BARCELONA – Taller sobre las DNSSEC (1 de 3)
Miércoles, 24 de octubre de 2018 – 09:00 a 10:15 CEST
ICANN63 | Barcelona, España

RUSS MUNDY: Todavía no son las 9:00 en punto pero nuestro panel es muy grande. Fui tratando de ubicar a todos los que entraron en la sala pero quizá me salteé a alguien porque hay un panel muy grande. Si hay alguien en la sala que está en el primer panel a quien yo todavía no haya identificado, aquí están las mesas y las sillas. Aquí es donde deben sentarse. Vamos a comenzar en un momento pero antes de comenzar, lo voy a decir otra vez. El almuerzo que ven allí no es para este taller de DNSSEC. Nuestro almuerzo va a ser arriba. Son dos pisos hacia arriba. Esto es para otro grupo. Es decir, en el horario del almuerzo vamos a tener que salir. Ahora Steve Crocker está por teléfono. Buenos días, Steve. Soy Russ. Está aquí en la sala con nosotros.

Son las 9:00 en punto ahora. Ya tenemos a casi todos en nuestro panel de nueve personas. Soy Russ Mundy. Quisiera darles la bienvenida a todos a este taller de DNSSEC de ICANN63. Tenemos un programa muy amplio hoy. No voy a hacer mucha introducción más allá de decir una vez más que el almuerzo que ven ahí no es para este taller de DNSSEC. Nosotros salimos y vamos dos pisos hacia arriba. Me dicen que es un lindo lugar para almorzar. De todos modos, tenemos que salir de la sala al medio día para el almuerzo y luego volvemos. Con esto vamos a nuestro primer orador que va a hacer la presentación. No me acuerdo cómo es el apellido de Erwin.

ERWIN LANSING: Yo ya no vivo en Holanda así que tampoco me recuerdo a mí mismo. Me voy a poner de pie. Buenos días a todos. Primero quisiera saber si todos estamos listos para empezar. Nosotros traspasamos la llave e Internet no dejó de funcionar. Todos los que sean del comité, por favor, levanten la mano. Les agradecemos a nuestros sponsors por el almuerzo. A Afilias y a SIDN. Siguiente diapositiva. Este taller está organizado por SSAC y por la sociedad de Internet con su programa Deploy360. Tenemos un programa muy apretado. Vamos a la diapositiva siguiente.

Tenemos muchos números y les voy a dar más números de Dinamarca después. Estos son los números para todo el mundo. Estos están hechos por Geoff para APNIC. Son estadísticas de validación de Google Ads. Todavía como vemos siguen aumentando. Un 14% para todo el mundo. Querríamos que fuera más alto. Algunas de las regiones que pueden ver que utilizan Google, Google por supuesto tiene su resolutor abierto que hace validación de DNS. El número 1, Micronesia, es 61-62%. Tenemos un porcentaje un poco más bajo de estadísticas de Google. Implican que los ISP también están haciendo su trabajo. Estos son algunos de los números de los dominios firmados. Quisiera saber si este número de Holanda es correcto, el de [62.000]. Son 62.240. ¿Dominios firmados, no? No sé muy bien cómo se recolectaron estos números.

.COM es el 1, .SE es el 2, .NU y .NET, .NL, .CZ. Pensé que los de Holanda sería un número más alto. Respecto de los TLD para los ccTLD que

están siendo firmados, el programa Deploy360 analizo quiénes son los que efectivamente firman un dominio, un TLD. Hay cinco niveles. Empezamos con experimental. No hay todavía nada en la zona. Está experimental. El amarillo es para Announce que son los compromisos públicos que se tienen que desplegar. Los azules tienen la zona firmada pero no colocan al DS en la raíz, lo cual quiere decir que la validación todavía no funcione. El verde claro es el DS en la raíz pero no está aceptando los registros de DS y por lo tanto todavía no está listo. El verde más oscuro es que el está completamente operativo. En la siguiente diapositiva vemos a todo el mundo que cada vez está más verde. Se ve bastante bien. Tenemos algunos espacios en blanco.

La siguiente diapositiva creo que es la de África, que está muy blanco. Solo hay algunos países que han hecho la firma pero todavía queda trabajo por hacer. En África del sur va bastante bien y en el África central no va tan bien. África cada vez está más verde. Sigue pendiente del Medio Oriente. Casi todo verde aquí. Muy bien Europa. Bien hecho. Aparentemente Bielorrusia e Italia ya están operativos. Siguiente.

América Latina se ve muy bien también. Groenlandia ya está llegando. Hay varios TLD en América del Norte. Estos mapas se actualizan semanalmente. Van a poder encontrar más en este link porque esto es actualizado manualmente. Creo que esta es la última diapositiva. No, todavía queda una más. El programa Deploy360 tiene un informe que se hizo en el año 2016. Esta es la última diapositiva. Con esto le vamos a dar la palabra al primer panelista.

RUSS MUNDY: Como nuestro primer panelista está por aquí vamos a tomar las preguntas al final de la sesión como hacemos normalmente. Gracias, Erwin por ayudarnos con esta intro y con los mapas. Con esto, vamos a pasar inmediatamente a nuestro panel y nuestro primer presentador en el panel es Erwin, que nos va a contar qué es lo que sucede en el .DK.

ERWIN LANSING: Soy Erwin Lansing, de .DK. Estos son los números para .DK. Está aumentando lentamente, a unos 24.000 firmados que es casi el 2%. Creo que son unos tres millones de dominios. Seguimos trabajando en convencer a los proveedores de alojamiento de que firmen la raíz. No estoy muy seguro de los números en verde pero el azul se ve bastante interesante porque aparentemente la gente está usando el algoritmo ocho pero en el último año o dos fuimos directamente a otro tipo de algoritmos que me parece a mí que es algo que está muy bien. Creo que el pequeñito que está en el medio es de algunos algoritmos que no fueron firmados.

Respecto de la validación estamos hablando de 14%. Dinamarca tiene el 64%, que es cuatro de un total de cinco ISP que están firmando y esto está basado en números de APNIC también. Mis últimas diapositivas son los próximos planes hacia el futuro. Nosotros tenemos un sistema único donde todos los nombres tienen que ser registrados en el registro, lo cual también implica que todos los nombres tienen que estar operativos en los servidores. Eso quiere decir que lo podemos usar para permitir que se actualicen los registros DS en los

operadores de nombres de servicio e incluso si esos operadores son un registrador.

Hemos tenido un proveedor desde el año 2010. Esto se firmó después de la raíz. Al fondo de la página ustedes ven que se indica con el login y con la información clave. Esto se hace automáticamente una vez que uno utiliza una interfaz de servidor autorizado. Utilizamos también los protocolos CDS y CDNSKEY. Sin embargo, al mirar en la zona y ver cuántos registros de CDS y CDNSKEY hay es difícil validar los recursos con solamente 1.200 dominios que utilizan CDS. De todos modos, esto es solo para el futuro, para hacer que la firma sea más fácil para los operadores. Estos son mis números para .DK.

RUSS MUNDY: Gracias. Nosotros le agradecemos mucho por esto. En la próxima vamos a escuchar a Michael Hausding de SWITCH y .CH.

MICHAEL HAUSDING: Muy bien. Les voy a dar algunas actualizaciones sobre los números y lo que hacemos para promover DNSSEC. En el primero tenemos los números de los dominios firmados con DNSSEC. Hasta hoy tenemos 57.000 que están firmados. Son alrededor del 3%. Este es un gráfico. Lo publicamos también en Internet. Como ven, aquí hay del año 2017 un aumento importante en las firmas de DNSSEC. Los registradores firman por defecto. Ven allí una pequeña meseta y eso es porque el operador se olvidó de firmar, hizo algunos cambios y se olvidó de firmarlos. Siguiente diapositiva.

Nosotros pensamos que los números son importantes y por eso publicamos el .CH resilience dashboard. Lo hicimos con el fundador del .CH donde se menciona la implementación de estándares de seguridad para web y para email. Nosotros tomamos los dominios principales de .CH y analizamos cuál es el nivel de seguridad. Como vemos, tenemos un 91% de HTTPS. Para email también está bastante bien pero si vemos la siguiente diapositiva vamos a ver que DNSSEC solamente tiene un 3% dentro de los dominios .CH. Nos parece que es importante darle visibilidad para que la gente pueda ver cómo le va.

También promovemos DNSSEC. Este año hicimos una capacitación de DNSSEC. Al principio tuvimos tres capacitaciones. Hubo tres de un solo día donde se aprendió lo básico de DNSSEC y cómo firmar una zona con PowerDNS. Dentro de las 24 horas estamos a capacidad completa y tuvimos que hacer dos seminarios más. Fue un éxito y sabemos que hay algunos registradores y algunas empresas de alojamiento que están firmando su nombre de dominio.

También dimos algunos premios de DNSSEC al registrador que firma con DNSSEC por defecto. Hay una parte de Suiza que firmó 38.000 de 57.000 dominios en total. Estamos hablando de un 60%. Nosotros empezamos CDS al principio de octubre. Es posible optar hasta finales de año. Está habilitado para todos y ya tenemos el primer registrador que optó. Vamos a firmar unos 27 dominios creo que mañana. Voy a hablar después de esto.

Vamos a hacer una implementación del algoritmo con el traspaso de la llave. Por último pero no menos importante, estamos muy contentos

de que nuestro gobierno federal firmó el dominio utilizado por el gobierno federal que es admin.ch. Esto se planeó durante años. Eso es lo que sé. Por suerte, en enero de este año hubo una pregunta en el Parlamento respecto de si el gobierno federal utiliza DNSSEC. El ministro no sabía que era DNSSEC. Nosotros, por supuesto, sí pero en este momento ellos no lo tenían y allí empezó a haber un poco más de presión y finalmente lo firmaron.

RUSS MUNDY: Nuestro próximo presentador es Peter Koch, de .DE.

PETER KOCH: Buenos días. Este soy yo, que estoy del otro lado de la herradura. Voy a compartir algunos números y algunos gráficos con ustedes. Esto va a ser interesante, respecto del desarrollo de DNSSEC desde el principio del año. Solo para recordarles a todos el tamaño y la cantidad de dominios DNSSEC que no se ve muy impresionante, tenemos 16.2 millones de dominios en total, 300 miembros que son registradores. Algunos son revendedores. Para que los registradores puedan presentar DNSSEC no hay una firma necesaria en nuestro sistema de registración con lo cual se hacen presentaciones y no hay ningún testeo. Los tres registradores principales tienen alrededor del 50% de los dominios firmados. Hay concentración, por supuesto, como en todas partes. En esos casos, el registrador también es el operador de DNS para casi todos los dominios. Es decir, tienen que presentar materiales principales que los sacan de su propia operación. Este es un modelo que también es cierto para los registradores más pequeños o

registradores con números más pequeños. Lo que Michael mencionó de Suiza también es conocido. Es un país conocido para el DNSSEC para .DE.

Como dije, y para completar, estamos trabajando con los registros de llave de DNS. Los registradores presentan ese registro y cuando van al registro nosotros calculamos los registros DS y utilizamos un algoritmo hash para eso. Tenemos verificaciones de predelegación para las registraciones normales y si un registrador presenta materiales de llave también hacemos algunas verificaciones adicionales. Esos materiales de llave tienen unas validaciones. No pueden presentar llaves que no están en la zona. Perdón, es muy temprano en la mañana… Vamos a aceptar llaves que no estén presentes en la zona únicamente si hay al menos una que valide completamente el registro SOA. Es decir, que es un traspaso de la llave que estaba aceptado por las otras llaves.

Nosotros tenemos unos 100.000, a veces 200.000, dominios que están servidos autoritativamente por la zona .DE y, por supuesto, no son contactados en las estadísticas en términos de publicidad. Sigue siendo temprano pero hay un tema que atraviesa todas las reuniones esta semana. Obviamente, el 25 de mayo tuvo una gran influencia. Imagínense qué pasó ese 25 de mayo. ¿Alguna apuesta? Alguien dijo GDPR. Muy bien. Diapositiva siguiente. ¿Podemos moverlo hacia la izquierda, por favor? No, es demasiado. Una diapositiva hacia atrás. Una diapositiva hacia atrás. ¿Podemos volver una para atrás? Sí, esa es.

Por supuesto, esto no tenía nada que ver con GDPR. Era una indentación en el número de dominios con DNSSEC. Por coincidencia, eso pasó en el 25 de mayo. Podríamos decir que el registrador estaba tan ocupado con DNSSEC que no se dio cuenta y suprimió las claves de una cantidad de dominios. Con un registro fuimos al registrador. Nos dimos cuenta del error y volvimos a presentar las claves de todos estos dominios y así procedimos. Otra diapositiva.

Fíjense en esa indentación en mayo. Es la fecha de mayo. esto lo muestro no solo por este dato curioso de que haya ocurrido el 25 de mayo sino para marcar que algunos registradores tienen procesos que requieren más monitoreo y también intervención manual como sucedió en este caso. Dos diapositivas más.

Los materiales presentados muestran que comenzamos con 80.000 dominios en enero y 100.000 en la actualidad. Un crecimiento del 25% sin actividades de promoción. La siguiente, por favor. Esto lo salteamos. La próxima. Hablando de los algoritmos. No, la siguiente. Debería haber una más.

Aquí vemos los algoritmos. El dominante es el 8-RSAHA256. El 7 en rojo y también 9% de ECDSA y el resto son los otros, incluyendo un DSA porque la gente sigue testeando. No debería ser muy diferente de los otros. Muchas gracias.

RUSS MUNDY: Muchas gracias, Peter. El que sigue en la agenda es Bret Carr, de Nominet.

BRETT CARR: Buenos días a todos. Yo tengo el clicker. Cuando hablé al principio con Jack sobre esta presentación él me dijo que normalmente la gente da estadísticas. Yo decidí no hacer eso y hacer algo distinto. Espero que les parezca bien que haya cambiado la estructura. Como ven, la primera diapositiva dice nada de estadísticas. Quería hablar un poquito acerca de cómo simplificamos el DNSSEC en Nominet. Una historia de cosas que hicimos en el pasado.

En el 2009 firmamos .UK. Seguramente ustedes recordarán que tuvimos un pequeño problema en el 2011 cuando comenzamos a usar una nueva clave sin haber hecho la prepublicación necesaria. Eso se debió a una combinación de fallo de hardware y error humano. Esto lo recordamos todos los años porque esta fotografía que aparece en pantalla… Seguramente no pueden leer el texto pero la publicó mi esposa en esa época en que yo estaba intentando resolver el problema y dice: “Ayudando a Papi a arreglar la Internet o alguna otra cosa”. La terminamos arreglando, lo cual fue bueno.

En el 2014 comenzamos a firmar también los gTLD. En los años, las distintas cosas que ocurrieron. En el 2009 comenzamos a usar SCA6000. Bastante confiable pero fue la causa del problema del 2011. No podríamos haberlo resuelto sin generar otro problema. También hubo error humano. Algo que provocó el problema fue que Oracle compró Sun.

En 2013 pasamos a la red basada en Thales HSM y OpenDNSSEC y ambas situaciones fueron muy complejas. Era confiable pero muy

complicada su administración. Era complicada y cuando algo andaba mal, la gente no sabía muy bien cómo resolverlo. Tuvimos casos de poco apoyo, poco soporte y trabajamos con Thales y OpenDNSSEC y no fue fácil.

En 2016 llegamos a elaborar una solución más sencilla. Ahora no usamos HSM en absoluto. Toda la firma se hace en una máquina virtual replicada geográficamente con BIND. Obviamente, si tenemos problemas los tenemos que manejar pero no ha sido nada muy serio que haya impactado la producción. Debo decir que el apoyo de ISC ha sido muy bueno.

Nuestras claves están en una partición encriptada protegida por una contraseña partida. Es una contraseña con un número X de caracteres y la mitad la tiene el equipo de ingeniería y la otra mitad a un grupo de funcionarios de seguridad. Si se quiere trabajar en la máquina se requiere que dos grupos de personas se junten y hay una política de gestión de cambios muy estricta. Si alguien quiere hacer un cambio tiene que decir exactamente los detalles de lo que quiere hacer. Ambas personas en grupo se evalúan y tienen que decir lo que van a hacer para concretar el cambio.

En las operaciones normales el acceso a la máquina es XFR en entrada y salida solamente. Es decir, no hay orquestación externa ni nada por el estilo. Se accede a la máquina solo por la consola para hacer cualquier trabajo. La contraseña está en la partición encriptada y se hace a través del equipo combinado. Eso llevó al 2018. Fíjense que

desapareció el estrés. Mi bebita ya es un poquito mayor. Eso es todo. Gracias.

RUSS MUNDY: Gracias, Brett, por su actualización del Reino Unido. El que sigue es Patrik Fältström.

PATRIK FÄLTSTRÖM: Patrik Fältström, de Netnod. Hubo un interés de Suecia. Les prometo que voy a hablar de otros temas que les interesen. Como ustedes saben, para que quede claro, esto no es una actualización de .SE sino una actualización mía. No tengo ninguna diapositiva, no tengo ningún PowerPoint.

Noté hace unos segundos que hubiera sido bueno tener algunas diapositivas. A ver cómo funciona. Lo primero que diré es que fuimos los primeros en firmar. Lo hicimos mucho antes de que se firmara la raíz, al igual que muchos otros ccTLD. Algo que notamos y que quiero remarcar muy al principio es que la zona se firmó empujando la validación. Seguimos tratando de empujar la validación mucho y recomiendo que se haga. La comunidad no ha analizado la validación en las zonas firmadas formales. Nuestra experiencia después de 10 años es que esto no funciona. Hay que comenzar la validación. Hoy, de acuerdo con las mediciones que Geoff Huston está haciendo, tenemos un alto porcentaje de validación en Suecia pero no es el mejor en el mundo. Estamos un poquito antes de Noruega, lo cual para nosotros es mucho mejor. 0,1% mejor que Noruega. Sí, tenemos este jueguito

con nuestro vecino. Nadie puede ganar a mi hermano excepto yo. Si alguien ataca a mi hermano, yo lo defiendo. Entre nosotros, tenemos estas luchas amistosas.

Algunos números más. En este momento hay 1.77 millones de dominios en .SE. 800.000 están firmados. Si tienen algo de memoria, hay aproximadamente un millón que no están firmados. Eso significa que hemos tenido cierto éxito en la validación pero es mucho más fácil vender el concepto de la parte firmada cuando hay validación. Hablamos con mucho cuidado respecto del traspaso de la llave en Suecia porque había muchas cosas pero se traspasó la llave y si bien estábamos nerviosos, no hubo ningún problema.

Otra cifra interesante es que tenemos 86.000 nombres de dominio IDN. Algo interesante en Suecia en este momento, algo que supuestamente iba a pasar ayer pero se pospuso a hoy es el cambio de algoritmo de .SE de RSASHA1-NSEC3-SHA1 a ECDSA Curve P-256 con SHA-256. Hoy hablé a la mañana de que se suponía que iba a hacerse ayer. El cambio de algoritmo se postergó a hoy. No tengo más información técnica acerca de por qué se pospuso pero es lo que está pasando.

Hay dos URL, tendría que haber traído una diapositiva pero que voy a aportar a los materiales, en iis.se/se-tech/rolling-rolling-rolling. Es la información del cambio de algoritmo. Hay más información. Algo más que tenemos en Suecia es un señor muy loco que hace estas camisetas. También tiene un sitio web que es dnssecandipv6.se. Ahí tiene un mapa de los distintos países escandinavos y otros países más si quieren participar y mide si los municipios y las organizaciones, las

entidades han firmado adecuadamente su zona usando IPv6, si tienen los registros MX bien configurados. Es muy útil para las organizaciones. Es un desafío. Cuando los políticos no tienen absolutamente ninguna idea de lo técnico y dicen que se enorgullecen de participar y se dan cuenta de que sus ciudades están de color rojo cuando no están participando, sirve mucho.

RUSS MUNDY: Gracias, Patrik. Ahora vamos a escuchar qué nos cuenta Arianna, de Italia, sobre .IT.

ARIANNA DEL SOLDATO: Buenos días. ¿Por qué no podemos ver la diapositiva? Soy Arianna del Soldato, del registro .IT. No podemos ver la diapositiva en su totalidad. Les pido disculpas. Para nosotros, DNSSEC es el resultado de un largo proceso. Comenzó en 2014 en colaboración con el registro sueco y Netnod para consolidar el conocimiento tecnológico que ya existía en el registro .IT. En el 2016 se configuró un grupo de trabajo entre el registro y el registrador, y se decidió desarrollar el software. Unos meses después, en el mismo año 2016 se ofreció el acceso a una plataforma a todos los registradores. Esta es la plataforma de prueba que replica la plataforma de registración real con un servidor de prueba EPP, con una base de datos. Usamos BIND para firmar la zona. Es una zona distinta de la de producción.

También replicamos los servidores esclavos y el resolutor de prueba específico que el registrador usa para testear las operaciones para

hacer las queries de la base de datos. Había dos posibilidades de implementación en la interfaz de datos con DS. No tenemos interfaz web para administrar los servidores de DS. Lo hacemos a través del protocolo EPP. Tenemos un nuevo validador de DNS que tiene una interfaz web que el registrador usaba antes de firmar el nombre de dominio.

DNSSEC para nosotros no es obligatorio pero el registrador debe pasar una prueba de acreditación para poder registrar los nombres de dominio firmados. Los registradores acreditados son identificados a través de un logo específico en el sitio web que puede ser usado, lo pueden poner en su sitio web como una demostración de que están acreditados. La prueba de acreditación les permite hacer una reserva de su espacio de prueba. Reciben especificaciones técnicas que deben seguir para hacer la prueba como el nombre de dominio, la máquina que van a usar, el algoritmo que van a usar para firmar la zona. Tienen que registrar el nombre de dominio que no está firmado. Tienen que crear una KSK y una ZSK y luego tienen que transmitir el registro DS. No tienen límite de tiempo para probar esta prueba. La duración de cada prueba es de 90 minutos. Si hay un fallo, tienen que esperar una semana antes de poder hacerla otra vez.

Este es el estado actual de la situación. En 2016 la plataforma de prueba de DNSSEC se puso a disposición. En el 2017 se firmó la zona .IT. El registro DS entonces funcionó. En el 2018 se publicaron las nuevas guías técnicas que incluyen las especificaciones del DNSSEC. Un mes después, en septiembre, abrimos la prueba de acreditación

para el registrador. Finalmente, en septiembre tuvimos la primera acreditación del registrador y el primer nombre de dominio firmado.

Las cifras actuales. Ahora tenemos una sorpresa. Tenemos que cambiar esta carita porque ayer logramos tener seis registradores acreditados con 1.384 dominios firmados. En un día solo el registrador decidió enviarnos el registro DS de más de 1.300 nombres de dominio. Mientras tanto, organizamos un curso de capacitación sobre el DNSSEC dentro de la capacitación que les brindamos a los registradores y de la maestría de ciberseguridad organizada por el departamento de informática e ingeniería de la Universidad de Pisa. Gracias.

RUSS MUNDY: Gracias, Arianna. Un aumento significativo del número. Tenemos a José López, de .ES. Nos contará un poquito qué está pasando por aquí.

JOSÉ LÓPEZ: Bon día, buenos días, good morning. José López, del registro .ES. Voy a hablar de DNSSEC en el registro .ES. Empecemos con un poquito de historia. En 2006 creamos un laboratorio de prueba, un banco de prueba para saber un poquito más cómo funcionaba el DNSSEC, cómo implementarlo y demás. Luego, en el 2013, incluimos DNSSEC en el software de nuestro sistema de registro. Lo activamos en julio de 2014.

Algo de información sobre nuestra plataforma. Estamos usando BIND más OpenDNSSEC y un par de servidores HSM abiertos. Respecto de la política para la firma, hacemos traspaso de la clave cada dos años y

definimos esta llave cada tres meses. La plataforma ha sido bastante estable. Tuvimos un solo problema este año. Tuvimos tres errores aleatorios de DNSSEC. Al investigar dónde estaba el error, estaba en uno de los servidores HSM. Queremos agradecer a algunos registros como el sueco, el holandés y el danés que nos ayudaron a finalizar este trabajo y a encontrar el origen de este problema.

Algunas cifras. El número de dominios firmados está subiendo lentamente. Ahora tenemos 17.000 dominios firmados de 1.900.000 que hay en la zona. Ustedes sabrán que los registradores son muy importantes aquí. Los principales cinco registros que firman dominios están gestionando el 95% de los dominios firmados. Esperamos tener un aumento del 70-80% para finales de año en el número de dominios firmados con DNSSEC.

Los desafíos. Tenemos algunas iniciativas porque tenemos menos de un 1% de los dominios firmados. Queremos por supuesto aumentar esta cifra y también queremos tener más participación de los registradores locales para que incorporen DNSSEC y ver también cómo identificar más factores para promover el crecimiento. Además, estamos migrando. En lo que hace a la parte operacional estamos migrando de los servidores HSM hacia FIPS nivel 4. También hemos colaborado con la Agencia Nacional de Ciberseguridad para ver cómo ayudar a la gente a implementar DNSSEC. Tenemos actividades de concientización con ESNOG, que es el grupo operativo de redes nacional. Eso es todo. Gracias.

RUSS MUNDY: Excelente. Muy buena presentación. Ahora vamos a oír a Jaromir Talir, del registro .CZ que nos va a contar qué pasa en la República Checa.

JAROMIR TALIR: Yo soy de CZNIC. Les quiero contar un poquito qué está pasando con .CZ. Estamos lentamente llegando a la marca de 700.000 dominios firmados. Es aproximadamente el 53%. Hace poquito cruzamos la línea superando el 50% de los dominios firmados, lo cual es muy importante para nosotros porque ahora podemos decir que es normal tener DNSSEC. Es muy bueno para marketing. No obstante, en los últimos años, hemos visto un estancamiento. El crecimiento no es al ritmo que tenía antes.

También publicamos estadísticas sobre el soporte de algoritmos en la zona .CZ. Vemos que hay una gran prevalencia del algoritmo ECDSA a través de nuestros registradores más grandes. Hay tres registradores grandes que son los responsables de esta situación, que el algoritmo ECDSA o algoritmo 13 sea el más usado en la zona checa. También tenemos otros dos registradores más pequeños que migraron al algoritmo 14 que no es tan usual.

Con ese apoyo de ECDSA esperamos que haya más dominios TLD en la zona raíz. En este momento hay dos TLD que son .CZ y .BR. Hemos implementado la llave y lo hicimos en agosto. El .BR fue en agosto. Voy a darles una presentación más adelante sobre el traspaso.

Información ahora sobre el software que estamos desarrollando. Somos un registro de código abierto que es lo que están usando

también otros TLD recientemente. Hicimos una verificación de algoritmo de DNSSEC. Cualquier algoritmo puede ser incluido en el registro. En este momento se nos permite poner el algoritmo en el registro pero al menos ahora es posible configurarlo si uno quiere que no se permita que un algoritmo anterior quede en el registro y le explica al registro cómo configurarlo.

El año pasado implementamos el [inaudible] CDS/CDNSKEY. Les voy a mostrar algunas estadísticas. Nuestro software de DNS tiene una nueva versión que se publicó recientemente y que soporta el caching agresivo NSEC3 y también tenemos la implementación de sentinel KSK. Los servidores DNS autoritativos tienen también una KSK offline. Esto debería ayudarnos a utilizarlo en nuestro propio escenario donde tenemos este split management de KSK donde pregeneramos llaves prefirmadas con anterioridad y las firmamos offline, con lo cual, este escenario también va a ser respaldado. Cualquiera que utilice este escenario, me gustaría saber si esto es algo que les pueda resultar interesante. Eso es todo. Gracias.

RUSS MUNDY: Muchas gracias. Ahora vamos a escuchar a Paul Ebersman, de Neustar. Nos va a dar una actualización también.

PAUL EBERSMAN: Gracias. Neustar es una empresa comercial. Nosotros operamos registros y registradores. Tenemos servidores resolutores y también operamos operadores de DNS. Estamos en distintas partes de DNSSEC.

Nuestros resolutores han sido validados desde hace varios años. Hacemos validación de DNS en todas las consultas. Hacemos 10.000 millones de consultas todos los días y hasta ahora no tuvimos incidentes según nuestro [NOC] en el último año. El argumento de que DNSSEC es un poco frágil queda descartado de esta manera.

Somos una empresa comercial y nosotros soportamos casi todo en enterprise. Nuestra historia de zona firmada es un poco menor. Tenemos un porcentaje bajo de zonas firmadas. La cantidad de zonas que firmamos están en alrededor del 30% y de aquellos creo que son un 29 que están en secundarios y están allí firmando los datos. La mayoría es un proveedor de alojamiento en Suecia. Parte del desafío que yo escucho mucho con los clientes comerciales es que nosotros hacemos mucho del DNSSEC. Hacemos IP geográfica. También usamos Apex. Están mucho más interesados en trucos de DNS que en el trabajo del DNSSEC.

Yo soy relativamente nuevo pero para los que están allí hay nuevas características en el DNSSEC para que sea más correcto. Tenemos nuestro propio resolutor recursivo y nuestro propio resolutor autoritativo pero estamos en el camino de rediseñar el código. Una de las cosas que haremos es signing on the fly, con lo cual nos va a permitir mejorar un poco estos trucos del DNS y que de todos modos el DNS esté firmado.

En cuanto a otros usos, nosotros también estamos en una curva conservadora. El algoritmos nos ha permitido utilizar ECDSA en algunos casos pero la mayoría no lo han podido hacer. Como registro,

estamos mirando qué es lo que sucede con CDS suponiendo que ICANN no habla negativamente para hacerles la vida más complicada. Esta es otra cuestión que se está colocando en la hoja de ruta y espero poder tenerlo para el año 2019. ¿Hay alguna pregunta?

RUSS MUNDY: Gracias, Paul. Nosotros tenemos cinco minutos para preguntas para el panel. Antes de aceptar las preguntas quiero agradecer al panel por una excelente presentación. Ahora vamos a iniciar el espacio de preguntas para cualquiera en el panel.

RAED ALFAYEZ: Hola. Mi nombre es Raed Alfayez. Soy de SaudiNIC. Mi pregunta, como operador de registro, ¿ustedes creen que tenemos que chequear que los DS son válidos o no, o dejamos que el registratario suba lo que él quiera y que incluso pueda dañar su propio archivo de zona?

JAROMIR TALIR: Nosotros simplemente aplicamos el CDS y verificamos si la zona validada con la llave CDS es utilizada. Es decir, uno no puede romperla al publicar su propio record de CDS.

RAED ALFAYEZ: El problema aquí es que los clientes preguntan por qué uno no subió el [inaudible] nuevo.

JAROMIR TALIR: Nosotros tenemos algo que se llama portal de estado. Ahí se puede ver cuáles son los DS que están en el registro de CDS y cómo se implementaron en la zona madre. Así tratamos de responder la pregunta desde el principio. Voy a hablar más adelante sobre el CDS.

RUSS MUNDY: ¿Hay alguna otra respuesta?

ORADOR DESCONOCIDO: Nosotros tenemos un enfoque distinto. Pedimos que el registrador suba lo que quiera al registro. No es solamente DNSSEC. También son servidores de nombres. Lo que nosotros hacemos es verificaciones técnicas. Escaneamos regularmente e informamos al registratario que está haciendo algo mal. Son ellos los que tienen que corregirlo. Es un enfoque más liberal, diría.

RUSS MUNDY: Peter, adelante.

PETER KOCH: Gracias, Russ. Obviamente, estamos un poco sesgados porque hacemos verificaciones de predelegación desde el principio y decidimos aplicarlas al DNSSEC también. La razón es que es menos para proteger al registratario o al registrador pero especialmente en el caso de DNSSEC para evitar una protección negativa del DNSSEC como un todo. Es decir, es más bien una calidad del espacio de nombres general que evitar que la gente cometa sus propios errores.

PATRIK FÄLTSTRÖM: Creo que si se implementa una política hay que tener mucho cuidado en una situación en la que el registrador subió muchos DS porque no sabe si son nuevos o si son antiguos. Hay que tener mucho cuidado. También hay otra gente a la sala a la que le puede impactar en la responsabilidad de la zona de trabajo en relación con el cliente, ya sea registro o registrador y quién tiene la mayor responsabilidad va a depender, y hay mucha diferencia entre los distintos actores. Escuchamos a Dinamarca hablar sobre los distintos actores que también hay ahí y quizá deberíamos hacer algo para mejorarlo.

ORADOR DESCONOCIDO: Si es un DS o una llave DNS existente y tiene la información equivocada, se debe hacer saber que eso está incorrecto.

RUSS MUNDY: Muy bien. Creo que básicamente nos hemos quedado sin tiempo y tenemos que pasar a nuestro siguiente panel pero de nuevo les agradezco a todos los presentadores. Quisiera saber si hay alguna otra pregunta. En ese caso, pueden responderlo después. Esta comunidad ha sido muy buena en responder las preguntas individuales. Gracias, panelistas. Ahora tenemos a Frederico Neves, de .BR, quien recientemente se comprometió a la implementación del algoritmo y nos va a dar una revisión de cómo le fue.

FREDERICO NEVES: Buenos días a todos. Como se dijo, soy Frederico Neves. Trabajo para NIC.BR. En los últimos tres meses estuvimos trabajando en la implementación de un algoritmo para .BR. Les voy a dar una breve presentación y les voy a comentar cómo nos ha ido. Este es el resumen ejecutivo. 10 meses de preparación. Muchos testeos y escritura de software. Pasamos de RSA-SHA1 a ECDSAP256. Se ejecutó desde el 20 al 23 de agosto. Prácticamente no hubo problemas detectados o reportados.

Una breve introducción. .BR se firmó en el año 2007. Tuvimos más de 128 zonas hijas. Alrededor del 90% de los dominios están en COM.BR y otros de segundo nivel con delegaciones de tercer nivel. Fue firmado con RSA-SHA1. En este caso tuvimos dos implementaciones de KSK regulares. En 2010, justo antes de que se firmara el 2010, y luego en el año 2015. Durante esas dos implementaciones de KSK aumentamos el tamaño de la llave, de la KSK. Primero de 1280 a 1536 para la KSK. En el caso de CSK que utilizamos para las zonas de segundo nivel, para las zonas .BR pasaron de 1024 a 1280. Esos son los tamaños de las claves que teníamos antes de la implementación del algoritmo. 1280 para ZSK y 1536 para KSK.

La motivación fue mejorar la seguridad y básicamente estar preparados para la implementación del algoritmo porque utilizamos nuestro propio firmante. No teníamos el soporte necesario y por eso decidimos estar preparados para una implementación regular en un tiempo en el que no teníamos que hacer una implementación de algoritmo rápidamente.

El tamaño de la respuesta del DNS reducido fue otra motivación. Al menos desde el key set y RRSIG tenemos una reducción del 60% en el tamaño. Tenemos una mejor utilización y menos TCP. Otra motivación es que el stat que estaba aprovisionando el DNS fue escrito en el año 2004. Está un poco desactualizado. Tenía algunos problemas de mantenimiento con el código y deficiencias en la gestión de la memoria. Causaba algunas restricciones operativas también. Por eso movimos el registro hacia otro sector.

Tuvimos un dilema sobre cómo hacer la implementación del algoritmo. Ya lo habíamos presentado antes pero no voy a entrar en detalles. Decidimos entonces testear ambos métodos, el conservador y el liberal. Finalmente, entramos en otro modo que básicamente es la doble firma es mucho más simple. El problema en realidad reportado por RIPE en el pasado solo afectaba a una versión antigua. De todos modos, hicimos el testeo con 10.000 partes y no medimos ninguna diferencia significativa entre ambos métodos. La referencia está incluida en las diapositivas.

La implementación del algoritmo pasó de RSA-SHA1 con el tamaño de las claves. Aquí ustedes ven ECDSA. También tenemos CSK simple. Para el segundo nivel, pasamos de RSASHA1NSEC3 para algunas zonas y tenemos también lo mismo para otras zonas. Lo mismo con ECDSA y la llave desplegada para .BR.

La ejecución preliminar. Hicimos varias actualizaciones sobre el sistema de aprovisionamiento más allá del software. Actualizamos el software en el HSM para soportar ECDSA. Además de la generación de

la clave y la exportación a los cuatro HSM que tuvimos en los distintos tamaños, que nos tomó un poco de tiempo pero se hizo en una ceremonia separada tres semanas antes del traspaso.

Nosotros redujimos el TTL de algunos registros y así fue que aceleramos la implementación y pudimos llegar a un tiempo de implementación de siete horas para el CSK, especialmente para .BR, que es una zona muy grande. La implementación de la CSK para .BR comenzó a las 12:00 UTC el 20 de agosto. Fue una firma doble. Esperamos a cinco TTL para propagar la nueva clave. Ya estaban todos listos para el nuevo key set. A las 17:00 cambiamos el DS en la zona de .BR y el CSK se removió dos horas después.

La implementación de la KSK comenzó al mismo tiempo y a las 17:00 le pedimos a IANA que cambie el DS, que haga todas las confirmaciones. Gracias a IANA ellos lo hicieron muy rápidamente y así pudimos terminar la transición de la zona en el mismo día y tres días más tarde ya pudimos quitar la llave anterior de la zona .BR.

La cadena de confianza en la implementación de la CSK funcionó muy bien. Esto fue siete horas después de haber hecho el traspaso. La línea azul son las resoluciones seguras medidas por las mediciones que se hicieron. Como ustedes pueden ver, no hay ninguna diferencia perceptible de un algoritmo al otro. Los inseguros siguieron básicamente en el mismo número, dentro del mismo porcentaje. Un poquito menos del 40%.

Este es el tamaño del key set antes del traspaso. 638 bytes. Después 289 bytes. Estos son histogramas de respuesta positiva y negativa. El

de arriba es de un mes antes. Creo que fue durante el mes de julio. Como pueden ver, el que está más abajo es el que vino después del traspaso. Como ven, tenemos partes de respuestas negativas que están en el entorno a los 1.200 bytes. Después de la implementación fue de 800. Fue una gran reducción.

Aquí tenemos el CDS de la respuesta, antes y después de la implementación. El azul es RSA. El verde es el ECDSA después de la implementación o del traspaso. Como pueden ver, en la respuesta de 512 bytes teníamos antes 42% de la respuesta por debajo de ese umbral. Luego tuvimos 65%. El 99% de las respuestas ahora están por debajo de los 850 bytes. Antes era por debajo de 1.200 bytes. Es decir, que fue un buen cambio.

Este es el porcentaje de consultas TCP. De nuevo, la línea azul es la de julio. Esto se hizo en un periodo de unas 24 horas. Tuvimos picos del 3,5% en el transporte TCP. Ahora estamos cerca del 0,9%. Fue una muy buena reducción. Estas son las referencias. Si alguien está interesado, hay muchos datos. Esto es entonces lo que tengo hasta ahora. Tenemos cuatro minutos. Si alguien tiene alguna preguntita.

RUSS MUNDY: Muchas gracias, Frederico. ¿Hay alguna pregunta? Geoff.

GEOFF HUSTON: Entiendo entonces que ustedes han truncado los tamaños a menos de 1.200 y daban respuestas truncadas bajo RSA. A mí me parece un número muy bajo.

FREDERICO NEVES: Tuvimos algunas respuestas por encima de 1.280 pero sí, tuvimos tasas de consultas TCP más altas antes. Sí.

RUSS MUNDY: ¿Más preguntas?

FREDERICO NEVES: Fíjense en el gráfico justo antes de la implementación de la CSK con .BR. Justo cayó después de la clave e incluso después de la implementación. No mostré el gráfico. Tengo otro gráfico que muestra el periodo de siete horas en el periodo de tres días para la implementación de .BR y el volumen de queries TCP aumenta un 4,5%. Para ese momento teníamos un key set con aproximadamente 1.600 bytes. El gráfico es anterior. Era una situación regular de .BR. Otro comentario es que hacemos implementaciones regulares de la CSK. Hacemos prepublicación con un key set un poquito más grande.

RUSS MUNDY: Adelante.

DUANE WESSELS: Primero, felicitaciones. Muy bien hecho. Esto no está relacionado directamente. ¿Podría explicarnos por qué usaron una clave de firma combinada para las zonas de segundo nivel?

FREDERICO NEVES: El ZSK para .BR y la clave combinada para los segundos niveles, controlamos todo en el stack y cuando está totalmente integrado es mucho más simple tener una clave única en el segundo nivel. Por eso tenemos un key set más pequeño. Es el mismo software que en las implementaciones regulares. Fue más sencillo usar la clave combinada.

DUANE WESSELS: Gracias.

RUSS MUNDY: Yo tengo una pregunta. Ustedes dejaron TTL como parte de esto. ¿Monitorearon también la carga en los servidores para ver si hay alguna diferencia, si sube la carga o si se queda igual durante este periodo de bajo TTL?

FREDERICO NEVES: De hecho bajamos el TTL de las delegaciones DS e incluso en las delegaciones de NS dos meses antes. Solíamos hacer delegaciones de NS durante 24 horas. Las delegaciones de DS durante seis horas. La bajamos a una hora y esto aumentó la carga en un 30%, la carga de queries. Solíamos tener un número bajo de queries que aumentó un 30% pero ahora las mantuvimos en un ahora. Fue bueno para los clientes, en especial en lo que hace al soporte para los cambios de NS.

RUSS MUNDY: Gracias. Nos queda una muy rápida.

ORADOR DESCONOCIDO: Relacionada la mía con lo que decía Duane. ¿Pensaron usar la clave CSK para TLD? Sé que hay una cuestión de subir la clave por el tema de IANA, que no está automatizado. Si no fuera así el caso, ¿lo han considerado?

FREDERICO NEVES: Para la KSK usamos HSM. Lo hacemos a través del HSM. Está el problema de gestionar la relación con el padre. Creo que no sería posible usar la CSK para .BR.

RUSS MUNDY: Gracias. Muy interesante. Ahora estamos en el momento del receso. Debería haber café en el pasillo. Vamos a reanudar a las 10:30 y a las 10:30 nuestros panelistas van a estar en la mesa. Disfruten el café. Gracias.

[FIN DE LA TRANSCRIPCIÓN]