SAN JUAN – Taller sobre las DNSSEC, parte 3
Miércoles, 14 de marzo de 2018 – 13:30 a 15:00 AST
ICANN61 | San Juan, Puerto Rico

JACQUES LATOUR: Estaba en la planilla este cuestionario. Tiene que haber suficientes. Si no tienen, por favor, díganme, así les alcanzo una. Si necesitan una, por favor, háganmelo saber. Vamos a poner el nombre de Warren. Bien. Por lo que he aprendido, uno puede crear sus propias reglas. Son seis respuestas por pregunta. 6.5 puntos por respuesta correcta. 8 puntos y medio. Tiene que ser bastante sencillo. Tenemos algunas horas para hacerlo. Además, yo puedo cambiar las reglas. Un punto por respuesta. Una respuesta por pregunta con un máximo 10 puntos. Hacemos la corrección y seguimos.

Pregunta 1. Hay una sola respuesta correcta por pregunta. Hay una respuesta por pregunta. Si usted pone ABCD, todas, no tiene ningún punto. Inténtelo, a ver qué pasa si responde varias veces.

Pregunta 1. ¿Cuál es el ccTLD que se firmó con DNSSEC más recientemente? Guinea-Bissau, las Islas Aland, Bután, Italia. ¿Cuál se firmó más recientemente? Una sola respuesta. A, B, C o D.

Pregunta 2. ¿En qué año firmaron Puerto Rico y Brasil por primera vez su TLD? Tuvimos una presentación hoy a la mañana sobre este tema. 2007, 2009, 2011 o 2013.

Pregunta 3. De acuerdo con las estadísticas de APNIC, ¿cuál es el país que tiene el despliegue más alto per cápita de usuarios capaces de hacer DNSSEC, incluyendo validación ECDSE y RSE? A) Suecia. B) Kiribati. C) Países Bajos. D) Groenlandia.

Pregunta 4. De acuerdo con la RFC 4509, ¿cómo deben manejar los resolutores de validación la presencia de SHA1 y SHA256 en un conjunto de registros de recursos de DS? Deben ignorarse ambos registros DS. Debe ignorarse el SHA1. Debe ignorarse el SHA256 o se deben soportar ambos DS. Pregunta 4. Sobre esto hablamos ya en el taller.

Pregunta 5. ¿En qué año se celebró la primera ceremonia de firma de la KSK en ICANN para su zona raíz en Culpepper, Virginia, Estados Unidos? No sabemos. 2004, 2007, 2010, 2012.

Pregunta 6. Esta es complicada. ¿Qué representa la H en el paquete de software SoftHSM? A) Homogeneizado. B) Heurístico. C) Harden (endurecido). De) Hardware.

Pregunta 7. ¿Cuál es el TLD individual que tiene el número más alto registrado de registros DS desde que se firmó la raíz? A) .SE, B) .NL, C) .BR, D) .US, E) .BANK. Esto viene de las diapositivas

de Roy en alguna parte. Es una serie de diapositivas de la DNS-OARC.

Pregunta 8. ¿Cuál de los siguientes términos relacionados con el DNSSEC no es un acrónimo? A) DANE, B) ENAM, D) [inaudible], E) DNS. Este cuestionario lo armó Jake Zack, que hace muchos cuestionarios. Esta pregunta es interesante. A, B, C o D.

Pregunta 9. ¿Qué porcentaje de la totalidad de TLD en la raíz están firmados? A) 97-100%, B) 94-96%, C) 90-94%, D) 86-89% y E) 81-85%.

La última. ¿Cuál de los siguientes TLD no está en la zona raíz? Interesante, ¿no? A) .AAA, B) .ABC, C) .ACO, D) .AEG, E) .ANT. No fue necesario desplazarme varias páginas para decir: “Qué interesante”.

Vamos a corregir entonces. Pásenle la hoja con su nombre al vecino. Vamos a hacer las correcciones. Yo siempre tengo razón. Soy la fuente autorizada de las respuestas.

Pregunta 1. Bután. 2 de diciembre. La más reciente. C.

Pregunta 2. 2007, Puerto Rico. La respuesta es A. Cuando firmaron por primera vez el TLD, ahí es cuando lo firmaron. No sé cuándo hicieron el DS. En las estadísticas dice Verisign, DNSSEC. La siguiente.

Según APNIC, la respuesta es D) Groenlandia, con el 77%.

Pregunta 4. Todos estuvimos en el taller DNSSEC. La respuesta es B. Hay que ignorar el SHA1, si es que está. A su vez, invalida la implementación del KSK o algo así.

Pregunta 5. 2010. Las preguntas tenían que ser fáciles para poder almorzar, ¿no?

¿Qué representa la H en el paquete de software? Hardware. A diferencia del nuevo router, este es más flexible.

Pregunta 7. .US es el que tiene el mayor número de registros DS. Creo que es el registro ADS. En algún lugar encontrarán las diapositivas de Roy y ahí está. Está probado y garantizado esto. Mándenle un mail a Roy. Yo siempre tengo razón. Este es el número de registros DS en la zona raíz para un TLD. ¿Qué TLD individual tiene el número más alto registrado de registros DS desde que se firmó la raíz? Las dos KSK con cuatro DS de distinto tipo por clave.

ORADOR DESCONOCIDO: Él es el narrador del cuestionario. Lo que él quiere decir es que el narrador del cuestionario siempre tiene razón.

JACQUES LATOUR: Exactamente. Me equivoqué entonces. No es E-N-U-M. No se dice D-A-N-E ni se dice E-N-U-M. Tengo razón. [inaudible], NUM, DANE, DNS.

El porcentaje es 90% todavía. 90.6 está entre 90 y 94.

La última, .ANT, que es la única que yo podría imaginar de qué se trata. Ahora corregimos.

Recuperen la hoja. ¿Quiénes tienen cinco o más respuestas correctas? ¿Seis o más? ¿Seis o más, una sola persona? Siete, ocho, nueve. Bien. Usted es el gran ganador.

RUSS MUNDY: Gracias a todos. Siempre nos divertimos con esto. Ahora vamos a tener que apurarnos un poquito porque el cuestionario estaba planeado para antes del almuerzo. Le voy a dar rápidamente la palabra a Viktor, quien hará una presentación. Adelante, Viktor.

VIKTOR DUKHOVNI: Me siento más cómodo de pie, si no les importa. Hay otro micrófono por allí. Vamos a ver cómo funciona. Soy Viktor Dukhovni. He trabajado en el espacio de seguridad del email desde el 2001. Me conocen como mantenedor de espacios de Internet. He escrito algunos RFC respecto de este espacio. Hablemos de varias cosas ahora.

Voy a darles un poquito de antecedentes para quienes no sepan qué es DANE. Para quienes no sepan qué es DANE, lo voy a presentar brevemente. Luego les voy a contar qué hacer aun cuando ustedes no implementen DANE pero sí tienen DNSSEC y están aun en el riesgo de no recibir emails si no tienen el saneamiento adecuado. Voy a hablar un poquito de cómo implementar DANE de manera confiable. Algunos adoptantes entusiastas lo hicieron prematuramente sin la debida planificación. Hay que planificar, automatizar y monitorear DANE.

Luego les hablaré de una encuesta que estoy haciendo, que rastrea datos de adopción de DANE y ayuda a la gente que pueda haberse equivocado. Ayudamos a corregir. Luego hay un apéndice. Hay muchísimo material pero no tengo tanto tiempo. Encontrarán una copia de las diapositivas en el sitio web. Son muchas las diapositivas. Voy a saltear algunas porque no me alcanza el tiempo.

Bien, una breve reseña de lo que es seguridad del email. Era bastante seguro. Tenemos el remitente que tiene un TLS autenticado. Representa a un agente de presentación de mail, el mailserver. El destinatario puede leer el mail de manera segura en el IMAP con TLS autenticado y es seguro porque tanto el remitente como el destinatario están bien pero hay un problema. El mail tiene que llegar del remitente al destinatario.

Hay un espacio en el medio que se llama MTA o agentes de transferencia de mail que mueven los correos entre las organizaciones y que se aseguran milagrosamente de que el mail llegue del lugar A al B totalmente encriptado. Bueno, no exactamente. Voy a describir en más detalle qué pasa en este paso dos, entre el remitente y el destinatario, que es el espacio donde operan software como Postfix, que tiene por finalidad dar seguridad.

¿Qué pasa entonces entre en la organización cuando las cosas pasan de un lugar a otro? Tenemos lo que se llama STARTTLS oportunistas que son mailservers que tratan de determinar si el destino soporta encriptado del mail en tránsito. Esta tecnología es bastante útil. Resiste el monitoreo pasivo. Si alguien está interfiriendo en la línea pero no hace nada para oír la comunicación, el tráfico sigue siendo confidencial en la transferencia de un mail server a otro. Esta tecnología es vulnerable a ataques activos. Hay muchos papers que demuestran cómo esto se hace. El atacante activo que interfiere con el tráfico puede hacer a través de secuestro BGP que puede derivar el tráfico durante algunas horas o puede hacerlo a través del envenenamiento de la cache si no hay DNSSEC o puede hacer strip de STARTTLS y al destinatario le aparecerá como que el remitente no tiene capacidad de encriptado y se despejará el envío.

No obstante, STARTTLS de Gmail fue un enorme éxito. En 2014 había un 25% del tráfico Gmail encriptado. Antes era 5-10%, cuando yo estudiaba, pero ahora, a la derecha, es difícil ver, el 90% del email que va y viene en Gmail hace encriptación STARTTLS. Funcionó bastante bien. Hay un vínculo donde ustedes pueden ir chequeando estas estadísticas periódicamente para ver cómo cambian, pero podríamos hacerlo mejor. Llevar el [inaudible] a un estado para que la gente que quiera pueda resistir los ataques activos.

Para lograr esto, en un ecosistema donde en gran medida hay STARTTLS oportunista, necesitamos una señal que le diga al remitente que este destinatario necesita seguridad y que debe hacer un downgrade de la resistencia, si no, vamos a entrar en STARTTLS stripping. Hay un mecanismo de señalización.

Un mensaje a llevar de esta sesión es que muchos piensan: “Ese NTP usa TLS, es como HTTP. Por supuesto, todo lo que funciona bien para HTTP debería funcionar para el mail”. La respuesta es distinta. Pueden leer en el vínculo que aparece en la diapositiva que lo primero que es distinto es la dirección. El mail establece la dirección según el registro del DNS. Se está confiando fundamentalmente en el DNS ya para contar con parte de la seguridad.

Otra cosa es que las autoridades de certificación web, y hay miles, en realidad son demasiadas como para tener un sistema de seguridad. En especial cuando hay una excepción y no se confía en un CA, no como en el HTTP, se puede hacer clic y decir: "No me importa. Voy a hacer clic igual. No es mi banco. Muéstrame la página insegura". Con email, no hay usuario que quiera que le muestren la página insegura. Hay que confiar en la mayor cantidad de posible de CA, lo cual no es una buena estrategia de seguridad.

Aquí aparece DANE. DANE está muy bien preparado para SMTP. DANE significa Autenticación basada en DNS de Entidades Nombradas, que es un nombre un poco raro. En SMTP, la forma en la que está definida la RFC 76 que Wes y yo escribimos, se indica que se pueden recibir mails de modo seguro al publicar un registro en DNS. Un registro en la zona firmada de DNSSEC.

Ese registro que se publica comienza con un número de puerto que en SMTP es 25. La etiqueta de protocolo es TCP y luego nombra el MX, donde vamos a tener la seguridad. Después incluye algún parámetro que indica cómo asegurar el tráfico. La presencia de ese record de TLSA, según está definido en la RFC, dice que yo absolutamente siempre voy a hacer STARTTLS. Si no ven STARTTLS, debe de haber un ataque o un error operativo importante en mi zona donde yo accidentalmente me olvidé de habilitar STARTTLS.

Esto es importante porque esta señal se emite a través de DNSSEC y si alguien trata de decir que no hay esto en la zona, porque DNSSEC hace suficiente autenticación, el resolutor validante no va a creer en el ataque. Va a haber una falla y va a pasar al siguiente. Nosotros luego encontramos un contrato para hacer STARTTLS pero también tenemos un contrato no solo para STARTTLS sino para tener una cadena que haga coincidir esos registros TLSA. Ahí es donde aparecen estas claves. Voy a hablar de estas claves en un momento.

DANE autentica el control de dominio a través de DNSSEC para que no tengamos CA encriptados en las que quizá confiemos o no. Este sistema está autocontenido dentro del DNS para una publicación secura de los registros. También es un sistema resistente al downgrade. Yo prometí que iba a hablar un poco sobre cómo llevarse bien con DANE. Los dominios lo están empezando a implementar. Comcast, no sé si el caballero está aquí todavía, está haciendo validación de DANE outbound, así que si ustedes quieren recibir un email de Comcast, presten atención aquí. Si quieren recibir mails de alguna otra organización, incluso ietf.org, que creo que también hace validación DANE, lo hace inbound y creo que también outbound.

Si ustedes quieren convivir con DANE tienen que entender que quienes envían DANE no hablan con un host MX que busque fails. El lookup TLSA puede probar que el registro no existe. No

existente no es una falla. Falla es que los datos incorrectos vuelven. Hay malas firmas, hay algo que está mal sobre el paquete de DNS o alguna firma que expiró o que simplemente no responde. Si alguna de esas cosas sucede, especialmente si sucede en los hosts MX, no van a recibir ningún mail de DANE cuyo número yo espero que siga aumentando en los próximos años.

Para los dominios que no tienen TLSA, si no están haciendo DANE, al menos tienen que garantizar ustedes la denegación de existencia, el hecho de que no están allí, se entregue de manera confiable. DANE es el primer protocolo para lo cual esto es importante. Hay muchos que han confiado en DNSSEC para proteger registros que están allí y asegurarse de que esos registros se entregan con seguridad.

DANE necesita registros que no están ahí para demostrar que es correcto. No sorprende que a principios de 2014, cuando empecé a trabajar en DANE, hubo muchos servidores de nombre que no lo hacían bien porque a nadie le importaba, nadie confiaba en eso. Ahora sí. En los últimos dos años logré que la mayor parte de los operadores con un nombre equivocado lo arreglen pero la mayoría no han testeado su propio nombre. Para coexistir con DANE tenemos que tener una cierta higiene. Todo lo que está en estas diapositivas sobre EDNS0, IP fragments, respuestas a no data versus MX domain, etc. No los voy a leer… Tenemos que

sacarlos y testearlos con el dominio para asegurarse de que anda bien.

Monitorear, por supuesto, es importante. Quiero destacar que ha habido firewalls, middleboxes, todas las cosas que creemos que nos ayudan a proteger contra el tráfico hostil a bloquear consultas de ciertos registros. Si ustedes ve un query para un registro A o MX, está bien, pero las queries para TLSA, CA, CDS, nuevos tipos de DNS, esto es algo que hay que bloquear porque la firma al fin y al cabo no los tiene. Hay que bloquear esos queries.

Esto no parece ser una muy buena idea porque bloquearlas hace que falle DANE pero también hace que fallen las cuestiones de certificado o incluso la potencial implementación de la KSK. No hay que implementar firewalls que bloqueen el DNS. Es una mala idea. Nunca se deben implementar. Pero si tienen un firewall de este tipo, no hay que habilitar esta característica. Aquí les muestro un par de ejemplos con Digg. En este caso, no hay que habilitar ni no data ni MX domain.

Aquí una lista de DNSSEC. No los voy a leer todos. Vi algunos puntos en el final sobre el NSEC3. Es algo que descubrí al realizar esta encuesta. Aquí tenemos una imagen con DNSviz de un sitio al que los dominios con DANE no podrán enviar mails. Techtrack.gov, después de firmar su zona, hace algo que utiliza

para subir el número de serie después del SOA. La denegación de existencia nunca funciona. Ustedes pueden escribir un código que haga ingeniería inversa a las firmas y si yo pongo este número de serie, la firma se valida, pero siempre hay uno más alto que el otro. No hagan esto. Tengan cuidado. Es el mismo monitor. Se habrían dado cuenta de todo. Esto es sobre la higiene de DNSSEC. Practiquen esto, aunque no estén haciendo DANE. Hay algunas diapositivas más con ejemplos de mala higiene de DNSSEC en el apéndice, si tienen curiosidad.

Adopción de DANE. Se supone que tienen que estar todos contentos como yo y quieren adoptar DANE. Lo primero es que no voy a llegar muy lejos con DNSSEC. Hay que firmar la zona. Una vez que firmaron la zona, ahí empieza lo difícil. Gestionar DNSSEC es más difícil que gestionar DANE. Creo que me van a creer al final de esta conversación que es fácil.

Lo difícil es coordinar los registros TLSA y las cadenas de certificado que pueden ser más complicadas. Hay que hacer cambios para rotar las claves en dos lugares. Uno es en los certificados desplegados en las claves privadas y lo otro es que tenemos que actualizar los registros TLSA en el DNS. Hacer estos cambios parece más difícil pero los vamos a hacer fáciles.

Lo primero es que vamos a hablar sobre DANE outbound. Supongamos que no estamos listos para firmar la zona o no se

entrenó al equipo sobre cómo hacer mantenimiento de TLSA. De todos modos, podemos habilitar DANE para emails que estamos mandando a sitios que han implementado DANE. Para eso necesitamos un resolutor validante de DNSSEC. En general, los servidores de email en máquinas que no son laptop, que no son teléfonos, son máquinas en centros de datos que pueden tener un resolutor local y que pueden mejorar el desempeño y permitir una validación. Muchos de los MTA que están implementando DANE no hacen la validación DNSSEC sino que se apoyan en un resolutor. No hay nada más seguro que correrlo en la misma máquina si quieren tener una ruta segura.

Los MTA que habilitan DANE que pueden conseguir fácilmente son Postfix, XM. Cloudmark son proveedores que tienen una escala un poco más grande que los MTA más pequeños. Hay otros que van a venir. No debería mencionar a las personas que todavía no lo implementaron pero hay proveedores que lo van a hacer.

Luego tenemos un resolutor validante. Buscamos la documentación. Lo habilitamos. Va a funcionar. Lo mismo que con Comcast y los anclajes de confianza negativos. Hay algunos casos en los que podemos utilizar anclajes negativos DANE y hay una página GitHub donde un voluntario mantiene una lista parcial de los fallos de DANE a la que se puede contribuir. Pueden contribuir si quieren o si encuentran otros dominios que

no funcionan. No hay tantos pero se puede tener una excepción de tanto en tanto.

Vamos a hablar de inbound DANE. ¿Cómo implementamos los registros TLSA? Definitivamente, MTA tiene que soportar STARTTLS. Los registros MX tienen que estar firmados. Si la dirección de su dominio a quien sea que gestiona el email es insegura, entonces el intermediario puede redirigir el email a quien quiera y no va a haber seguridad de email salvo que su dominio esté firmado.

Luego va a haber algo más interesante. Una vez que se firma el registro de MX, si el email es alojado por un proveedor que no es ustedes y que opera los servidores para ustedes, ahí ya está. Le toca al proveedor implementar el resto de DANE inbound, no con el dominio alojado. Si ustedes son un cliente que gestiona muchos dominios, tienen un trabajo fácil. Gestionar todos los mails en una rotación específica con todos los bits específicos, eso lo hace un proveedor externo.

Si ustedes tienen su propio alojamiento de mail, básicamente van a ser un proveedor y el resto va a tener que ver justamente con cómo ser un proveedor. El proveedor publica dos tipos de registros TLSA. La especificación define 24 tipos de registros TLSA diferentes. 22 son una mala idea. No los usen. Hay solamente dos que ustedes tienen que considerar publicar. El

primero es el 311 que tiene un código de certificado DANE EE. La E es de entidad. Ustedes están publicando el resumen de la clave pública en el certificado. Yo me comprometo a que mi servidor va a tener una clave pública.

La alternativa es que ustedes pueden decir: “Bueno, no sé muy bien cuáles son los certificados que conoce mi servidor pero seguramente los va a emitir una anclaje de confianza específico. Estoy publicando el hash de la clave pública de quien sea que va a emitir mi certificado de servidor”. También podemos ver que se pueden publicar ambos.

Los registros TLSA tienen 211 o 311. El resto del registro es un valor hash. Ahí es donde ustedes van a decir cuál es el resumen de la clave pública. Para ietf.org, que es el que está abajo, ustedes van a ver que el hash empieza con OC72 y que termina con D3D6. Pueden haberlo rotado en este tiempo.

¿Cómo gestionamos los registros de TLSA? Lo que ustedes tienen que hacer es que el registro TLSA esté en el DNS antes de que se implemente la cadena de certificado. Este cache entre el resolutor y el servidor autorizado e incluso dentro de los servidores autorizados, hay esclavos y masters. Por lo tanto, hay una demora muy importante entre los cambios del servidor autorizado y cuando el cliente empieza a ver todo esto antes en lugar de lo que teníamos antes. En los registros TLSA yo puedo

decir que tengo este certificado o el otro y que lo tengo que colocar cierto tiempo antes de que el certificado se active en el servidor de mail para que cuando esté activado los clientes que van a ver ese certificado miren el certificado TLSA y vean uno adecuado. Van a decir que está bien.

Por suerte, nosotros no tenemos un problema imposible de sincronización de las actualizaciones y del cache de DNS. Podemos tener múltiples registros TLSA, algunos que van a funcionar en el futuro y otros ahora, y el verificador que consume los registros no tiene que tener una coincidencia total. Es suficiente con que coincida uno solo. Lo que nosotros hacemos es que publicamos las claves por adelantado y garantizamos que al menos uno de estos registros coincida, ya sea con la clave presente o la futura.

Hay dos formas, la que yo verdaderamente recomiendo es la primera, donde uno publica dos registros TLSA de identidad. Uno coincide con la clave pública y el otro coincide con la próxima clave pública que va a haber la próxima vez que se implemente el certificado. En el otro modelo que yo recomiendo, ustedes publican dos claves. Una para el servidor y la otra para el emisor del CA. Voy a explicar las ventajas de cada uno. Adelante.

En el actual más el próximo vamos a tener uno de ahora y uno para el futuro. ¿Qué hacemos para mantener la cordura mientras

lo hacemos? Supongamos que rotamos las claves cada 90 días pero no queremos hacer muchos pasos de secuencia coordinados para que tres o cuatro veces en esos 90 días tengamos que recordar algo y después esperar que termine y después hacer lo siguiente. Simplemente vamos a tener un cambio de ciclo cada 90 días. Para que quede simple, generamos la próxima clave en el mismo día en que implementamos la clave actual. Supongamos que este es el día 0. Yo implementé la llave actual pero también generé la clave que voy a utilizar a 90 días de ahora. Puedo dejar la clave offline y cuando me ocupo del public key value puedo inmediatamente implementar los cambios en el nuevo certificado con la nueva clave y publicarlo para que coincida con la clave a 90 días de ahora. En esta diapositiva ustedes ven dos registros de TLSA. Uno coincide con el que yo acabo de habilitar y el otro coincide con el que voy a habilitar en 90 días. Años o meses o días después, yo los aliento a que lo hagan con frecuencia porque es mejor hacerlo con cierta frecuencia y no cada tres o cinco años.

Cuando hablamos de la próxima ventana de mantenimiento, ustedes van a obtener un certificado para la llave pregenerada. Esto es fácil porque uno firma una CSR y ve que es la misma que hace 90 días. Va al CA, obtiene un certificado de nuevo y antes incluso de pensar en obtener el certificado, implementarlo. Hay que asegurarse de que el registro TLSA tiene que coincidir.

Tendría que haber estado allí hace mucho tiempo. Esta verificación los va a mantener fuera de peligro. No van a implementar un registro TLSA no está y no está desde hace bastante tiempo.

Luego volvemos al primer paso. Generamos la próxima clave otra vez y con este tipo de proceso podemos garantizar que no estamos ocupándonos en el último momento de actualizar el DNS con los últimos registros. Esto funciona bien y puede implementarse incluso con claves menos encriptadas si utilizamos la opción CSR, que es la que permite especificar la propia clave en lugar de tener que generarla.

Muy bien. Este fue entonces el primer modelo. El segundo es un modelo donde en lugar de tener la llave actual y la próxima para el servidor tenemos la llave actual para el servidor y la próxima para el CA. En este modelo publicamos ambos y si alguno de ellos verifica que funciona bien y que es el momento de hacer el rollover, si todo sigue igual está bien si ustedes implementan un nuevo certificado con la nueva clave que no coincide con el registro 311 y el registro 211 va a seguir funcionando como si tuviese el mismo CA. Luego lo implementamos, lo testeamos, nos aseguramos de que funcione bien y el registro no va a coincidir. Una vez que estén conformes y todo esté bien, pueden rotar el registro 311 después de haber implementado. Si ustedes no quieren planear y quieren ser reactivos e implementar y

después hacer los cambios, este modelo nos permite ser alguien que deja las cosas para más adelante, implementar el certificado en el último momento y luego actualizar el registro 311.

Por otro lado, si en algún punto ustedes eligen emitir un nuevo certificado CA y una clave nueva, solo en ese caso se van a asegurar de que obtenga del nuevo CA una nueva clave con un certificado con la misma clave que utilizaron antes. Ahí ustedes mantienen la continuidad y el registro 211 va a cambiar pero el 311 va a seguir siendo el mismo. Ahí ustedes pueden ir rotando, manteniendo 311 como la misma o periódicamente mantener 211 como la misma y cambiar el 311. Siempre que ustedes sean disciplinados en este sentido, el proceso es bastante simple.

Por supuesto, cualquier proceso que se haga con frecuencia está sujeto al error humano, si la gente lee un script de pasos que tienen que hacer manualmente. En lo más posible, al implementar DANE, como proveedor de servicios en especial, no queremos que el equipo lo haga a mano sino tener cierta automatización.

Lamentablemente yo no puedo decirles cómo hacer el despliegue de certificados por la forma en que están almacenados y desplegados según el MTA pero les puedo decir cómo son las actualizaciones porque los distintos backend tienen distintos mecanismos para insertar datos. A lo mejor se

actualiza. Quizá haya algunos scripts. A lo mejor lo publicaré algún día. Digamos que durante un tiempo todavía va a depender del sitio.

Si despliegan registros TLSA en DANE, les pido por favor que contacten con el responsable en WHOIS o con el responsable del registro de SOA o con la dirección del postmaster, si no, la gente no podrá enviarles un mail y hacerles saber qué es lo que está pasando. A veces para mí es difícil encontrar el contacto para la gente que comete errores.

El monitoreo de DANE. Yo me estoy ocupando en este momento pero no seré el monitor para siempre. Por favor, monitoreen sus propios despliegues para que se aseguren de que está bien desplegado. Esta es una lista de mejores prácticas de DANE. No utilicen los certificados comodines. Hay muchas cosas que pueden hacer.

Bueno, eso era acerca del despliegue de DANE. Hay algunos software de DANE como mencioné: Postfix, Exim, Cloudmark. Si hacen mailbox para su propio dominio, les recomiendo mailinabox.email. Tiene una appliance que hace el cambio de certificado totalmente integrado. Simplemente se activa, se delega. Aquí hay un ejemplo. Se ocupa de todas las cuestiones, incluido el antispam. Es un software excelente. Si son desarrolladores, pueden usar OpenSSL 110, que tiene una

librería de validación y hay documentación. Si quieren usar GnuTLS, pueden hacerlo pero teniendo en cuenta ciertas cosas. Yo no lo recomiendo demasiado. Por favor, pónganse en contacto conmigo si van a hacer DANE sobre GnuTLS. Si son mantenedores o planear correr software relacionado con DANE, por favor, pónganse en contacto conmigo para hablar de ideas, comentarios.

Esta es una lista de herramientas. Hay un sitio para testear los dominios en la web. Hay una lista de usuarios que publica estadísticas mensuales. Paul Wouters escribió este hash-slinger. Phil Pennock, del equipo de desarrollo, publicó este SMTP DANE, que es un validador [inaudible]. Es del que yo me ocupo pero todo el mundo le tiene miedo. Incluso pueden hacerlo solos con un shell script. Hay un ejemplo en el apéndice de cómo hacer los comandos para testear la corrección de las MTA.

Me quedan dos minutos nada más para la encuesta. Tengo una encuesta que cubre la mayor cantidad posible de DNS con 200 millones de dominios, de los cuales 5 millones ya están firmados con DNSSEC. Con casi 180.000 dominios que hacen DANE SMTP, con millones de usuarios, Comcast, GMX, etc.

Algunos números sobre los hosts MX y hay una cantidad pequeña de problemas. Más de 100 dominios con problemas de higiene de DNS. Unos 150 con registros TLSA incorrectos. Todos

mis intentos para notificarles de los problemas han sido infructuosos. Este es el crecimiento a lo largo del tiempo, desde 2016. Teníamos 1.800 organizaciones con hosts. Ahora estamos cerca de 3.200. O sea que sigue creciendo bastante rápido. Estos son algunos de los dominios. Registrar.br, Comcast, GMX, Domeneshop tiene un gran despliegue y obviamente .ORG como ietf.org y los que trabajan en seguridad como Torproject. Hay muchos más, por supuesto, pero estos son los más prominentes.

Esta lista es de proveedores que tienen muchos dominios firmados con DNSSEC y el host de mail pero no tiene DNSSEC o lo tiene pero no tiene DANE. El mundo sería mucho mejor si estos proveedores en particular, ya sean ustedes o conocen a gente sobre la cual pueden influir, apuntaran sus registros MX al DNSSEC.

One.com, con una gran población que aloja mail podría pasar a DANE, pero todavía no lo ha hecho. Google está pasando de google.com a googlemail.com y entiendo que DNSSEC para Google es un problema bastante importante pero siendo DNSSEC para googlemail.com sería mucho más fácil. En cierta forma soy optimista en que los 335.000 dominios de googlemail.com quizá en el año que viene, si todo va bien y estoy muy entusiasmado, pasen a DANE. Hay otros proveedores que sería bueno que implementen DANE.

Necesito ayuda. Sin duda necesito monitorear muchos más ccTLD. Si quieren compartir su zona para investigación, voy a firmar todos los acuerdos de confidencialidad que quieran. Necesito más datos. Quisiera que la gente remedie los más de 100 problemas de los mailservers para que no haya bloqueos. Por favor, permitan el DANE saliente. En especial si son remitentes importantes porque la gente que maneja mal los registros TLSA saben que esto pasa si hay presión de los grandes proveedores que no envían los mails. Rápidamente van a notificar el problema.

Por favor, habiliten DNSSEC y DANE. Si son OVH o one.com, estos proveedores lo van a hacer. Gente como GoDaddy, por ejemplo, que tienen millones de dominios, muy pocos de sus dominios están firmados. Sería fantástico si GoDaddy quisiera trabajar con DANE por los millones de dominios que tienen. Apéndice. No voy a hablar del apéndice. ¿Alguna pregunta o ya no tiempo para eso tengo?

RUSS MUNDY: Perdón, Viktor. Muchísimas gracias por su presentación. Si usted se puede quedar después en el pasillo, la gente le puede hacer preguntas en ese momento. No hay más tiempo. Gracias, Viktor. Warren, si puedes acercarte para tu presentación. Kathy tiene las diapositivas. Este es quizá el panel más emocionante del día.

Estoy seguro de que todos en esta sala saben que los planes de traspasar la clave que se habían diseñado inicialmente han sido pospuestos. Hay que una serie de actividades en curso en este momento. Matt nos va a hacer una presentación sobre esto. Luego tendremos una pequeña mesa de discusión con Joe de Comcast, Jacques de CIRA y Warren de Google. Matt, aquí tenemos el reloj.

MATT LARSON: Gracias, Russ. Gracias por invitarme. Esta es la misma serie de diapositivas que voy a presentar en dos horas en la sala Ballroom A. Tenemos una sesión en la agenda principal sobre este tema. Voy a ir muy rápido con esto. Estoy seguro de que ya algunas de estas las mostré. Por una cuestión de restricción de tiempo voy a ir muy rápidamente. Si tienen preguntas o si hay algo que falta, pueden volver a verme en el Ballroom A.

Rápidamente, una recapitulación de cómo llegamos al día de hoy. En septiembre del año pasado pospusimos el traspaso de la KSK después de analizar los datos del informe del anclaje de confianza del RFC 8145. El primer análisis lo realizó Verisign. Identificamos distintos porcentajes, dependiendo de cómo se clasificaran los datos, de más resolutores que todavía reportaban la clave antigua. No sabíamos realmente qué anticipar pero estos porcentajes parecían más altos de lo que

nos parecía conveniente pero lo peor es que no sabíamos por qué teníamos este valor, entonces quisimos investigar.

Investigamos. Una persona en esta sala hizo la investigación. Intentamos contactar a 500 resolutores que habían reportado esta situación en septiembre de 2017 y encontramos que hacer seguimiento de los operadores de rastreo basándonos solo en la IP es difícil. Del 20% que sí pudimos contactar, aparentemente el 60% estaban en rangos conocidos para los dispositivos hosts con IP dinámicas. Había una gran cantidad de instancias que iban y venían. Los informes de 8145 son queries regulares de DNS, así que están sujetos a reenvío. También descubrimos otras cosas extrañas como implementaciones que enviaban informes 8145, incluso sin hacer validación.

Esperábamos encontrar una o dos causas raíces y luego ajustar nuestros mensajes y después contactar a los proveedores, si es que era cuestión de proveedores, pero no fue lo que identificamos, entonces no había un camino claro hacia el futuro. Le pedimos a la comunidad que nos diera guías acerca de cómo proceder. Eso pasó a finales de diciembre, enero. A finales de diciembre fue cuando se anunció que íbamos a solicitar comentarios sobre el traspaso de la KSK a la organización ICANN. Se invitó a la comunidad a dar sus opiniones. Hubo acuerdo de que realmente no había manera de medir con exactitud el número de usuarios que se verían afectados por el traspaso.

Necesitábamos una guía mejor para proceder con el cambio. En definitiva, eran los usuarios los que iban a ser afectados.

Las discusiones llegaron a la conclusión de que era muy difícil medir esto con exactitud. Hasta que hubiera mejores mediciones en el futuro, el consenso fue que la organización de la ICANN tenía que postergar el traspaso de la clave. El 1 de febrero publicamos un borrador de plan que planea traspasar la clave el 11 de octubre de 2018, sin criterios de medición específicos en la discusión. Vamos a continuar con las acciones de difusión. Vamos a publicar los datos del anclaje de confianza 8145, a ver qué pasa.

Lo más importante es que hay un periodo de comentarios públicos sobre este plan, que cierra en un par de semanas, el 2 de abril. Les invitamos a todos a que por favor hagan sus comentarios porque vamos a proceder según el resultado de los comentarios. La idea es hacer este plan para que la comunidad lo presente. Esta es una recapitulación de dónde nos encontramos y los pasos a seguir. A mediados de abril es cuando se publicará el borrador del plan, los comentarios públicos y el plan revisado sigue con esta fecha de 11 de octubre.

Vamos a proceder tal como dice la diapositiva, con un taller de la junta el 10 de mayo. El SSAC y el RSSAC revisarán y comentarán el plan. Habrá otra sesión. Hablaremos nuevamente en Panamá,

en la ICANN62. Esperamos que para agosto SSAC y RSSAC nos den su opinión. Luego publicaremos el plan final pero dependeremos de la decisión de la junta.

La junta, si no lo saben, se reúne seis veces por año, en todas las reuniones de la ICANN y tres veces en medio, en lo que se llaman talleres de la junta. Habrá un taller de la junta en septiembre y se solicitará a la junta entonces que adopte una resolución autorizando a la organización ICANN que traspase la clave, que será el 11 de octubre.

Volvamos a los datos. Lentamente venimos añadiendo datos RFC 8145 que recibimos de los distintos servidores de zona raíz. Esta diapositiva, si bien está actualizada, hubo acontecimientos recientes. Ahora tenemos datos creo que de 12 servidores raíz. Solo hay uno que no participa. Los operadores que corren DNSCAP cada 60 segundos reportan a través de un query DNS, muy inteligente, lo que informan los anclajes de confianza. Estamos recopilando todos estos datos. Este es el gráfico principal. Este gráfico quizá sea un poquito difícil de leer al principio porque hay dos ejes. La línea roja y la verde son el número de direcciones IP fuente por día que nos reportan datos RFC 8145. La línea verde es el número total de fuentes que reportan. En este momento son aproximadamente 50.000 y la roja es la que solo reportan KSK 2010, los que perdieron el tren.

El porcentaje a la derecha es el de la línea roja versus la línea verde. Fíjense que en este momento estamos en un 20% que es mucho más que lo que teníamos cuando comenzamos con estos datos en septiembre. Seguimos sin saber por qué esto sucede. Estamos tratando de dilucidarlo. En algún momento tendremos que dejar de hacer diapositivas y empezar a presentar soluciones.

Fíjense que hay un gran pico en mitad de enero. ¿Qué es eso? Estamos muy seguros de que corresponden con el release unbound, que tuvo un fix de seguridad. La sospecha es que la gente se sintió motivada de hacer el upgrade porque tenía que ver con la seguridad. Aún hay sospechas de por qué no hubo un drop-off después de 30 días. Aun cuando estos son nuevos contenedores, este nuevo unbound sigue teniendo la clave antigua. Después de 30 días en el proceso de RFC 5011 marca que la clave es antigua.

Aquí vemos un desglose de todos los servidores raíz de los cuales tenemos datos. Más allá de la raíz J, los gráficos son bastante parecidos e incluso el porcentaje en la raíz J es bastante bajo. Aquí están las IP individuales que se fueron agregando a lo largo del tiempo. Son aquellas que nunca habíamos visto antes y que van adquiriéndose día a día. Fíjense en los picos. Cada vez tenemos nuevas IP. El pico de mitad de enero pareciera que nos llevara a un estado constante en cantidad de IP nuevas. Hay

cierta actualización de los datos del RFC 8145. Aquí la explicación posible sería que hubo un despliegue de una gran cantidad de direcciones IP únicas.

Aquí vemos las fuentes únicas a lo largo del tiempo. La línea verde muestra las fuentes únicas a lo largo del tiempo que reportaron datos RFC 8145. Fíjense en las cifras. Fueron subiendo desde que comenzamos a recopilar los datos en septiembre. La línea roja es el número de los que reportaron KSK 2010. Este informe es peor, es un tercio. Aquí vemos las que son /24. Hay muchas /24 en estas direcciones IP.

No hay mucha diferencia entre las fuentes que reportan. Lo voy a decir de un modo más fácil. Hay poca evidencia de que el upgrading ocurra, de que haya alguien con KSK 2010 que se pase a la llave nueva. Pueden ver estos gráficos publicados semanalmente en esa URL. Hay uno para cada uno. Esta es mi última diapositiva. Yo tengo autorización de ICANN legal para publicar esta lista. Lo voy a hacer. Va a ser algo similar a esto. Va a ser una lista en orden inverso de frecuencia por ASN. Así van a poder ver todas las IP asociadas a una ASN vinculado. Claramente van a ver en los que hay algunos lugares con los que podemos contactar y decir qué es lo que está pasando. Hay muchas veces en las que uno tiene que parar y decirle qué está pasando. Por supuesto, un llamado al ASN 55836 es lo ideal para

saber qué sucedió. Voy a parar entonces aquí. Creo que tenemos suficiente tiempo para que el resto del panel hable.

RUSS MUNDY: Muy bien. Gracias, Matt. Gracias por tu presentación. Hay otros miembros en el panel y queremos tener perspectivas diferentes. Jacques Latour va a ir primero con una perspectiva de los TLD.

JACQUES LATOUR: Este es un TLD en un país relacionado con un ciudadano. Yo lo estuve siguiendo mucho. Como dije en el comentario, en la implementación de la KSK, es prácticamente imposible medir esto y hacer el cutover sin daños colaterales. Desde mi punto de vista, si nosotros queremos mantener la confianza percibida en la llave, tenemos que poder hacerlo de un modo confiable. Es decir, nosotros lo hacemos, lo estamos respaldando y si falla, la gente lo va a arreglar muy rápido porque es fácil de arreglar. No son días, semanas, meses antes de que alguien lo arregle. O se actualiza el anclaje de confianza o se deshabilita la validación.

Esto va a tener un gran impacto en algunas regiones. Desde mi punto de vista, cuanto más demoremos, más incertidumbre vamos a incluir en este proceso. Esto va a impactar en la confianza de lo que queremos generar. A pesar de que la ceremonia, la llave y todo el proceso para crear esto es

impecable, si lo demoramos más, esto va a erosionar la confianza.

Hay que hacerlo. Hay daños colaterales. Son fáciles de reparar. Tenemos que rotar la llave también el año que viene. Tenemos que rotarla todos los años como un proceso estándar y automatizarla. Si un día nosotros tenemos que hacer una implementación o un traspaso de emergencia, va a funcionar y no va a haber ningún problema.

Si usamos DANE dentro de empresas a escala grande y utilizamos también el CA, todo depende de la llave de la raíz. Creo que tenemos que hacerlo y vivir con ello. Tenemos que utilizar relaciones públicas para explicar cómo se arregla, o lo apagan o deshabilitan la validación. Si alguien utiliza DNS en la búsqueda, Google y Bing y todos los motores búsquedas deberían decir que eso es lo que tienen que hacer. Esperar más no es bueno para la comunidad.

RUSS MUNDY: Gracias, Jacques. Ahora Joe, si pudieses darnos una perspectiva de los ISP, por favor, hágalo.

JOE CROWE: Yo estoy de acuerdo en que tenemos que decir que debemos implementarlo todos los años a nivel operativo y que podemos

encontrarnos con algunos problemas, como que nosotros no queremos deshabilitar la validación de DNSSEC. Cuando se suponía que iba a ocurrir el primer traspaso, nosotros la validamos y la testeamos durante meses para cumplir con el 5011. Después confiamos en los resolutores en sí pero si había un problema, nosotros podíamos estar ahí para resolverlo.

En ese punto, si nosotros tenemos la automatización para implementarlo todos los años y ese proceso mejora, nos quitaría la carga de los operadores que mantienen los resolutores actualizados con llaves y creo que el éxito aquí implica testear, testear y testear, y que el software esté actualizado. Esa es mi sugerencia más importante.

RUSS MUNDY: Gracias, Joe. Ahora vamos a escuchar los comentarios de Warren en general desde la perspectiva de la operación de los resolutores públicos, que es muy conocida por todos nosotros.

WARREN KUMARI: Soy Warren Kumari, de Google. No tengo mucho para agregar, más allá de que es muy conocido que nosotros utilizamos un software personalizado y que no utilizamos la RFC 5011. Implica mucha complejidad. Es muy bueno para sistemas automatizados pero tenemos muchas personas que cuando se publica la nueva

llave, la chequeamos, hacemos un clúster, nos aseguramos de que funcione bien y luego hacemos el traspaso de la llave manualmente.

Muchos de nosotros, no en Google pero sí aquí, que nos estamos preguntando si la 5011 es el modo adecuado de hacer el traspaso de las llaves. Quizá tenemos que tener algo que sea un poco más rápido, que sea una solución mejor. Mi comentario lo voy a detener aquí porque cuando llegue el momento de las preguntas, tengo preguntas para Matt.

RUSS MUNDY: Muy bien. Gracias, Warren, Joe, Jacques y Matt. Ahora ya llegó el momento de preguntas y respuestas. Warren tiene una así que le voy a dar la palabra. Mientras tanto, ustedes piensen en sus preguntas y se las vamos a poder formular.

WARREN KUMARI: Volvemos por favor un par de diapositivas atrás. Yo quizá no estoy entendiendo algo. Si el pensamiento era que quizá este unbound se actualiza para solucionar esta vulnerabilidad, lo que no entiendo es por qué vemos tantas fuentes únicas dado que se actualizó a partir de algo que no utiliza RFC 8145. Ya lo entendí entonces. Es bastante obvio cuando empieza a hacer preguntas

delante de mucha gente y todos dicen: “Sí, sé adónde quiere llegar”.

RUSS MUNDY: Muy bien. Peter Koch.

PETER KOCH: Soy Peter Koch, DENIC. Tengo un par de preguntas. Tengo un comentario para Matt porque escuché rumores esta semana. Sé que es una mala presentación del comentario. ¿Podría aclarar qué pasaría si el traspaso se pospusiese? ¿Podría clarificar qué pasaría si se postergase incluso más? Internet no dejaría de funcionar.

MATT LARSON: Yo no creo que posponerlo haga que Internet deje de funcionar.

PETER KOCH: Quizá puedo clarificar el rumor. Hay gente que tiene la percepción de que la implementación era urgente y que tenía que ocurrir. Tenemos que dejar registrado que eso no es así. Es posible que el feedback de la comunidad nos diga que hay que esperar hasta que ocurra alguna otra cosa y luego podemos revisar el plan y quizá hacerlo un poco más adelante. Gracias.

MATT LARSON: Creo que la preocupación aquí es que cuando la clave se firmó, se dijo que se iba a implementar en cinco años. Luego hubo la transición de la NTIA, etc. y hubo que postergar. El riesgo central es una pérdida de confianza en el material de la llave a lo largo del tiempo. ¿Esta concesión es más riesgosa para la reputación de DNSSEC, que nosotros implementemos y que haya cosas que dejen de funcionar, o que no implementamos y la gente diga que esta clave es vieja y que huele a viejo? ICANN tiene un periodo de comentario público y obviamente hay que pedirle a la gente que venga y dé su comentario.

JOE ABLEY: A mí me parece que es un error pensar en esto como un riesgo o una evaluación de riesgo o una ecuación de riesgo de un solo lado porque también hay riesgo en no implementar la llave. En cualquier sistema encriptado, la capacidad de remplazar la llave va de la mano con las precauciones de la seguridad física. No se puede tener una seguridad física y pensar que es perfecta. No hay blanco y negro. Siempre hay unos grises. Estamos evaluando el riesgo de no tener ninguna experiencia operativa al traspasar la llave que, dicho sea de paso, es importante. Podría ser un riesgo menor que algunos sistemas vayan a dejar de funcionar pero se pueden reparar rápidamente. El riesgo de no traspasar la llave es que no sabemos nunca cómo hacerlo. Si lo hacemos

rápido, va a ser un lío mucho más grande que el potencial que vamos a enfrentar ahora.

WARREN KUMARI: Yo estoy de acuerdo con Joe pero debo decir también que si tenemos que traspasar la llave con rapidez, es un proceso completamente diferente a este. Si tenemos que hacerlo así es porque perdimos confianza en la llave, en cuyo caso no podemos usar la 5011 porque no podemos confiar en la llave anterior. Pero estoy de acuerdo. Lo que originalmente esperábamos que podríamos hacer es publicar el DURZ y cada dos meses cambiar a una nueva llave para poder testearla. Después de eso, cada año o cada dos años, cambiar a una nueva llave para poder testearla. Pero por distintas razones no lo hicimos. El primero va a ser un rol de entretenimiento. Peter debe de estar cansado de esperar de pie.

MATT LARSON: Warren, no sé a quién se refiere con “nosotros”. Estamos trabajando en implementar esto en el 2010 y nuestra intención nunca fue implementarla como usted dice. Hay alguna gente en la comunidad que habla de cambios frecuentes pero esa nunca fue la intención. La declaración práctica para la KSK dice después de cinco años, pero no dice entre cinco y seis años. Simplemente dice después de cinco años.

ORADOR DESCONOCIDO: Matt, ¿podría avanzar sus diapositivas a la lista de los AS? El que tiene 41.482 fuentes individuales es AS 55836. La cantidad de archivos es básicamente cero. Lo que dice en un sentido real es que lo que viene a partir de la RFC 8145 es complicado en modos que nosotros no entendemos. En septiembre nosotros dijimos que lo entendíamos pero de algún modo nuestro apetito de riesgo no está cambiando. Nuestra confianza en la RFC 8145 está creciendo exponencialmente. Estos son datos que no reflejan los resolutores que validan y si no validan, no importa el traspaso.

ORADOR DESCONOCIDO: Aquí hay un panorama un poco más grande que refleja el entorno más grande y si hay un conjunto de validaciones esto es incluso más inexplicable. Lo que estoy diciendo no es que cambie nuestro apetito de riesgo pero nuestra confianza en la señal del 8145 se está erosionando. Es decir, parece que esta señal no los ayuda a tomar decisiones razonables. Llevamos siete años con este traspaso y podríamos tardar otros siete años más. Francamente, no veo el punto. En algún punto ocurrirá algo que nos obligará a realizar el traspaso y si no lo planeamos, estaremos en problemas.

Los aliento, también lo haré en mis comentarios, a que se produzca el traspaso tal como está planeado. También los

aliento, pero esta va a ser la próxima conversación, a hacerlo en forma regular. Cuando no hay nada regular, yo diría 12 meses como documento base para el próximo debate. Ciertamente, yo diría que implementen este año, que traspasen este año y que sigan haciéndolo todos los meses de octubre. Gracias.

PETER KOCH: Tengo una segunda pregunta. Escuché que hay gente que habla de traspasos regulares. Uno de los beneficios es que esto ayudaría con un mecanismo que funcione en caso de que necesitemos un traspaso de emergencia. Yo entiendo que la 5011 es incompatible con el traspaso de emergencia. Nadie puede escuchar que usted está asintiendo con la cabeza.

ORADOR DESCONOCIDO: Todos estamos de acuerdo. Warren y yo queremos ir más allá de la 5011. Creo que necesitamos un nuevo estándar.

PETER KOCH: Necesitamos otra explicación y otra motivación.

ORADOR DESCONOCIDO: Creo que hay que remplazar la 5011 completamente.

PETER KOCH: Tenemos que comunicar esto al operador de resolución. Quizá no tenemos que estar todo el día trabajando en esto. La preparación de emergencia no es lo que debe motivarnos.

MATT LARSON: Yo no soy parte de la PTI. Soy parte de la oficina de la CTO. Todos en ICANN org querríamos estar en una posición en la que tuviésemos una configuración diferente y no tengamos que usar la misma metodología para el traspaso regular. Yo preferiría claves standby en los ápex y esto significa que las llaves actuales, cualquier cosa que hagamos nosotros para generar una llave con la infraestructura actual se va a enfrentar a la llave actual. Si nosotros pudiésemos tener otra forma de generar claves, vamos a poder hablar de llaves múltiples en el key set y estar en una posición de implementarlas sin problemas.

Ahora, la 5011 tiene problemas en cuanto al tamaño de la ápex key set pero tenemos trabajo aquí tanto en términos de protocolo como en los procedimientos operativos. Creo que podemos ver una manera de hacer la implementación de emergencia, incluso una implementación planificada, de manera más sencilla.

FREDERICO NEVES: Soy Frederico Neves, de NIC.br. Buena presentación, Matt. Me gustaría estar de acuerdo contigo, además del hecho de que ya comenté en el registro público. Ir en esa dirección, como dijiste, o tener claves adicionales públicas, va a implicar pensar en un cambio en el algoritmo porque nosotros tenemos un problema con las claves adicionales y el algoritmo actual dentro de las claves que estamos usando. Esto es probablemente lo próximo en lo que tengamos que pensar, utilizar una tecnología que use claves públicas mucho más pequeñas.

WARREN KUMARI: Yo quería responder a las preguntas de Peter. Hay dos tipos de traspasos de emergencia. Uno donde alguien publica accidentalmente la clave en el New York Times, en cuyo caso uno entra en pánico y hay que decir que aquí la 5011 no funcionará. Hay otro tipo de traspaso de emergencia donde queda en claro que lo que estamos usando no es lo fuerte que pensábamos. Hay gente que dice que esto puede ocurrir para el SHA1 y quizá queramos implementarla pero un par de semanas está bien o incluso un par de meses. Dependiendo de cuál es el nivel de emergencia, la 5011 puede funcionar o no.

Para el próximo comentario, hemos estado hablando de cuestiones de implementaciones diferentes que no son del 5011. Con esto podríamos tener claves que, al no publicarlas en la

zona ápex, sería perfectamente razonable publicar llaves extra como registros de zona DNS, pero no firmarlas y no como el DNSSEC actual y el keyset. Esto implica un registro adicional y si tenemos siete llaves, decimos que esta es la lista y que hay que buscar los nombres. Así no sabríamos cómo traspasarlas.

ORADOR DESCONOCIDO: Hola, Matt. Estoy muy contento de que esté a cargo de esto. Quiero recordar que el servidor puede notificar a algunos de estos operadores de red y tenemos un sistema existente por si quieren recibir alertas sobre estos temas, incluso si esa alerta es que los resolutores están haciendo algo raro y no que usted está usando la clave de 2010 y que podemos ayudarle. Yo tengo los números de la diapositiva. Tenemos un 30-40% que sí quieren recibir informes y nosotros podemos ayudar con el proceso de notificación.

MATT LARSON: Fantástico. Vamos a intercambiar los mails. No lo tengo en la diapositiva pero otra táctica es ir en la otra dirección que es ir a buscar los datos. Tenemos buenos datos de APNIC. Podemos empezar por arriba y determinar la gente que tiene información. Podemos chequear y llegar a un punto en que digamos: "Podemos no saber quiénes no están listos pero sabemos

quiénes sí están listos". Podemos ir a hablar con ellos, a ver si nos ayudan.

RUSS MUNDY: Creo que estamos casi llegando al final de nuestro horario. Si hay una última pregunta urgente… Sí, adelante.

ORADOR DESCONOCIDO: Soy fellow de ICANN. Tengo un par de preguntas que quizá sean básicas. ¿Cuál es el rol de las claves antiguas en el traspaso? ¿Se usarán para validar las claves nuevas? Si es así, ¿no habrá un compromiso en alguna de ellas? Si existe, ¿hay algún plan de mitigación disponible o no?

WARREN KUMARI: Sí. El protocolo actual es el RFC 5011. Funciona de la siguiente manera. La clave antigua firma la clave nueva. Cuando se empieza a creer en la nueva, ya no se usa la antigua y entonces se revoca o se deja de tener confianza en ella. No obstante, cualquiera de estos protocolos tiene el problema de que si la clave antigua se vio comprometida, hay otro proceso, no sé si está muy publicitado. Qué pasa exactamente si se compromete la clave y hay evidencia al respecto. Sé que nos han dicho que habrá sesiones de emergencia para generar la nueva clave, etc. ¿Cómo se va a distribuir esto? No lo sé. En un acontecimiento así

no es cuestión de ir a www.iana.org y firmarla porque no estaría bien. Debe haber un proceso bien documentado y posiblemente probado si es que hay un compromiso de la clave, que no sea el pánico.

RUSS MUNDY: Con esto creo que debemos cerrar y dejar la sala. Quiero agradecer mucho a Matt Larson, a Warren Kumari, a Joe Crowe y a Jacques Latour por participar en el panel. Un agradecimiento especial a Kathy Schnitt, quien ha administrado esta sesión sola, en la que normalmente hay más de una persona. Has hecho un trabajo fantástico, Kathy. También has ayudado en la organización. Muchísimas gracias. Bueno, vamos a publicar el programa para la ICANN62 probablemente en un mes. Nos interesa saber qué piensan. Piensen en ideas para el próximo taller. Nos vemos entonces. Gracias.

[FIN DE LA TRANSCRIPCIÓN]