ABU DABI – Taller sobre el DNSSEC – Parte 1
Miércoles, 1 de noviembre de 2017 – 09:00 a 10:15 GST
ICANN60 | Abu Dabi, Emiratos Árabes Unidos

RUSS MUNDY: Buenos días a todos. Bienvenidos al taller sobre despliegue del DNSSEC. Soy Russ Mundy. Aquí está Jacques Latour, del registro CA, que es nuestro anfitrión hoy. ¿No me oyen bien? Entendí que era uno de esos micrófonos que hay que comérselos. Bueno, vamos a tener una sesión hoy que trae nuevos rostros. Algunas personas que nunca antes vinieron al taller. Queremos que sea una actividad lo más interactiva posible. Todos debieran tener el programa frente a ustedes. Al dorso del programa está el ticket para el almuerzo, si quieren quedarse a almorzar con nosotros. El almuerzo es cortesía de nuestros auspiciantes. La diapositiva con los auspiciantes la vemos en pantalla: Afilias, CIRA, SIDN, .CA y el registro Afilias. Muy buenos auspiciantes. Esta es la parte importante. Si les parece, vamos a darles un aplauso a nuestros auspiciantes por el almuerzo gratuito del taller de DNSSEC. Muy bien. Dan York es el que suele ocuparse de este taller pero hoy, en lugar de ser el roadshow de Dan York es el roadshow de Russ. Yo soy Russ. Jacques va a hacer la presentación que suele hacer habitualmente cuando comienza. Para eso le paso la palabra a Jacques.

JACQUES LATOUR: Vayamos a la agenda. Hoy haremos primero las presentaciones estándar del mundo. Luego un relato sobre lo que es DNSSEC y luego las actividades que se centrarán en las regiones. El segundo taller describirá el estado actual del traspaso de la llave de la zona. Vamos a hablar un poquito al respecto. Luego tenemos ese gran cuestionario sobre el DNS y el DNSSEC. Sé que muchos de ustedes sabrán cómo manejarlo. Después del almuerzo tenemos un par de presentaciones sobre cuestiones relacionadas con el DNSSEC. ¿Empezamos? La primera diapositiva.

Vamos entonces a dar una vuelta al mundo. Yo tengo el control aquí. Este es el informe del estado del despliegue DNSSEC 2016. En este informe se describe muy integralmente la situación y la iniciativa hasta 2016. Dan y los demás hicieron un muy buen análisis. Si quieren enterarse de qué es DNSSEC, es un buen lugar para comenzar, con muchas referencias y otros vínculos para adquirir más conocimientos sobre el DNSSEC.

¿Quiénes de ustedes asisten a este taller por primera vez? Conviene saberlo para manejar la velocidad, para saber si conocen o han oído sobre este tema o no. Voy a ir más despacio. Esto está basado en el APNIC Lab. Es un gráfico de la validación en el mundo del DNSSEC. Cuando vi esta diapositiva, este gráfico

por primera vez, noté esta caída alrededor del mes de julio. Sospecho que ustedes tendrán comentarios al respecto.

GEOFF HUSTON: El backbone… ¿Cuándo fue que se activó? ¿Hace un año? En India BSNL es muy grande. Tiene muchos clientes. En julio lo desactivaron y ese fue un glitch notable en las cifras por la desactivación. El abordaje típico es analizar por qué. Dos razones primarias es que quizá no lo hicieron a propósito, quizá por accidente, y otra explicación posible que es más deprimente es que anticipaban el cambio de la llave e hicieron eso. No sé cuál es la explicación. Si alguien de la India y conoce la situación de BSNL, por favor, infórmenme. Eso es todo lo que sé.

JACQUES LATOUR: ¿Alguien de la India en la sala?

ORADOR DESCONOCIDO: Sí. Yo soy de la India pero no tengo ninguna información al respecto. Lamentablemente no tengo información.

JACQUES LATOUR: Aquí tenemos una acción a concretar. Enviar un mail. No sabemos cuál es la situación. Más allá de eso, el crecimiento ha sido bastante constante. En la región, la primera que tenemos es

Sudáfrica con el 38% de DNSSEC y luego baja hasta un 2%. Lo bueno es el número de la dependencia sobre el DNS de Google. Hay algunas regiones que tienen una situación mejor que otras de infraestructura. Hoy día depende casi todo de Google para hacer DNS y eso viene bien.

Con respecto a la validación en Asia del DNS tenemos a Iraq con un 57% y un 25% de DNS de Google, lo que está bien. Baja a un 0% casi en Kuwait. Ahí hay trabajo para hacer. Lo podrán hacer antes o después del cambio de la llave que requerirá más validación. Esa va a ser una buena oportunidad.

Con respecto al despliegue de los TLD en el mundo, seguimos con un 90% de la totalidad de los TLD en la zona raíz firmados. Un 4% de los de segundo nivel detrás están firmados. En general, un 13% de los usuarios están validando. Estos son números clave, cifras a recordar. Deberían recordarlas. Esta información está basada en la investigación de Rick Lamb de DNSSEC Stat. Imagino que va a llevar un tiempito lograr el 10% que falta pero es un trabajo en curso.

Los TLD en número de dominios firmados, estos son los TLD que tienen más dominios formados. .NL con un 48% de los dominios firmados, 2.8 millones de 5.7 millones de dominios. Eso está bien. Seguido por Brasil con un 23%. Estos son números totales de dominios. Casi un millón de dominios firmados. Luego baja.

En .CA tenemos 500.000 y tendríamos que apuntar al millón. Lo nuevo es que Rick está haciendo un seguimiento del número de dominios. Si quieren saber más, entren a este sitio y ahí van a tener más estadísticas. Si quieren hablar con Rick, está por ahí.

Ahora estamos hablando de la implementación de DNSSEC en los TLD en la región. Tenemos cinco estados distintos. Dan hace un seguimiento de cada uno de los TLD según estén experimentando internamente con DNSSEC o hayan hecho un compromiso público de desplegarlo en su zona o de que esté firmada pero no en operación. Tienen la tecnología para firmar. La DNS está en la raíz, está firmado, hay una cadena de confianza pero ninguno de los registradores acepta un registro DS todavía. Luego operativo significa que acepta delegaciones totalmente firmadas.

Esto en su mayor parte es manual porque no funcionó el cambio de la llave. Está basado en la información de los TLD. Cuando se planea hacer algo nos tienen que informar, así podemos actualizar nuestra información. Así es como funciona. Con esto Dan generó el mapa del mundo con los estados actuales. En los últimos cinco años hemos avanzado bastante. Creo que deberíamos comparar hace un año o dos. Podemos decir que el avance ha sido bastante bueno. Antes era todo rojo y amarillo. Ahora está mucho mejor. Para comentar, hay 46 registros DS en la raíz. Eso significa que están trabajando con el registrador para

aceptar el DNSSEC. La clave es un desafío para algunos TLD y es algo que tenemos que estudiar.

La región africana. Aquí vemos el estado actual de la región por colores. Guinea-Bissau, se firmó en octubre. Sudáfrica, .SA, entró en estado operacional. Es bueno. Son cosas a recordar. Usted tiene que recordarlo. En Asia, .SA, entró en estado operacional. Fantástico. Deberíamos aplaudirlos. Es bueno. Más o menos el mismo escenario, 24 en operacional, 17 en la raíz. ¿Hay alguien aquí que tenga el DS en la raíz? ¿Qué es lo que les impide entrar en estado totalmente operacional u operativo? ¿Hay alguien aquí de alguno de estos TLD? ¿O es solo una cuestión de que no estamos totalmente actualizados en la operación? Bueno, vamos a preguntar después, cuando la gente esté más despierta.

En Europa tenemos las Islas Aland, .AX. Las agregamos en agosto. Falta Italia. No sé cuáles son los otros dos. ¿Qué países son? Bueno. Podemos avanzar. Argentina, en América Latina, todavía tiene algo de trabajo por hacer. Es más o menos la misma situación. Bermudas se agregó en junio. Aquí queda cierto trabajo por hacer. Groenlandia firmó. No tiene el DS en la raíz pero hablamos con alguien de ese país y sabemos que están trabajando. No sé si les interesa este material, este tema, pero todos estos mapas e imágenes, si ustedes se suscriben a esta lista, pueden recibirlos mensualmente. Todo el conjunto de mapas con los cambios. Si ustedes se dedican a investigar el

DNSSEC, ahí tienen información que se basa en las actualizaciones que hace Dan.

Hay un proyecto de historia del DNSSEC en curso que pueden consultar, entender el estado actual. Hay una URL. Cómo se trabaja, pueden saber qué se está haciendo. Si tienen contenidos o cosas que puedan ser útiles para el despliegue del DNSSEC, ustedes pueden subir contenidos y contribuir a este proyecto de la historia del DNSSEC. Eso es todo. ¿Hay alguna pregunta?

JULIE HEDLUND: Tenemos un comentario en Adobe Connect que es de Abdalmonem Galila. Pido disculpas si no lo pronuncié correctamente. Son dos comentarios. El primero es con respecto a los datos de los mapas, si se pueden tener en cuenta, se pueden considerar los TLD con IDN. El segundo comentario dice: "Pienso que estos mapas son para TLD en ASCII y con IDN. ¿Podríamos diferenciar cuáles son de ASCII y cuáles son IDN, para que sea más claro?"

JACQUES LATOUR: Creo que esa pregunta se la podemos hacer a Dan York. Como decía, gran parte del trabajo es manual y depende de la comunidad o del estado. Si nos acercan la información,

seguramente podemos hacerlo. Pongo a Dan como voluntario para hacer este trabajo. La siguiente pregunta.

ORADOR DESCONOCIDO: Soy [inaudible], del registro .ID. Vi en el mapa que Indonesia, por el registro del DS en la raíz, ¿cuál es el criterio?

JACQUES LATOUR: ¿Cuál es el criterio para el DS en la raíz? Significa que se firmó la zona con DNSSEC y que se le pasó el registro DS a la IANA para ponerlo en la raíz pero si su registratario quiere firmar el dominio, o firmó el dominio, no se puede poner el registro DS en la zona porque el traspaso todavía no tiene soporte. No se hizo el traspaso. Se necesita EPP para hacer DNSSEC o se necesita una interfaz web u otra cosa.

ORADOR DESCONOCIDO: ¿Nos podría dar alguna URL que nos firme de cómo dar soporte sobre esto para otros TLD?

JACQUES LATOUR: ¿Al registro?

ORADOR DESCONOCIDO: Sí, al registro.

JACQUES LATOUR: ¿Utiliza un tercero?

ORADOR DESCONOCIDO: Nosotros usamos parcialmente un tercero pero también nos ocupamos de estudiar el DNSSEC en un estado de desarrollo. No estamos totalmente operativos en el despliegue. En este momento estamos recurriendo a un tercero.

JACQUES LATOUR: Entonces usted tiene que pedirle a ellos que les den soporte.

ORADOR DESCONOCIDO: Sí, tenemos que hacerlo.

JACQUES LATOUR: Ese es el camino.

ORADOR DESCONOCIDO: Le hemos pedido al registrador que soporte DNSSEC pero no todos los registradores tienen soporte pleno.

JACQUES LATOUR: ¿Soportan EPP con DNSSEC? Técnicamente tendría que estar operacional. Si es un registrador y no lo soporta el registrador,

esa es otra cuestión. Si usted soporta DS o la clave de DS a través de EPP tendría que estar bien.

ORADOR DESCONOCIDO: Sí. En este momento tenemos 15 registradores pero quizá 7 u 8 nada más tienen soporte pleno para DNSSEC. El resto no. El TLD es Indonesia, .ID.

JACQUES LATOUR: Entonces está en verde. Está en verde. Deberíamos poner un color distinto cuando todos los registradores soporten DNSSEC. Ofrezco a Dan como voluntario para que trabaje en esto. ¿Hay alguna otra pregunta? Esta es una sesión interactiva. Cuanto más pregunten, más vamos a poder sacar de la sesión. Gracias. Ahora tenemos el taller 1, la discusión del panel de las actividades de DNSSEC. El moderador soy yo. Luego tenemos a Raed Alfayez, que nos va a hablar sobre la implementación del DNSSEC y los nombres de dominio saudíes.

RAED ALFAYEZ: Hola a todos. Soy Raed Alfayez. Yo di esta presentación en el Tech Day. Espero que no les resulte aburrida a muchos de ustedes. Achiqué un poco la diapositiva para ahorrar un poco de tiempo. Soy del SaudiNIC, donde desplegamos los TLD en Arabia Saudí, .SAUDIA e IDN. Eso ocurrió este año. Las letras en árabe no

se están viendo bien. No sé muy bien por qué. Están en los dos idiomas, en árabe y en inglés. Las letras están separadas, no sé muy bien por qué.

Empezamos con DNSSEC en tres fases. Nuestra metodología era dividir las tres fases. La primera es la fase de seguimiento y allí monitoreamos los RFC, las herramientas, los software y también esperábamos a que estuviesen maduros para poder ingresar sin errores ni cambios radicales en el futuro porque hay que tener un despliegue adecuado para Arabia Saudita.

En el 2015 iniciamos el trabajo. Hicimos un estudio completo donde incluimos varios países, los países principales que usan DNSSEC. Luego hicimos un mapa de despliegue para saber cómo lo íbamos a tratar en detalle. Ejecutamos el plan durante la fase de ejecución, el primero fue en 2016 y el tercero este año. Ya los completamos a los dos.

Nuestra metodología fue paso a paso. Nos fuimos focalizando un poco más y fuimos aprendiendo a partir de los test que hicimos. Establecimos que los nuevos términos que encontrábamos en el DNSSEC, los íbamos a ir desplegando. Hicimos el estudio y el estudio terminó con el despliegue en tres etapas. La primera fue ganar experiencia dentro de SaudiNIC y dentro de nuestra organización, la SITC y también dentro de los proveedores de telecomunicaciones. La segunda fase fue generar un prototipo.

Empezamos a generar los IDN en una zona muy pequeña. La firmamos y permitimos que nuestros clientes también carguen sus registros de DNS, hagan estadísticas y que tengan una información para que luego puedan desplegarla de modo correcto y seguro en todos sus dominios y en los dominios de sus clientes.

Hicimos una lista de correo interna. Tenemos mucha gente suscrita. Cualquier cosa que quieran preguntar o leer, lo pueden hacer en esa lista. Se pueden también tomar decisiones en cuanto a cuáles son los parámetros para el DNS, los parámetros para el cambio de la KSK. Luego operamos directamente para nuestros clientes. Hicimos capacitación. Creemos que el entrenamiento es un factor clave para DNSSEC. Hicimos dos sesiones de entrenamientos. El primero es un curso de tres días. Hubo 25 participantes de 11 agencias de gobierno junto con preparadores de las TIC. El segundo ocurrió en octubre. El tercero en mayo de este año. Lo expandimos un poquito más. Allí hubo 41 participantes de 29 agencias de gobierno y operadores de TIC, y algunos bancos también. Luego hicimos un evento de un día en mayo inmediatamente después del entrenamiento. Allí hubo 120 participantes de Arabia Saudita. La mayoría de ellos son jefes de departamentos de IT o de seguridad, de operaciones. Todos estaban interesados en DNSSEC. Todos

estos entrenamientos los hicimos en coordinación con RIPE y con la ICANN.

Estas son algunas imágenes de la sesión de entrenamiento. El de la derecha fue el primero. El de la izquierda fue el segundo. Este fue el evento público. Entregamos certificados a los entrenadores para que estén orgullosos de tener esta tecnología. Estos son algunos de los entregables. Tenemos declaraciones para SaudiNIC, tanto en árabe como en inglés, que son compatibles con la RFC. RFC 6841. Esta es la declaración de práctica de DNSSEC. Hicimos también la configuración del DNSSEC.

Hubo varios procedimientos sobre cómo abordar el DNSSEC, cómo hacer la ceremonia de la llave, cómo instalar la llave, qué hacer si en alguno de los sitios ocurre un desastre, muchos procedimientos. También hicimos una evaluación de riegos para DNSSEC, en caso de que haya algún problema crítico con las clave, con los passwords o con el firmante, qué es lo que se debe hacer si uno de los firmantes tiene un problema, qué se debe hacer en ese caso. Hay una tabla de gestión de riesgo donde se muestra qué hacer. Hicimos un sitio web y las herramientas y ambos están en árabe y en inglés. También nos pusimos completamente operativos.

Esta es la configuración de nuestro DNSSEC y de nuestra infraestructura. Como ven, tenemos una sala de DNSSEC donde hacemos la instalación y la generación de la llave. Allí almacenamos el HSM junto con las tarjetas. Después de que lo generamos, nadie puede entrar ni salir de la sala salvo que se siga un procedimiento específico establecido para eso. Tenemos una sala de backup. Tenemos dos sitios donde está el firmante, el máster y los servidores públicos. Estos son los procedimientos que fuimos generando. Lanzamos la operación de DNSSEC en .SAUDIA como prototipo en junio de 2016 y fuimos el primer país DCC que tiene DNSSEC. Como les dije, invitamos a los ISP y a los DSP para que puedan participar en DNSSEC.

El lanzamiento oficial para ambos fue en junio y fuimos los primeros en la región de abrir el servicio para nuestros clientes. Hicimos una ceremonia de generación de la raíz. Firmamos la raíz y firmamos los registros para IANA, actualizamos el registro para iniciar el DNS para nuestros clientes y también hicimos promoción en los diarios y en Internet a través de la lista de correo y generamos un sitio en árabe que es www.dnssec.sa, que está en árabe y en inglés.

Este es el mapa de despliegue que nos muestra que .SA y .SAUDIA están en verde. Estas son imágenes de la generación de la llave. Tenemos también ahí un auditor y tenemos al jefe del departamento de seguridad. Tenemos también allí algunos

expertos en DNSSEC. Este es el sitio web que pueden ver. Esta es la parte en árabe. Aquí hay algunas imágenes. Tenemos que mostrarle a la gente que DNSSEC es fácil de entender. El contenido tiene que estar en su idioma porque tienen dificultad para entender el inglés. Si el usuario no tiene conocimientos de inglés, lo puede leer en árabe y le va a resultar más fácil para él o para ella.

Este es el verificador del registro. Si uno pone la clave y el registro de DNS, la herramienta va a verificar si coinciden o no o ponemos también el nombre de dominio y la herramienta va a buscar el registro de DNS de la llave del archivo de zona y le va a ayudar a generar lo que haga falta. Tenemos hasta fin de septiembre. Tenemos más de 50.000 nombres de dominio. 55 que habilitaron el DNSSEC hasta ayer o el día anterior. 33 en .SA, 8 en .SAUDIA, 6 en .COM.SA, 6 en .NET.SA y 1 en .ORG.SA y 1 en .GOV.SA. Todavía tenemos que trabajar un poco más en el sector bancario para que desplieguen el DNSSEC lo antes posible.

Es decir, nuevamente, tenemos que hacer más concientización y promoción. Los números son muy bajos. Pero con suerte vamos a poder ir aumentándolo en el futuro. Tenemos que empezar a monitorear las mejores a los protocolos de DNSSEC y nuevas actualizaciones en la llave. También tenemos que tener los ojos puestos en la implementación de la llave, en el traspaso. Por eso debemos ir controlándolo. Quiero instarlos a que se focalicen en

la experiencia local porque hay que tener un laboratorio de testeo para testear el sistema, la aplicación y los parámetros para DNSSEC y monitorear y testear las herramientas. Para todo ello tiene que haber herramientas de testeo. No es solamente generar el archivo de zona raíz y publicarlo sino que hay que monitorear si las firmas siguen siendo válidas, hay que poner los dominios importantes en foco para que el archivo de raíz no se publique, que si hay algún problema en alguno de ellos, hay que tener automatización, especialmente en la ceremonia de generación de la raíz que no tiene que depender de humanos, porque los humanos cometen errores. Hay que dar herramientas, sitios web porque los usuarios pueden confundirse. Esta es la última diapositiva. Muchas gracias.

JACQUES LATOUR: ¿Hay alguna pregunta?

JOHN LEVINE: Esto es muy importante. Gracias. ¿Cuáles son los procesos que utilizan los registratarios para cargar las claves?

RAED ALFAYEZ: Se pueden loguear en nuestro registro y ahí subir su nombre de log.

JOHN LEVINE: ¿Hay alguna API?

RAED ALFAYEZ: No, es automático. Llenan el DS y hay una verificación.

JOHN LEVINE: ¿Cómo lo puedo preguntar mejor? Si yo soy un registrante con 20 nombres, ¿lo tengo que hacer individualmente?

RAED ALFAYEZ: Sí.

JACQUES LATOUR: Esa era mi pregunta. ¿Hay alguna otra pregunta? ¿Russ?

RUSS MUNDY: Gracias por esa excelente presentación. Han hecho un muy buen trabajo. Yo sé que este es el énfasis en DNSSEC pero me da curiosidad saber si tienen procedimientos de gestión de riesgo y si tienen en cuenta el flujo del contenido cuando los registrantes dan la información en los registros de DNS. ¿Ustedes tienen algún conjunto de procesos o procedimientos comparables con énfasis en el contenido de la zona en sí? Eso es lo que hace DNSSEC. Es decir, preservar y proteger y verificar el contenido de

la zona. Por eso mi pregunta es si ustedes tienen en cuenta las mismas actividades para el contenido de la zona.

RAED ALFAYEZ: Primero, si alguien quiere cargar este DS, nuestro sistema va a verificar que el DS coincida con la llave del DNS. Nosotros le vamos a dar una alerta y si la quiere ignorar, el usuario va a tener un mensaje donde dice que la gente no va a poder llegar al nombre de dominio pero en el futuro podemos tener alguna herramienta que mire en la zona raíz y que analice si las firmas son válidas o no. Esto está en nuestros planes. Espero haber respondido.

RUSS MUNDY: Tenemos que avanzar. Quizá se lo pregunte después. Julie.

JULIE HEDLUND: Tenemos una pregunta en el chat y también un comentario. La pregunta proviene de Zainab Al Farsi. ¿Cuáles son los desafíos principales que ustedes enfrentan?

RAED ALFAYEZ: Bueno, el desafío principal es generar un equipo de especialistas en DNSSEC. Este fue el obstáculo principal para nosotros porque la herramienta estaba pero teníamos que leer las RFC y entender

que si queremos construir un equipo, tiene que haber gente que entienda los distintos tiempos, los parámetros para el DNSSEC, porque están vinculados. Dedicamos cuatro meses para ver que si aumentamos el TTL, la firma tiene que tener relación con esto y este parámetro tiene que tener otra relación con un tercero. Es fácil para nosotros si alguien construyó una relación entre los distintos parámetros de DNSSEC, como una especie de fórmula. Si ponemos el TLZ3, esto va a haber que triplicarlo. Si va a haber un parámetro de fórmula, va a ser mejor. Podemos planear tener algo que ayude a los otros, generar experiencia local es el desafío principal que hemos enfrentado.

JULIE HEDLUND: Tenemos otro comentario que es de Abdalmonem Galila. "Muchas gracias, Raed, por utilizar el idioma árabe en la presentación. Usted está haciendo un buen plan de concientización al utilizar el idioma local".

JACQUES LATOUR: Gracias. El siguiente orador es Kadir Erdogan, de Turquía. Nos va a hablar sobre las actividades de DNSSEC en Turquía.

KADIR ERDOGAN: Buenos días. Soy Kadir Erdogan, del ccTLD .TR. Soy de Turquía. Les voy a dar una breve presentación sobre las actividades de

DNSSEC en Turquía. Van a ver que es un país muy colorido. Deberían ustedes ir a visitarlo si todavía no fueron. Turquía es un país con la mayor cantidad de conocimiento de DNS. Para el que no lo sepa, es el 8.8.8.8. Como ven, se puede encontrar esta configuración incluso en la pared de un departamento en Turquía. Esta foto se tomó hace algunos años cuando el gobierno estaba bloqueando las redes sociales con filtros de DNS. Todos aprendieron en el país cómo configurar sus DNS. Yo sé que esta es una presentación de DNSSEC pero en Turquía no hay muchos ISP con DNS. Por eso es importante. Al filtrar el DNS, el gobierno de hecho nos ayudó. La gente conoce el DNS de Google.

Esta es una breve historia de NIC.TR, que es el ccTLD. La primera conexión se estableció en 1991. En 1995 se empezó a monetizar. En el 98 establecimos un grupo de trabajo de DNS. Es un modelo de gobernanza temprano de múltiples partes interesadas. Todas las partes deciden cómo se debe regular. En 2003 establecimos aplicaciones web, aplicaciones de web, de documentos, de procesamiento, completamente automatizadas.

En el 2006 implementamos IDN. Son seis letras que no están en ASCII. Era más fácil para nosotros. No es como el idioma árabe. En 2008 implementamos un sistema de registro-registrador. No es EPP sino que está basado en API. En 2010 se publicó una

norma. Tuvimos un conflicto con el ministro de transporte y comunicación. Todavía estamos negociando.

Sobre el DNSSEC en Turquía, nadie lo conoce. A nadie le importa. No es que no seamos nadie. Trabajamos duro nosotros para que se conozca. El estado actual, .TR todavía no está firmado lamentablemente. Ninguno de los grandes operadores valida. No es que sean los operadores grandes los que no validen sino ningún operador valida. Los que toman las decisiones no tienen conocimiento en Turquía. No conocen qué es DNSSEC pero hay aspectos positivos. Tenemos intenciones de llegar a la firma. La comunidad técnica habla sobre el tema. Tenemos varios pedidos de titulares de dominio para firmar sus dominios. Eso es bueno. Estamos organizando capacitaciones y talleres en el país.

¿Qué hicimos hasta ahora? La primera capacitación se hizo en 2014. Nosotros fuimos los organizadores y con el apoyo de ICANN y NSRC fue un taller técnico. Todos los estudiantes eran técnicos. El capacitador era Phil Regnauld, del NSRC. En marzo de 2016 hicimos una capacitación sobre DNSSEC en Estambul. Fue una capacitación internacional. La organizamos con RIPE en MENOG 16 con el apoyo de ICANN. Rick Lamb y yo fuimos los capacitadores. Otra capacitación tuvo lugar también en el 2016. Esa fue nacional. Estas capacitaciones fueron de cinco días. Muy técnicas, muy complejas. No es fácil organizarlas ni es fácil encontrar gente para capacitar. De hecho, DNS ya es un tema

específico y DNSSEC es aun más específico. No es sencillo encontrar a las personas correctas.

Organizamos otro taller en 2017 en el foro de DNS de Turquía. De hecho, fue el tercero. Un taller de medio día. Estas son fotos de los talleres. Ahí está Rick dando la clase. ¿A quién capacitamos? Hasta ahora hemos brindado capacitación a más de 50 personas técnicas, además de los responsables en las organizaciones, 20 del área de gobierno, ministerios, del ente regulador, del ejército; 10 de universidades; 10 registradores y 10 de los operadores de red.

Como decía, es muy difícil identificarlos pero tenemos un buen grupo en este momento. Debemos organizar más capacitaciones porque necesitamos expertos. El DNSSEC es una situación que no sabemos cuándo va a explosionar. Necesitamos expertos. Tenemos que saber cómo hablar con los jefes, con los que no son técnicos. Tenemos que tener conocimientos para presentarlo no técnicamente. Bueno, gracias. De paso, esa es mi voz. Eso es todo.

JACQUES LATOUR: Muy bueno. Es la primera vez. ¿Alguna pregunta para Kadir?

CHRISTIAN: Soy Christian. Soy del registro de los Países Bajos, .NL. ¿Dónde piensa usted que van a comenzar el DNSSEC, con los ISP, con los registradores?

KADIR ERDOGAN: Será con nosotros, con el ccTLD. Nosotros deberemos firmarlo primero y después los ISP.

CHRISTIAN: Seguimos el mismo modelo en los Países Bajos. Cuando comenzamos no había nada de validación pero hay que empezar por algún lugar y nosotros comenzamos con el registro.

JACQUES LATOUR: ¿Alguna otra pregunta? Geoff.

GEOFF HUSTON: Hace un año y medio vi que el uso del DNS público de Google había bajado significativamente. ¿Esto se debe a que los ISP han puesto interceptadores de DNS o a qué motivo?

KADIR ERDOGAN: No puedo darle la respuesta pero puedo conjeturar que el gobierno está interceptando. No sé en qué etapa está.

GEOFF HUSTON: ¿Esto promueve interés en encriptar o tunelizar para impedir esa intercepción? ¿Hay algún interés en esta tecnología para resolver este problema de intercepción forzada?

KADIR ERDOGAN: No sé cuál es la respuesta.

JACQUES LATOUR: ¿Alguna otra pregunta? Gracias. La siguiente es de Rajiv Kumar. Una actualización sobre el tema del DNSSEC en los registros.

RAJIV KUMAR: Buenos días a todos. Soy Rajiv Kumar, del registro de la India .NIXI. ¿Me oyen? Como decía, es una buena oportunidad para mí hacer una actualización sobre el DNSSEC en el registro .IN. Mi agenda es hablar del DNSSEC en el registro .IN, hablar de la participación de los registradores, cuáles son las acciones del lado del registro, los recursos para los registradores y el estado actual de la validación. El registro .IN adoptó DNSSEC en una etapa temprana. La zona se firmó en noviembre de 2010. Se hicieron programas para amigos y familiares, programas sencillos inicialmente para testear el entorno, jugar con el ambiente y si había algún bug, las personas acudían a mí para resolver las cosas. Durante un año hasta el 2011 se producían en un entorno de prueba. Cuando comenzamos a testearlo y eso

nos permitió a nosotros y a los registratarios tener una idea. Hasta noviembre de 2011 vamos a aceptar registros de DS.

Ahora la participación del registrador. Tenemos 121 registradores acreditados. De estos, 39 tienen habilitación con DNSSEC, incluidos los 10 principales. Ellos brindan servicios de DNSSEC a sus registratarios. Tenemos dos millones de nombres de dominio registrados y de estos dos millones, 1.287 están firmados a septiembre de 2017, que es menos del 1% pero estoy haciendo lo imposible para mejorar este porcentaje.

Hacemos sesiones con los registradores acreditados para alentarles a promover el DNSSEC. Hicimos una reunión presencial con ellos. Hicimos una presentación y también organizamos capacitaciones prácticas y talleres, programas de concientización para la comunidad técnica, los ISP, con la ayuda de ICANN y APNIC. Cada año lo hacemos en el grupo de organizaciones de redes. Tenemos proyectos diferentes. También tenemos en nuestro sitio web recursos a disposición de los registradores, add-ons disponibles en el sitio web del registro. El entorno también está disponible en nuestro sitio web.

En lo que hace a la validación, tenemos un investigador individual que ha compartido datos. Indicó esta investigación que hay 447 servidores de nombres de los cuales solo 34 validan

DNSSEC. 144 servidores de nombres conocen lo que es DNSSEC pero no lo validan. 299 no soportan DNSSEC. Este es el estado de la validación en la India. También soportamos nombres de dominio con IDN en la firma. Esta que ustedes ven en pantalla es un ejemplo. Muchas gracias. Si tienen preguntas.

JACQUES LATOUR: No sé si hay preguntas. Russ.

RUSS MUNDY: Gracias por su presentación. Me pregunto si podemos volver a la diapositiva de la validación. Creo que fue la anterior a esta. Me pregunto cómo identifican los nombres de los resolutores de validación.

RAJIV KUMAR: Se ha hecho una evaluación en la comunidad india y hay una herramienta que indica el estado de validación del DNSSEC.

JACQUES LATOUR: ¿Entonces ustedes piensan que hay más resolutores abiertos en la India?

RAJIV KUMAR: Sí. Esto es subjetivo. Tendría que hablar con el investigador individual, que es quien me dio los datos.

JACQUES LATOUR: ¿Alguna otra pregunta? Gracias.

JULIE HEDLUND: Hay una pregunta en el chat pero no está lista todavía. Abdalmonem Galila dice que no ha podido venir aquí en persona pero tiene su presentación en un clip de audio. Vamos a comenzar su presentación de audio. Él va a aparecer después para las preguntas pero en este momento está ausente.

RAJIV KUMAR: ¿Podría repetir? No entendí la pregunta.

ABDALMONEM GALILA: Yo soy gerente del ccTLD de IDN. También soy fellow de ICANN. Estoy en el grupo de trabajo sobre IDN. Mi presentación se referirá a los desafíos que presenta el despliegue del DNSSEC, los desafíos antes y después del despliegue y un poco sobre el script de automatización del DNSSEC, que se usa para firmar o refirmar la zona MASR. Desplegamos DNSSEC en 2015. Antes del despliegue del DNSSEC no teníamos idea sobre el DNSSEC y por lo menos debemos saber qué es DNSSEC y cómo funciona.

Escuchamos el término en el 2014 en la reunión de África por primera vez y desde entonces empezamos a pensar en DNSSEC, buscando información. Empezamos a asistir a talleres sobre DNSSEC. Tenemos dos entornos para los registros. Uno es de producción y otro de prueba, que utilizan las mismas herramientas que los registros, base de datos y demás pero todavía estamos buscando información sobre cómo funciona el DNSSEC.

En nuestro entorno de prueba hacemos resolución validada del servidor. Estamos recabando la información para hacer despliegue del DNSSEC en nuestro entorno de producción. El de prueba en nuestra versión del software de registros tiene características para edición de registros de los dominios hijo. Utilizamos el software CoCCA. Subimos el software al entorno de producción. Uno fue demorado por 10 minutos. Tenemos que sincronizar nuestro servicio. Para eso desarrollamos un servidor temporizado e hicimos todos nuestros servidores clientes.

Queremos asegurar las comunicaciones entre los servidores maestro y esclavo. Entonces usamos firma de transacciones para garantizar la transición del entorno de prueba. También intentamos familiarizarnos a través de la identificación de problemas. Después del éxito de las pruebas queríamos replicar lo que hicimos en el entorno de prueba en nuestro entorno de producción. Llevó 15 minutos reconfigurar el entorno para

desplegar el DNSSEC. La mayoría de los problemas del DNSSEC están relacionados con los firewalls. Hay que asegurarse de involucrar a los administradores de seguridad y networking para que ellos puedan hacer los cambios requeridos antes de llevar el DNSSEC a producción.

Hay dos tipos de problemas de firewall. El primero, más común, involucra el TCP, el protocolo de control de transmisión. Hay una concepción equivocada entre los proveedores de firewall y los administradores de seguridad al respecto. Las consultas de DNS utilizan UDP. Las transferencias de zona también usan UDP. Lamentablemente, esta presunción no es totalmente cierta. Si no se recibe respuesta de la query UDP inicial o si hay demoras en la respuesta, la posibilidad de que haya un retraso en la respuesta es mayor con DNSSEC por el tamaño mayor de la respuesta. Para que el DNSSEC funcione correctamente, es obligatorio abrir el firewall. Es obligatorio abrir el firewall, tanto para TCP y UDP en el puerto 53.

El segundo problema está relacionado con el tamaño del reassembly del buffer. El estándar de DNSSEC dice que puede haber un problema potencial con las queries de TCP, que representan una mayor carga sobre los servidores de DNSSEC. El TCP es mucho más costoso en términos de proceso y para evitar demasiado tráfico TCP es obligatoria la extensión cero. El DNS 0 es uno de los mecanismos de extensión para el DNS, un

estándar. Es capaz de recibir las respuestas a través de UDP. Hay un límite de 512 bytes. Algunos firewalls no saben que la norma DNS 0 permite paquetes más grandes. Este paquete usa DNS 0 o bloquea paquetes que tienen más de 512 bytes, independientemente de la señalización DNS 0.

Otros firewalls permiten tamaños más grandes. Algunos proveedores requieren que el firewall se configure manualmente para esta tarea. En la capa de aplicación hay que conocer este estándar DNS 0 para tomar la decisión correcta acerca de si se va a enviar o no el paquete. Si no se puede testear en el firewall, si no se puede enviar la query del DNS hay que testear y se pueden recibir respuestas más grandes que las que envía el servidor DNS. Una manera de hacerlo es usar resolutores de DNS abiertos. Hay que testear y configurar el firewall para que permita el uso de DNS 0 y de paquetes de DNS más grandes de 512 bytes por UDP. Por último, pedirle al administrador del contacto que someta a los registros a la ICANN para chequearlos y registrarlos dentro de la zona raíz.

Después del despliegue del DNSSEC, debemos, por supuesto, saber cómo mantener nuestros sistemas en línea todo el tiempo. Hicimos un script para refirmar la zona después de generada del sistema de registro con la capacidad de buscar los errores para el administrador. El DNSSEC también introduce nuevas tareas operativas tales como el traspaso de la clave y la refirma de la

zona. Estas tareas tienen que ser realizadas a intervalos regulares. Cualquier cambio de la llave de nuevo debemos preparar el firewall para DNSSEC. La mayoría de los problemas con DNSSEC se vinculan con el firewall, por eso hay que estar seguro de que de nuevo se involucre al administrador de seguridad y redes. Nuestra misión ahora es implementar DNSSEC en nuestros cuatro registradores locales.

También vemos que uno de nuestros servidores de DNS no responde a queries de TCP. Las respuestas que se encuentran en general están en el alrededor de 1500 bytes. Incluso en ese caso, se excede rutinariamente las respuestas de DNS y hay muchos elementos de red que imitan esta respuesta. Para evitar eso, lo que hacemos es firmar la raíz con solamente el ZSK. La mayoría de los resolutores no tienen validación habilitada. También es una línea de la configuración. Próxima diapositiva.

La mayoría de nuestros registradores son ISP, por eso decimos que es difícil firmar sus dominios y ninguna región lo quiere hacer. También tienen otra fuente en la que el sistema se muestra un poco más estable y ellos se preguntan por qué tienen que cambiar el sistema actual. Otro de los problemas también es que se requiere más tiempo para resolver los nombres de dominio. Los dominios con firmas inválidas se van a bloquear. Tienen ataques pero los pueden mitigar. Los registrantes no tienen una idea sobre el DNSSEC y la interfaz de registrador no

tiene la capacidad de enviar registros de DNS al sistema de registros. No hay suficiente personal para monitorear y resolver problemas de DNSSEC.

Ahora les quiero mostrar la estructura de la firma de .MASR y del script automatizado. Este script fue escrito originalmente para los archivos de zona raíz nuevos y fue luego editado por el equipo de .MASR para que también se pueda firmar DNSSEC. La estructura del script empezó con ciertas variables de inicialización. Se generaron los archivos de registro…

JACQUES LATOUR: Aquí es donde termina este audio. Quiero saber ahora si hay alguna pregunta. Estamos justo a tiempo para hacer nuestro receso. Nos vemos en 15 minutos.

JULIE HEDLUND: Abdalmonem iba a venir para las preguntas y respuestas pero no sé si está aquí. Sí, aquí está. Si hay alguna pregunta.

ABDALMONEM GALILA: Nuestro script comenzó con una inicialización como los archivos de zona raíz que se generaron nuevos. Luego se aplicaron algunas verificaciones para los archivos de las zonas generadas para ver si se pueden aplicar consultas de DNS o no. Después

abrimos los archivos de zona raíz y los generamos a partir del registro. Es decir, si ustedes tienen muchas zonas que quieren generar, tienen que utilizar nuestro script y luego firmamos la zona y después de eso utilizamos las zonas de loop quizá para reiniciarlo pero no les recomiendo que lo reinicien si tienen alrededor de 800 nombres de dominio de IDN.

Esta es una captura de pantalla de nuestra automatización de script. La primera parte es la variable. La segunda es verificar si el archivo de zona raíz viene del anterior. Luego buscamos las zonas, vemos si tenemos múltiples zonas en DNSSEC y eso es todo lo que tengo para decirles. Gracias.

JACQUES LATOUR: Muchas gracias. ¿Hay alguna pregunta?

ORADOR DESCONOCIDO: Gracias por esta presentación. Primero remotamente y después físicamente. Tengo una pregunta. ¿Ustedes empiezan a aceptar registros de DNS para los clientes y pueden validar el DNS o no?

ABDALMONEM GALILA: A partir del día uno aceptamos registros de DS de nuestros registradores pero nuestros registradores no son muy conscientes, no conocen mucho el DNSSEC. Lo mismo ocurre con

nuestros clientes, que son registros, no registratarios. Solamente aceptamos de los registradores. Gracias.

JACQUES LATOUR: ¿Hay alguna otra pregunta? Muy bien. Entonces ahora sí estamos oficialmente en el receso. Nos vamos a reencontrar en 15 minutos, a las 10:30.

[FIN DE LA TRANSCRIPCIÓN]