SAN JUAN – Taller sobre las DNSSEC, parte 1
Miércoles, 14 de marzo de 2018 – 09:00 a 10:15 AST
ICANN61 | San Juan, Puerto Rico

JACQUES LATOUR: Bienvenidos al taller DNSSEC. Hoy tenemos streaming de audio únicamente. Todas las diapositivas están disponibles en el sitio web de ICANN para el taller de DNSSEC. Hay una dirección de email allí, donde podemos responder a sus preguntas. Las pueden mandar a esa dirección de email.

Bienvenidos entonces al taller DNSSEC. Este es el comité de programa. Como dije, nos reunimos semanalmente para planear el taller DNSSEC. Tratamos de tener contenido relevante con gente de todo el mundo que participa. Tenemos un almuerzo también, que está patrocinado Afilias, CIRA y SIDN. Ji, Christian, gracias. Necesitan al menos una respuesta correcta en el cuestionario que les vamos a hacer para que les demos el ticket del almuerzo.

El cuestionario hoy, hay que recordar la pregunta de esa reunión y también responder en el orden correcto. Ese va a ser el desafío de hoy. Tenemos un almuerzo patrocinado. El ticket está sobre la mesa. Lo van a necesitar para que les den su almuerzo.

Este es un esfuerzo conjunto con SSAC e ISOC, con el programa Deploy 360. Estamos trabajando conjuntamente. Tenemos a Dan York, que está a cargo de esto. Parece que funciona bien hasta ahora. La agenda de hoy tiene un día completo. Tenemos una discusión del panel sobre las actividades de DNSSEC. Comcast, CIRA, Nic.PR, Nic.BR, Fred y empresas que van a tener una hora allí. Por la tarde tenemos un par de presentaciones. Sentinel KSK, experiencia de validación en el CPE, CIRA sobre la implementación de HSM o la KSK, y Joe sobre la NTA. Después tenemos el quiz de DNS y un par de presentaciones de DANE. Es un taller más bien práctico. Va a ser una buena sesión. Luego vamos a tener una discusión del panel sobre la implementación de la KSK.

Como hacemos tradicionalmente, miramos la implementación de DNSSEC en el mundo. Cuentas. Dan York va mirando lo que sucede en el mundo con DNSSEC. Hay un informe detallado que está disponible en el sitio web de ISOC con el despliegue hasta 2016. Ese es el último reporte que tenemos. Estas son las estadísticas en el mundo. La tendencia fue en alza hasta julio de este año. No recuerdo el nombre. BNSL apagó la validación de DNSSEC. Allí pueden ver el impacto. Quizá lo vuelvan a activar después de la implementación. Esto es lo que muestra el impacto. Hay muchos usuarios. Es lamentable pero es lo que está pasando.

En términos de estadísticas por región, lo pueden ver aquí. La primera es el 58% que va hasta un 2% en el final. DNSSEC no es igual universalmente. Hay regiones o ISP que hacen más que otros. Seguimos teniendo trabajo allí para que los ISP validen.

Por otro lado, en la implementación de los TLD, ¿quién firma cada TLD? estamos en un 90% de TLD firmados en la raíz. Creo que ese número se va a mantener allí durante cierto tiempo. El último 10% toma el 90% del tiempo. Todavía tenemos un camino por recorrer. Tenemos 1.544. Estamos todavía haciendo un avance. Estas son las estadísticas de los dominios firmados. Este es un porcentaje de dominios firmados por TLD. Pueden mirar la diapositiva. Estas son más estadísticas. Ahí abajo está el link, DNSSEC stats. Si quieren pueden ir y verlo. No hay ninguna otra razón por la que mirarlos.

Algo que nosotros generamos son mapas globales con colores. Estos son los estatus de cada uno de los colores. Aquí ven el mapa global de DNSSEC. Recuerdo que hace siete u ocho años estos mapas estaban muy vacíos. No tenían mucho verde y tenían mucho parcial y mucho experimental. Ahora se ve bastante bien. Hay unas cuantas regiones en las cuales hay que trabajar. Vamos a llegar a eso pero ahora se ve bastante respetable. Todavía tenemos bastante en que trabajar. Tenemos que trabajar aquí. En África hay muchos cc que no están

anunciados o que ni siquiera están en la fase experimental para sus ccTLD.

Podrían ocurrir dos cosas. Si ustedes tienen la intención de implementar DNSSEC, tienen que notificar a Dan York o a alguien en el comité de programa, y así podemos actualizar el mapa, por lo menos con la intención que ustedes tienen de implementar DNSSEC. Asia-Pacífico se ve bastante bien. Todavía tenemos algunos que faltan pero tenemos buena tracción. Hay un recuadro con información ahí abajo. Italia, finalmente, todavía está como DS en la raíz, con lo cual quiere decir que no acepta registraciones de DNSSEC de los registradores. ¿Hay alguien de Italia aquí? ¿No? Suponemos que ese es el color que tiene DS en la raíz. Si alguien conoce a alguien de Italia y si aceptan DS de algún registrador, quizá deberíamos cambiar el color a un verde más oscuro.

La región LAC. Aquí hay algunos que faltan. Tenemos que hacer un poco de difusión en esa área. LACTLD está trabajando en eso. Fred, es tu responsabilidad. América del Norte, Groenlandia, está casi en verde oscuro. Estamos avanzando bien. Ese color cambia bastante el porcentaje para América del Norte. Va mejorando.

ORADOR DESCONOCIDO: Jacques, ¿podrías volver a la parte de Centroamérica? Estoy viendo que está Panamá. Ese va a ser nuestro próximo paso, Panamá.

JACQUES LATOUR: Sí, Quizá tengamos que hacer un evento de DNSSEC el sábado o algo así. América del Norte. Los mapas están disponibles online a través de Deploy 360. Se pueden suscribir. Creo que es bimensual o un email mensual y les envía todos los JPG y todo lo que necesitan para generar estas diapositivas. Se pueden suscribir y están online también. Dan, de ISOC, está trabajando en DNSSEC, en ese proyecto. Aquí van a tener un poquito de historia y van a poder actualizarlo. Si quieren conocer toda la historia de DNSSEC, la pueden encontrar ahí. Y eso es todo. Algunos minutos más temprano hemos terminado. ¿Hay alguna pregunta?

ABDALMONEM GALILA: Soy coach de ICANN de Egipto y trabajo en un ccTLD. Mi pregunta es cuál es la diferencia entre DS en la raíz y operacional. Creo que DS en la raíz significa que el registrador tiene que poner su record en el registro o si es que el registrador puede ofrecer facilidades DNSSEC para el registrador.

JACQUES LATOUR: El verde más claro es DS en la raíz, que quiere decir que está firmado. El verde oscuro nos muestra que el registro acepta DS del registratario. Pueden firmar la zona hija. Tienen EPP y lo aceptan en la web. Ustedes tienen DS en la raíz entonces.

ABDALMONEM GALILA: Gracias por tomar mi comentario antes en otras reuniones sobre agregar. Es decir, tomar los IDN ccTLD en cuenta. Esto es para el ccTLD con IDN de Egipto pero quizá tenemos que hacer una identificación entre IDN y ASCII. Si yo veo esto, voy a ver que esto es para .EG no para un IDN.

JACQUES LATOUR: Ese es un buen punto. Vamos a tomar nota de esto.

ORADOR DESCONOCIDO: Es más fácil si uno puede enviar un email directamente a Dan o al programa de taller de DNSSEC. Nos gustaría escuchar un poco más de detalle sobre esto. Gracias.

ORADOR DESCONOCIDO: Tengo un comentario rápido. No he encontrado ningún dominio formado en Italia. Si están delegando, lo están ocultando muy bien. Mi servidor no encontró ningún dominio firmado.

Probablemente no estén delegando o los estén ocultando muy bien.

JACQUES LATOUR: ¿Es un secreto? Gracias. ¿Alguna otra pregunta?

MATS DUFBERG: Me pregunto por qué el certificado de dnssecdeployment.org está vencido.

ORADOR DESCONOCIDO: En agosto de 2017.

JACQUES LATOUR: Dan York, ¿está escuchando? Antes de hablar tienen que decir su nombre. Cuando vayan a la diapositiva deben decir qué diapositiva quieren porque hay personas que nos están siguiendo solo por audio. Digan por favor entonces en qué diapositiva están.

MATS DUFBERG: Hay un link a la implementación de DNSSEC al que quería llegar y el certificado está vencido. Soy Mats Dufberg, de IIS.

JACQUES LATOUR: Muy bien. ¿Alguna pregunta? Tenemos un minuto más. ¿Hay alguien de África que tenga planificado implementar DNSSEC y que esté aquí en la sala, que nos pueda dar una actualización? Veo que no hay ninguna actividad. Muy bien. Gracias. La próxima sesión es una discusión de panel de las actividades de DNSSEC. Nuestro primer panelista es Joe Crowe, de Comcast.

JOE CROWE: Buenos días. Soy Joe Crowe. Como Jacques dijo soy de Comcast. Estoy trabajando allí como ingeniero sénior desde hace ya cuatro años. Comcast ha estado haciendo DNSSEC desde el año 2012. No solo empezamos a hacer validación a todas nuestras huellas digitales sino que también hacemos firma de DNSSEC para 5.000 zonas. Nosotros validamos para más de 20 millones de clientes. Son una de esas cuestiones que DNSSEC hace a escala y que nos enorgullece. Hay una operación donde hay algunas fallas a través de la validación DNSSEC. Nosotros recibimos llamadas. Hay una asociación vinculada con esas llamadas y es algo de lo más importante que enfrentamos, a pesar de que quizá no sepamos con certeza qué es lo que dejó de funcionar. Disculpen, es mi primera charla y es muy temprano en la mañana. Disculpen.

Algunos de los escudos operativos que tenemos mientras implementamos DNSSEC en nuestra huella es asegurar que

todos nuestros resolutores estén actualizados, asegurar que todo lo que se refiere a las versiones de números, software de los vendedores, todo esté en cumplimiento con todo lo que necesitamos en cuanto a automatización. La automatización ha sido nuestro gran paso hacia delante en los últimos tres a cuatro años. Hemos pasado de dos tipos diferentes de herramientas de automatización y terminamos utilizando SaltStack recientemente, que nos permite tomar un punto para automatizar a varios proveedores o sitios autoritativos o resolutores y nuestro DDNS/DHCP.

Cuando uno tiene cientos y cientos de servidores en la huella, es algo en lo que hay que involucrarse verdaderamente porque no se puede ir y cambiar todo de repente. Si uno cambia todo, va a haber algo que va a fallar y no quiere uno que falle. Nosotros recientemente empezamos a hacer EDNS0 en algunas de nuestras locaciones. Nuevamente, en nuestra escala, estamos tratando de implementarlo a través de un CPU y un costo asociado a nuestro desempeño a través de nuestros resolutores, debido al hecho de que tenemos muchas solicitudes por día y por segundo. Por eso tenemos que garantizar que hacemos lo correcto para la gente de CDN y que ellos tengan las respuestas correctas para las geoubicaciones. También tenemos que tener en cuenta qué es lo que tenemos que hacer para asegurar que no haya ningún error de desempeño para nosotros y para nuestros

clientes. En un par de milisegundos pueden generar un problema a escala y puede salir de un lugar que no sabemos.

A partir de 2015 también empezamos a utilizar DANE para email. Se trató de un tema operativo al principio, cuando lo empezamos a hacer, porque nuestros servidores autoritativos en ese momento tenían registros TLSA para que nosotros pudiésemos usar. Es solo un registro. Tuve que encontrar cómo usar el RR 52 para colocarlo en nuestros resolutores y así estar seguros de que sean lo suficientemente autoritativos para que el resto del mundo pueda utilizar esos registros. Después de que eso se hizo, impulsarlo no fue un problema. Lo tenemos operando desde el año 2015. Finalmente está en vivo y lo empezamos a testear en el año 2014.

El futuro de lo que nosotros vamos a hacer en nuestra infraestructura. Estamos pensando utilizar DANE con cualquier cosa que utilice registros TLS. Lo utilizamos como un CA interno. De este modo podemos autofirmar muchas de las cosas que hacemos internamente. No tenemos que preocuparnos de utilizar CA externos, especialmente con costos asociados a eso.

Algunos de ustedes seguramente saben que si ustedes están operando más de 5.000 zonas internamente, uno tiene que ver cuántos registros o certificados de TLD va a haber allí. Esto va a implicar mucho dinero. “Bueno, vamos a ir a Komodo” o “Vamos

a gastar algunos cientos de dólares durante varios años". Esto no es lo que queremos hacer, si lo podemos hacer internamente y utilizar DNSSEC para hacer nuestras zonas internas.

También estamos viendo cómo podemos hacer operativamente la implementación de las llaves DS. De nuevo, como dije, son más de 5.000 zonas. Esta es una tarea muy grande para realizar, especialmente cuando uno tiene los records de DS y quiere lograrlos automáticamente. Es un proceso manual en general que tenemos que hacer junto con nuestro registrador. Es una de las cosas que muchos de nosotros en el equipo empezamos a implementar para estar seguros de que podamos automatizarlo a un punto tal en el que podamos implementar y actualizar nuestro DS y refirmar cuando nos encontremos con temas como movernos, pasar de un servidor autoritativo a otro servidor autoritativo. En ese caso tenemos que refirmar. Tenemos que estar seguros de que estemos operativos y que esto funcione para nosotros.

Como estoy en una empresa grande, sé que todo el mundo enfrenta estos problemas pero, como decía antes, se combina con la cantidad de cosas que tenemos que hacer, que es asegurarnos de que funcione correctamente sin el impacto de tener altibajos. Un altibajo de 10 minutos podría costar muchísimo dinero. Cualquier llamado telefónico que entre con cualquier problema de DNSSEC realmente podría significar miles

de dólares, esos 5 o 10 minutos. Si dura más, va a depender de la cantidad de clientes que llamen.

Ayer precisamente tuvimos un problema donde hubo un fallo de DNSSEC. Recibimos un mail y un tweet de alguien que decía: "Miren, está fallando el DNSSEC" y en 15-20 minutos pudimos hacer un flash de la caché porque estábamos monitoreándolo. Hay pequeñas cosas. Si alguien quiere contactar al equipo de DNSSEC por esta cuestión, contacten @comcastdns en Twitter. Es una de las maneras más fáciles de contactarse con nosotros. Ahí no llegan a la persona que está en atención al cliente sino directamente al ingeniero de Comcast. Eso es básicamente lo que tenía para contarles sobre lo que estamos haciendo en Comcast en DNSSEC. No sé si alguien tiene alguna pregunta. Russ.

RUSS MUNDY: Gracias, Joe. Muchas gracias por venir hoy a este taller. Ha sido muy bueno el trabajo con Comcast en el pasado y esperamos seguir así. Cuando usted describía, usted se refirió al impacto de EDNS0. Seguramente han hecho algunas pruebas internas. Nosotros tenemos información publicada sobre el impacto de DNSSEC sobre los servidores autoritativos pero en realidad, o por lo menos yo, no recuerdo que tengamos ninguna información disponible públicamente que valide los resolutores,

en especial el impacto de los datos específicos, cuáles son los settings y cosas así.

Sé que usted no puede responder aquí pero le pediría que lleve esta pregunta a su compañía. Le pregunto si sería posible proveer algunos de los resultados de estas pruebas a la comunidad de DNSSEC de manera abierta porque esto ayudaría a los demás y constituiría un punto de referencia que otros podrían consultar y quizá les sirva para desarrollar sus propias pruebas.

JOSEPH CROWE: Sí, estoy de acuerdo. Creo que esto sería muy bueno para la comunidad DNSSEC en general. Tomo nota y veo qué puedo hacer.

RUSS MUNDY: Creo que esto también sería buena publicidad para Comcast.

ORADOR DESCONOCIDO: Una pregunta para aclarar. Usted está hablando específicamente de la extensión EDNS0 para subnet.

JOSEPH CROWE: Estoy hablando de geolocalización, principalmente para nuestros resolutores.

ORADOR DESCONOCIDO: Sí, eso era lo que quería confirmar.

ORADOR DESCONOCIDO: Tengo varios fallos en la historia de consultas. Empezó a fallar en 2016 y 2017. Me gustaría conocer los detalles técnicos. En el 2016 vi [RF6] que no estaba encriptado. Eran datos brutos antes de la firma. No sé si alguien logró manejar los datos de prefirma en esta zona. No sé cómo lo hacen. Si esto lo que pasó, me gustaría conocer más información.

JACQUES LATOUR: Jeff y luego Warren.

JIM: Uno de los mitos más populares que existen sobre el DNSSEC en la validación de los resolutores recursivos es que lleva tiempo y atención constante por el mantenimiento constante de los anclajes de confianza. ¿Cuál ha sido su experiencia en Comcast y qué puede contar de las otras ISP grandes que lo miran con mucho temor, con trepidación: “A ver qué puedo hacer”?

JOSEPH CROWE: Yo diría que habiliten DNSSEC. Es una operación para validar precisamente. Es muy fácil de activar en todos los proveedores

de resolutores de DNS. Parece ser algo muy oscuro pero operacionalmente, al tener activada la validación, está configurado y nos olvidamos. Ya no pensamos qué va a pasar. Como usted dice, los NTA y cosas así, va a haber una presentación más adelante sobre este tema específico pero ese sería mi consejo.

WARREN KUMARI: Quería decir que me siento mal porque nasa.gov ha decidido tener su propio DNS. State.gov también hizo algo muy interesante. Hasta que el último presidente decidió inhabilitarlo. Tenemos que hacer que la gente deje de deshabilitar el DNSSEC cuando salen estas noticias.

JOSEPH CROWE: Lamentablemente Google no recibe estas llamadas que nosotros recibimos. Estoy de acuerdo. Cuando pasan cosas importantes, HBO Now, cuando esto se active y DNSSEC caiga, cuando pasen estas cosas nosotros seremos los culpables.

JACQUES LATOUR: Tengo una pregunta. Usted dijo que hay más de 5.000 zonas que manejan la clave. ¿Están considerando automatización de la clave del CDS?

JOSEPH CROWE: No hemos llegado tan lejos porque tenemos muchos otros proyectos entre manos. Hay una persona, [inaudible], al que le hemos encomendado hacer esto.

JACQUES LATOUR: El último comentario que tengo para decir que aprovechar DANE significa obtener más beneficios. Sería fantástico tener una presentación sobre este tema para demostrar que si se lo implementa, se ahorra dinero.

JOSEPH CROWE: Estoy de acuerdo con usted. Cuantas más pruebas hagamos, y cuando se empiece a implementar, tiene que haber este tipo de conversaciones y creo que el paso próximo será su monetización. Gracias.

JACQUES LATOUR: ¿Alguna otra pregunta? Ahora vamos a escuchar a Jacques Latour, de CIRA. Hablará sobre las actividades en DNSSEC en Canadá y en .CA. Gracias a la herramienta de AP que monitoreó la situación en Canadá, en general la tendencia en Canadá ha sido descendente en lo que hace a la validación. Un par de ISP con el traspaso de la KSK decidió desactivar pero hay algunas

grandes. Lamentablemente la tendencia está yendo en la dirección incorrecta. Esperemos que la gente las reactive. Si tenemos información que puede significar ahorro de dinero en el manejo de las CA, tendríamos que generar por lo menos algún valor positivo.

En Canadá con CIRA hicimos presentaciones en cumbres de ISP, hablamos de la habilitación de DNSSEC, hicimos acciones con algunas ISP de difusión pero sigue siendo un desafío. Esto es de una empresa de telecomunicaciones en Canadá. Los clasificamos según el tamaño de la empresa de telecomunicaciones. Están ISP, Internet Exchange, que pueden compartir información. Es una de las más modernas que tenemos. El resto simplemente no les interesa. Tenemos mucho que trabajar con esta gente para hacer la activación.

Las actividades en .CA. Tenemos suficientes dominios firmados ya como para poder generar un gráfico, lo que es una buena señal. En la generación de este gráfico, a comienzos de este mes, teníamos 1.256 delegaciones. Para darles un ejemplo, en junio de 2017, GoDaddy habilitó la integración de DNSSEC con CIRA. Antes de esta fecha, GoDaddy nunca había apoyado el DNSSEC, lo que es una lástima. Ahora sí.

El impacto fue que a pesar de todo no se generó mucha demanda ni tráfico. No obstante, CIRA está trabajando para

hacer automatización de CDS, tal como lo está haciendo CZNIC, para automatizar los ads y deletes del DS y del registro de DNS y CDS. Hay muchos CDS disponibles en el archivo suficiente como para hacer que esto funcione.

La adopción es lenta. Además, son muy pocos los registradores que actualmente soportan el DNSSEC. GoDaddy lo activó pero a los registradores simplemente no les interesa hacer DNSSEC con sus registratarios, o sea, transferir claves que no tienen DNSSEC. Cuando hay llamadas para soporte del registrador, esa es una demostración de que existe la necesidad de automatización del CDS y de CDNSKEY.

Hace un par de días comenzamos a trabajar en la automatización de CDS. El desafío es que, como no hay suficientes recursos, no puede entrar la automatización en producción, incluso internamente, tenemos desafíos para que esto se convierta en una prioridad. Estamos haciendo muchas cosas con nuestros propios firewalls y nuestra plataforma pero faltan todavía algunas piezas específicas. Pienso que dentro de seis meses lo tendremos en producción. Es desalentador porque estamos trabajando internamente pero no lo logramos. Me gustaría dar mejores noticias pero no podemos. Es así. La vida es así.

El Internet Draft DNS operator, le pedimos al operador que añada y suprima el registro DNS. Vamos a revisar el draft completo, el protocolo, para que sea más API y más automatizado. Si hacemos una API para el operador, esto al operador le significa un costo cuando publica en su zona sin ninguna actualización o programación. Creo que escalar a la zona es lo mejor pero existe la necesidad de que el operador nos dé su apoyo y así lo podemos refinar y ajustar a la realidad. Eso es todo. Eso es básicamente lo que está pasando en Canadá y con .CA. ¿Preguntas?

ORADOR DESCONOCIDO: Como uno de sus registratarios y como uno de los pocos registradores que lo hacen, tengo dominios firmados pero además por eso tengo los problemas habituales que tiene un administrador de DNS. ¿Qué puedo hacer con CDS, por favor?

JACQUES LATOUR: Está en el 10%. ¿Puede decir su nombre, por favor?

VIKTOR DUKHOVNI: Sí, lo dije. Soy Viktor Dukhovni. Encontré 24 dominios en .CA que hacen DANE de esos 1.200. CIRA Labs es uno de ellos. Parece que ustedes lo están probando. Muy bueno. Eso es todo.

JACQUES LATOUR: Russ.

RUSS MUNDY: Jacques, ¿tienen algún plan para conseguir más registradores en Canadá que hagan DNSSEC o siguen siendo recalcitrantes y dicen siempre que les cuesta dinero?

JACQUES LATOUR: Lo que hacemos ahora con los registradores es hablar con ellos para implementar DNSSEC y CDS y CDNSKEY pero estamos en la etapa de intercambio de información. No obstante, les interesa habilitar el DNSSEC, activar DANE, publicar CDS y nosotros nos ocupamos del bootstrapping y de trabajar con ellos. La parte EPP, la transferencia del registro DS, eso no se está dando.

RUSS MUNDY: Entonces la cooperación en términos de dar soporte a DNSSEC es buena en tanto y en cuanto no exista un impacto operativo financiero. Ponen los registros pero no quieren poner dinero para incorporar todas las capacidades en sus sistemas. Okey.

JACQUES LATOUR: Hicimos un taller y la transferencia de la información DNSSEC no es parte de la registración del dominio. El registrador no le

interesa DNSSEC porque no forma parte de la información de registración per se. Creo que son más los datos operativos en el backend. ¿Alguna otra pregunta?

CHRISTIAN HASSELMAN: ¿Usted habla con estos ISP que mostró en la lista?

JACQUES LATOUR: Sí. Yo contacto a las empresas de telecomunicaciones y a los ISP del país. Les presento las estadísticas, les doy las tendencias sobre DNSSEC pero no les interesa. Excepto las estadísticas de IPv6 que están mucho mejor. Este fue un taller sobre IPv6. Tenemos muy buenas estadísticas de Canadá. DNSSEC, bueno, debemos seguir trabajando. ¿Alguna otra pregunta? El que sigue ahora es Carlos Acosta, de NIC .PR y Jim Galvin para hablar de la historia de DNSSEC en .PR.

CARLOS ACOSTA: Hola, soy Carlos. Una breve historia de cómo entró DNSSEC en .PR. En primer lugar, el registro era un laboratorio de investigación que se involucraba en varios proyectos. Desde watermarking hasta criptografía de clave pública y varios otros proyectos. Como comenzó con un centro de ciencias de la computación, por eso hacíamos todos estos temas de encriptación y demás.

Aproximadamente en el año 2000, un par de sitios de gobiernos locales fueron redirigidos a nivel de ISP que en .PR se determinó que esto debería haberse evitado. Tendría que haberse implementado DNSSEC. Un poquito después Suecia fue el primer ccTLD que ofreció DNSSEC. Nosotros pensamos que era el camino a seguir.

Para el 2006 en julio, comenzamos a firmar las zonas pero no fue hasta agosto que comenzamos a poner esos registros en los servidores públicos. Esta es la lista de las zonas desplegadas con DNSSEC. Una lista importante, considerando. Después armamos una página web pequeña para informar a la gente o a las partes interesadas de qué era lo que había, etc. En esa misma época, alentamos al gobierno a firmar los dominios del gobierno con DNSSEC para prevenir el ataque que habían sufrido hace un par de años.

Un par de años atrás comenzamos un programa de incentivos en el cual empezamos a firmar los clientes con DNSSEC. Este es un gráfico de diciembre del año pasado, con la cantidad de zonas firmadas que ya tenemos y las que no están firmadas. Tenemos un poquito más de un 1% a diciembre del año pasado. Este es el detalle de lo que representa ese 1%. El 91% fue firmado por nosotros y el 9% por los registratarios.

Esta es una reseña de los detalles, de cómo firmamos DNSSEC. Lo hicimos en una máquina Windows 2003. Se usó VBScript para hacer la firma de DNSSEC y generar los archivos de la zona y verificamos que todo funcionaba correctamente utilizando los resolutores DNSSEC de la OARC y utilizando DNSViz, que es una herramienta excelente. Eso sería básicamente todo. No sé si tienen alguna pregunta. Muy bien. Si no hay más preguntas, le voy a dar la palabra a Jim.

JIM GALVIN: Gracias, Carlos. Soy Jim Galvin, de Afilias. Voy a saltear aquí las primeras y vamos a ir a la diapositiva número cuatro. Afilias acaba de hacer una transición del .PR a nuestros servidores en enero de este año. Puede ser esta una buena oportunidad para hablar sobre los procesos de hacer la transición de TLD. Sé que hablamos mucho de la implementación de las claves pero esta es una buena experiencia para nosotros. Fue un placer unirnos al .PR en esta experiencia como uno de los que primero adoptamos DNSSEC. Quería dedicarle un poco de tiempo a este proceso.

Pasamos ahora a la diapositiva siete. Afilias, al igual que .PR, está involucrada en DNSSEC desde hace mucho tiempo. Fuimos uno de los primeros. Empezamos DNSSEC en 2008 y empezamos a firmar los TLD en 2009. Lo hacemos desde hace bastante tiempo y en el camino hicimos la transición de varios TLD.

Lamentablemente, algunos no pero hacemos la transición de estos TLD de todos modos.

Pasamos ahora a la diapositiva nueve. Lo que es interesante es que hay mucha atención que se le da a la implementación de la KSK de la raíz. Por supuesto, esto tiene que ver con que hay mucho riesgo. A pesar de que nosotros hacemos implementaciones de claves, DNSSEC requiere bastante tecnología para hacerlo. Es interesante a nivel de los TLD que es una propuesta de muy alto riesgo. Las consecuencias, los efectos de hacerlo mal, pueden ser muy traumáticas. A nivel de TLD se puede perder todo un TLD y hacer que se invalide. Aquellos de nosotros que estamos en la tecnología y vemos lo que sucede, queremos tomarnos el tiempo para analizar bien el proceso y ver cuáles son los puntos complicados a medida que avanzamos.

Diapositiva 11. Lo que resulta interesante aquí es que hay algunos pasos administrativos que están por fuera del control que uno tiene como proveedor de servicios. Una de las cosas con las que se encuentra es que hay dos partes que tiene que enfrentar. Es fácil decir: “Sí, tengo que hablar con los otros proveedores de servicio donde sea que esté alojado actualmente el DNS” pero a nivel de TLD también había interacción que tenía que ocurrir con IANA porque hay que tener los nuevos records de DS dentro de la raíz. Son procesos administrativos adicionales que no están bajo nuestro control y por supuesto IANA tiene sus

propios pasos de validación que realiza para estar segura de que esto es lo correcto que tiene que ocurrir.

Hay entonces una interacción entre ellos. Hay que documentarla y monitorearla. Lo siguiente que ocurre es que cuando uno está listo para iniciar todo esto, sigue habiendo interacciones adicionales con IANA. Cuando uno está implementando su propia llave en su propia zona y agrega nuevos records de llave o mueve los servidores de nombre y está moviendo todo el tiempo los servidores y cuando tiene la coordinación que tiene que hacer con esta parte adicional, el tema verdadero aquí es la línea de tiempo. Es un proceso bastante directo si uno tiene que hacer su propia zona en su propio entorno porque el tiempo que requiere todo esto generalmente está vinculado a algún múltiplo del TTL y cómo lo gestiona.

En nuestro caso, cuando nosotros hacemos este tipo de implementaciones con nuestros TLD, el proceso puede tomar semanas para que se haga bien. Lo que queremos es que todos los pasos administrativos se cumplan. Nuestro objetivo es hacer chequeos dobles. Cada vez que hacemos algo hay que verificar que se hizo bien antes de pasar al paso siguiente, que estén presentes todas las claves. Es una carga bastante grande desde el punto de vista administrativo.

Pasando ahora a la diapositiva 14, me voy a tomar un minuto para hablar de algunos de los retos más importantes que enfrentamos. Aquí .PR habló de cómo ellos operan gran parte de estas cuestiones en Windows machine, incluso hoy. Nosotros nos hemos encontrado con tecnologías bastante viejas en nuestros procesos para mucha gente. Lo hemos visto en muchos TLD más pequeños especialmente. Una de las ventajas, creo yo, que tenemos nosotros en ser un gran proveedor de servicios es que tenemos todo automatizado como ocurre con muchos otros aquí.

Una de las grandes sorpresas para nosotros en todo esto es la configuración que hay que tener. Es decir, hay que ver qué está haciendo el proveedor actual. Hay que integrarse con ellos y obtener datos de zona y ver cómo vamos a gestionar este cambio de las claves.

Otra cosa con la que nos enfrentamos es que hay distintas políticas. Yo sé que nos focalizamos mucho en la cuestión técnica pero es obvio que es una posición de una práctica mucho mejor cuando uno tiene dos servidores de nombre pero podría ser bastante sorprendente ver que hay ccTLD que solamente tienen un objeto de servidor de nombre en sus sistemas. Esto es un problema para nosotros porque implica que solucionar este problema en la marcha y tenemos que cambiar las registraciones en el sistema. No es solamente un TLD sino que

también hay datos que tenemos en los dominios de segundo nivel. Tenemos que garantizar que todas las políticas estén actualizadas. Esto es un trabajo adicional que puede ralentizar un poco el proceso de transición. Uno tiene así un efecto de los datos de registración también.

El otro problema que tenemos es encontrar inconsistencias en los datos. Incluso para nosotros, cuando tenemos problemas, a veces estos problemas están presentes en una zona o son parte de la transición y nosotros ni siquiera nos damos cuenta. Nosotros también tuvimos que actualizar nuestros procesos para no tener problemas en el futuro. El mensaje al hacer esto es que es un trabajo general muy grande implementar un TLD y hacer la implementación de la KSK. No es solamente la cuestión técnica sino que tiene que ver más bien con todas las actividades extra que vienen junto con eso. Tenemos una lista de verificación que vamos siguiendo cuando lo hacemos. Incluso en ese caso pueden surgir problemas y hay que ir resolviéndolos a medida que avanzamos.

En este entorno estamos pasando a una comprensión mejor de DNSSEC. A mí me gusta escuchar y monitorear la penetración del DNSSEC en los TLD en general y este tipo de cosas son muy importantes de reconocer. No es tan fácil y tan trivial como todos quisiéramos que sea este paso a este espacio. Eso es lo que tengo que decir.

JACQUES LATOUR: Gracias, Jim. ¿Hay alguna pregunta?

JAROMIR TALIR: Veo que ustedes están utilizando el algoritmo cinco para DNSSEC. ¿Están pensando ustedes en cambiar el algoritmo del DNSSEC?

JIM GALVIN: No tenemos planes inmediatos de cambiarlo pero sí, está en nuestro radar y es algo a lo que le prestamos atención. Todavía no decidimos si vamos a implementar un algoritmo. ¿Qué es el algoritmo cinco? ¿Hay alguna pregunta? ¿No? Gracias. El siguiente es Frederico Neves que nos va a hablar de la implementación del algoritmo DNSSEC de .BR.

FREDERICO NEVES: Estamos usando RSASHA1. Soy Frederico Neves. Estoy trabajando en .BR, el NIC de Brasil. Esta es la diapositiva dos. Les voy a contar un poco sobre el registro .BR. Básicamente, nosotros empezamos el año 2007 utilizando RSASHA1. En el 2009 con el advenimiento de opt-in pasamos a opt-out. Ahí pudimos firmar zonas más grandes así que lo hicimos. Firmamos todas las zonas .BR en ese momento. Tenemos unas 75 zonas

aproximadamente o teníamos en ese momento. Hoy tenemos unas 90 zonas con las adiciones de nombres geográficos de nombres de segundo nivel para algunos sitios en Brasil.

En 2010, un poquito antes de la firma de la raíz hicimos nuestra primera implementación KSK y actualizamos el DPS y el tamaño de la llave a 1280 bits e introdujimos una ceremonia completamente diferente con HSM y configuración DR completa. Esto es lo que estuvimos utilizando desde ese momento. También pudimos tocar la raíz con DS en junio ese año. En el 2015, después de nuestro DS, implementamos la KSK de nuevo y en ese momento aumentamos el tamaño de la clave nuevamente a 1536 bits. En este momento tenemos 3.9 millones de delegaciones. La mayoría de ellos están en la zona de segundo nivel .COM.BR y tenemos aproximadamente un millón de delegaciones firmadas.

Moviéndonos de nuevo a la presentación, en cuanto a nuestras motivaciones para hacer una implementación del algoritmo, la motivación más importante es básicamente estar preparado para una implementación eventual del algoritmo, preparar el software para eso. Tenemos nuestro propio firmante. El software actual no tiene la capacidad de implementar algoritmos. Por eso nosotros preferimos utilizar estos [peace times] para ejercer esto y estar completamente preparados.

Decidimos utilizar ECDSAP256. Gracias a nuestros colegas aquí a mi izquierda, porque ellos ya habían tenido el desafío de hacer un ping a IANA para soportar este algoritmo y ahora IANA ya está lista y no vamos a tener ningún problema en la implementación de este algoritmo en el futuro. Hay un beneficio adicional de esto porque algunas de las zonas que nosotros utilizamos son la prueba de no existencia en los nombres, en los tipos. Tampoco necesitamos ya tener una clave por separado por la historia del protocolo, la implementación del algoritmo que utilizamos para introducir NSEC3.

Nuestro sistema de aprovisionamiento actual está envejeciendo un poco. Fue escrito en el año 2009 y en ese momento nosotros no teníamos todas las buenas librerías de DNS. Teníamos a escribir nuestra propia librería y mantener esto así. Lo que queríamos es tener otra ventaja de cambiar este software.

Vamos a la diapositiva cuatro ahora. El enfoque de implementación del algoritmo. Como dije, nosotros tenemos nuestro propio firmante y tenemos que decidir cómo hacer la implementación del algoritmo. Así empezamos a investigar las recomendaciones, y el 6781 recomienda que hagamos la implementación de lo que ellos llaman la forma conservadora. Todos los firmantes de código abierto que nosotros pudimos contactar utilizan el modo de llaves gestionadas y el OpenDNSSEC que se llama enfoque liberal pero estamos un

poco más inclinados a utilizar el modo conservador y no el liberal.

En la última semana, durante nuestra reunión, tuvimos un poco más de información sobre esto y sabemos que el software que tiene este enfoque conservador ya tiene siete años y esto ocurrió entonces hace tiempo. Incluso hace cinco años teníamos la clarificación del 6840 sobre este lenguaje de 4035 un poco confuso que se aplica a los firmantes y no a los validadores. Esto es una controversia pequeña. Tuvimos una implementación del algoritmo muy exitoso en otros colegas en el .SE. Ellos utilizaban DNSSEC y les fue bastante bien. Vamos a la próxima.

De todos modos, vamos a testear los dos enfoques y les voy a mostrar esto un poquito más adelante. Lo que vamos a hacer en los próximos meses, como dijo Jim, es implementar un TLD. No es algo divertido. Hay muchos procedimientos y muchos pasos para garantizar que todo funcione adecuadamente. Básicamente lo que hacemos es actualizar nuestros HSM y vamos a encargar un tercer sitio en una ubicación más lejos de los dos que tenemos ahora en Sao Paulo. Nuestros HSM fueron comprados en 2010. Todavía están funcionando bien pero vamos a sustituir dos de ellos y vamos a hacer actualizaciones para soportar el nuevo algoritmo.

Incluso en mayo vamos a hacer una ceremonia regular de implementación. Es una ceremonia para cubrir el periodo que va desde agosto de 2018 a enero de 2019. En cuanto a la ceremonia de implementación, vamos a ejercer los dos métodos. Hay un pequeño problema en esta diapositiva. Estoy ahora en la diapositiva 6, para quienes estén conectados remotos, sobre el nuevo algoritmo.

Vamos a usar seis zonas. En tres de ellas vamos a utilizar el método conservador y en las otras tres vamos a utilizar el método liberal. La razón por la que mantenemos esas tres zonas es que en las zonas .BR tenemos llaves divididas y en la zona hija tenemos una llave única. Tenemos una que utiliza NSEC3 proof y otra que usa NSEC3. La mayoría de ellos utilizan NSEC. Por eso vamos a ejercer todas esas situaciones. Esperamos poder tener el principio de estas implementaciones en junio de 2019.

En cuanto al monitoreo de la implementación, vamos a seguir la implementación exitosa de .SE. SIDN Labs publicó un informe detallado sobre el monitoreo de la implementación y planeamos utilizar su metodología para monitorear los testeos y la implementación en sí. Le recomiendo mucho a la gente que lea este informe.

La ceremonia de la implementación que vamos a hacer en los días 23 y 24 de julio en nuestros dos sitios, ahí vamos a actualizar

todo el software y el hardware firmantes y vamos a prepararnos para la exportación de las claves porque cuando hacemos la generación de las nuevas claves en la ceremonia, esto implica muchos pasos de exportación de las claves y de importación de los HSM en producción plena. Por eso vamos a cambiar un poquito la manera en que hacemos los serials. Vamos a ir al formato juliano. Eso nos va a permitir tener más incrementos en un mismo día, porque estamos incrementando la publicación de la zona de cada 30 minutos a cada 5 minutos.

Para concluir, esta última diapositiva muestra los cambios visibles que la gente puede observar en los próximos meses. Las pruebas comenzarán el 19 de junio. Durarán hasta el 22 de junio. La implementación del algoritmo, si todo va bien, lo planeamos para el 20 de agosto. Si todo va según lo planeado, pretendemos terminar el 27 de agosto, que es la primera ventana de claves prefirmadas porque esa es la interacción con la IANA. Eso es lo que tenía para presentar. Si alguien tiene preguntas. Queda tiempo.

VIKTOR DUKHOVNI: Hay gran adopción pero hay un pequeño grupo de problemas residuales en las delegaciones, si nos puede ayudar. Principalmente [jus.br]. Repito, hay un número pequeño de

dominios cuya administración es menos que perfecta. Si me puede poner en contacto con ellos, se lo agradecería.

JACQUES LATOUR: ¿Alguna otra pregunta? Yo tengo una pregunta. .CZ trataba de migrar al protocolo en CIRA, pero no estaba soportada por la IANA. ¿Está soportado ahora?

FREDERICO NEVES: Sí. En este momento está soportado.

JACQUES LATOUR: ¿Alguna otra pregunta?

ORADOR DESCONOCIDO: ¿Puedo hablar en francés o tengo que hablar en inglés? Es en relación con la aplicación que ustedes han utilizado. ¿Tienen documentación sobre la prueba que han efectuado? Quiero saber cómo han transmitido las pruebas efectuadas a la comunidad, en especial para la comunidad francófona del Caribe. Gracias.

JACQUES LATOUR: Si ustedes pueden traducir. La documentación de la prueba, la comunidad de LACTLD.

FREDERICO NEVES: Sí. Esperamos al menos publicar el informe a finales de junio, comienzos de julio. Lo vamos a poner en un blog.

JACQUES LATOUR: La traducción fue perfecta. Gracias. ¿Alguna otra pregunta? Vamos a un break. Tenemos cinco minutos más en el receso. Debemos estar de vuelta a las 10:30 para la parte dos del taller. Gracias.

[FIN DE LA TRANSCRIPCIÓN]