustedes, como gobiernos, hagan algunos esfuerzos para que los operadores de red estén al tanto de que esto se va a llevar a cabo en el futuro.

THOMAS SCHNEIDER: Tiene la palabra Irán.

IRÁN: Gracias por la presentación. ¿Tiene algún aporte o algún comentario para garantizar que la acción que ha indicado se va a implementar debidamente antes de que algo no funcione? No todo el mundo está familiarizado con estas acciones y tiene velocidad para responder. ¿Ustedes recibieron alguna contestación de: "Sí, hemos recibido la carta. Lo estamos implementando"? ¿Saben de alguna posible dificultad?

DAVID CONRAD: En general, en todos los casos en los que hemos podido, hemos instado a las personas a que nos contacten si tienen alguna pregunta o alguna inquietud que nos quieran expresar. No tenemos ningún mecanismo explícito para pedir que nos brinden aportes. Estamos trabajando en particular con varios grupos de operaciones de red, varios TLD, varias organizaciones para brindar un lugar en el cual se puedan establecer canales de comunicación y que nos puedan hacer llegar las consultas.

THOMAS SCHNEIDER: Tienen la palabra Egipto, Noruega y luego Reino Unido. Países Bajos, perdón.

EGIPTO: Gracias, Thomas. Gracias, David, por la presentación. Tengo una pregunta con respecto a la diapositiva cinco. Mientras tanto, si

entendí bien, ¿hay alguna herramienta para saber si uno está preparado? ¿Han creado una herramienta así?

DAVID CONRAD: Sí. Creamos un banco de pruebas que les permite a los operadores de resolutores llevar a cabo una prueba en tiempo real del traspaso de la llave. No está en esta presentación porque está orientada a una audiencia más técnica pero, si desean, podemos brindar esa información al GAC para que se la brinden a sus operadores de red en los países correspondientes.

EGIPTO: Gracias. Eso sería muy útil. Mi otra pregunta es la siguiente. ¿Esto va a impactar específicamente a los resolutores? No veo aquí que estén los ccTLD. ¿Esto es para los operadores de registros de TLD?

DAVID CONRAD: Los que van a recibir el impacto es la parte del DNS que en realidad toma la información de los operadores de los TLD. Los TLD, los ccTLD, los gTLD no van a recibir el impacto del traspaso de la llave porque no tienen nada que ver. No hay una funcionalidad que ellos brinden. En realidad son los operadores de red los que van a recibir el impacto y también los resolutores.

THOMAS SCHNEIDER: Países Bajos.

PAÍSES BAJOS: Gracias, David, por la presentación. Quiero verificar algunas cuestiones. No creo que los gobiernos tengan una responsabilidad formal en todo esto pero ustedes están haciendo difusión externa para contactar a los ISP pero no hay una responsabilidad gubernamental en esto.

DAVID CONRAD: Correcto.

PAÍSES BAJOS: En segundo lugar, había una lista de los resolutores de DNS, los resolutores recursivos que efectúan la validación de la DNSSEC. Supongo que estos van a ser contactados directamente y son los que tienen que hacer el cambio real en sus sistemas. También hay otras partes interesadas que van a recibir el impacto, ¿pero tienen que cambiar sus sistemas?

DAVID CONRAD: La forma en la que se llevará a cabo el proceso del traspaso de la llave es de una manera automática. Si se trata de un operador de resolutor y tiene un software actualizado, entonces no tienen

que hacer nada en realidad. Probablemente tengan que ser prudentes y participar en los bancos de prueba para estar seguro de que nada extraño les vaya a suceder cuando se lleve a cabo el traspaso de la llave. En realidad hay un sistema automatizado dentro de estos resolutores que les ayuda a hacer el traspaso de manera automática. Si no tienen un software actualizado o si no han activado el traspaso automático, entonces van a tener que cambiar la configuración en el punto de datos. En realidad, esto está asociado con la KSK y esto va a tener que ser copiado en un archivo de configuración. Este sería el caso en el cual los operadores de resolutores tendrían que hacer algo, tendrían que tomar alguna acción.

THOMAS SCHNEIDER: Tiene la palabra el Reino Unido.

REINO UNIDO: Gracias, David, por esta presentación en el día de hoy. Todavía no hablé con los miembros de la unidad constitutiva de las ISP, la ISPCP, pero supongo que ustedes van a hablar con ellos para hacer difusión externa con ellos y supongo que eso se está haciendo así. No vi la carta así que también tendría que leerla y verificarla, de qué manera finalmente quedó redactada. También creo que usted dijo algo que tendríamos que verificar. Habló de los proveedores de redes gubernamentales. ¿Qué van a

hacer el 11 de octubre? Estamos todos prestando atención a esa fecha. Si algo sale mal, ¿habrá alguna medida de protección? ¿Cómo van a abordar las fallas significativas que puedan surgir el 11 de octubre?

DAVID CONRAD: Sí. Nos pusimos en contacto con la ISPCP y por supuesto los instamos a que se pongan en contacto con otros organismos similares. Con respecto a qué pasaría si sucede algo malo, bueno, nosotros establecimos un sistema de observación muy elaborado para monitorear el tráfico a los servidores raíz que serían la primera indicación de que hay algo malo que está sucediendo. Tenemos planes de contingencia que se podrían implementar en caso de que detectemos alguna especie de evento significativo en el caso que haya una falla en el traspaso de la llave.

Nosotros estamos bastante confiados en que probablemente los gobiernos no recibirán comentarios de los usuarios y de los operadores de red. Estamos trabajando en hacer llegar la información correcta para que todos tengan la clave actualizada.

THOMAS SCHNEIDER: Por favor, no se vayan. Hay un anuncio que voy a hacer en un minuto y que es importante. Ahora quiero darle la palabra al

caballero que está en el fondo. Creo que es de Nigeria. Por favor, no se vayan. Esta es la última intervención que vamos a tomar y luego vamos a tener que finalizar. Adelante, Nigeria.

NIGERIA: Muchas gracias por la presentación sobre el traspaso. Mi pregunta es la siguiente. Para los proveedores de servicios de red que no han habilitado la DNSSEC, ¿qué va a pasar después del traspaso?

DAVID CONRAD: No van a ver ningún cambio. Si no han habilitado la DNSSEC el traspaso de la llave no va a tener ningún impacto. Si en algún punto en el futuro deciden habilitar la DNSSEC entonces tienen que asegurase de que tengan la llave más actualizada. Caso contrario, la validación va a fallar y se van a confundir. Tienen que tener la llave más actualizada o el software de distribución más actualizado para poder recibir una actualización automatizada.

THOMAS SCHNEIDER: Vamos a tener que detenernos aquí pero quiero hacer un comentario breve dado que tenemos algo importante para contarles. Como ustedes saben, este es nuestro último almuerzo en esta reunión y también es el último almuerzo para Olof en su

cargo. ¿Cuál es su función en realidad? Es personal de la ICANN que brinda apoyo al GAC y que siempre hace bromas durante el día en las llamadas o a la noche. Su apoyo es necesario. Julia, que probablemente está escondida por algún lado, o salió, nos ayudó a organizar un pequeño presente para Olof. Vamos a verificar con la gente del equipo técnico para ver de qué manera lo puede llevar a su hogar. Esa es la tarjeta. Este es el regalo. No es muy pesado. Lo va a poder llevar.

Básicamente queríamos una vez más y finalmente decirle a Olof gracias. Hay algunas copas en el fondo. Hay algo para comer y algunas copas para brindar y para celebrar los últimos momentos de Olof en su puesto. Muchas gracias, Olof.

OLOF NORDLING: Muchas gracias. Yo siempre quise algo así. Muchas gracias realmente. Espero seguir en contacto, incluso aunque me retire. Voy a estar dando vueltas hasta finales de julio. No se van a liberar de mí totalmente, al menos no todavía. Muchas gracias.

THOMAS SCHNEIDER: Entonces podemos pasar al fondo de la sala.

ORADOR DESCONOCIDO: Thomas, quisiera hacer una pregunta. Después del almuerzo, nosotros nos vamos a reunir aquí nuevamente, ¿pero cuál es el objetivo? ¿Vamos a volver a debatir el comunicado o no es necesario? ¿Qué vamos a hacer? Ayer hablamos de reunirnos en algún momento a las 15:00.

THOMAS SCHNEIDER: Vamos a ver el texto que ya tenemos. Tom estaba trabajando. Lo vamos a analizar durante el almuerzo. La idea es que a las 15:00 tengamos todo listo y luego dediquemos unos cinco minutos al tema para poder finalizarlo. Gracias por recordármelo. No huyan todavía. No terminamos de trabajar. En primer lugar no es el trabajo. Vamos a festejar con Olof.

[FIN DE LA TRANSCRIPCIÓN]