ICANN85 Mumbai | Foro de la comunidad – Sesión conjunta: ALAC y el SSAC
Domingo, 8 de marzo de 2026 – 13:15 a 14:30 IST

YEŞIM SAĞLAM

Hola, bienvenidos a la sesión conjunta ALAC y SSAC, yo soy Yeşim Sağlam, administradora de participación remota para esta sesión. Tengan en cuenta que esta sesión se está grabando y se rige por los estándares de comportamiento esperando de la ICANN, así como por la política antiacoso.

Durante esta sesión los comentarios y preguntas se van a leer en voz alta, si se envían al chat de la manera adecuada. Hay interpretación en esta sesión que incluye inglés, francés y español, si desean tomar la palabra durante la sesión, una vez que se diga su nombre los participantes virtuales podrán activar su micrófono en Zoom, los participantes que están en la sala utilizarán un micrófono físico, digan su nombre para los registros, el idioma en el que van a hablar, si no es inglés, y hablen a una velocidad razonable.

Le voy a dar la palabra a Claire Craig, vicepresidenta del ALAC y a Ram Mohan, presidente del SSAC.

CLAIRE CRAIG

Gracias. Hola a todos, buenos días y buenas tardes, bienvenidos a esta sesión conjunta entre el ALAC y el SSAC, siempre es una buena

sesión, estoy esperando a Jonathan, que debe estar a punto de llegar. Siento mucho no poder estar ahí con ustedes, espero que hayan comido bien durante el almuerzo.

Voy a repasar la agenda y después Ram podrá darles la bienvenida. Vamos a empezar dándoles la bienvenida, después vamos a hablar del DNSSEC para usuarios finales, el próximo punto tendrá que ver con los grupos de trabajo del SSAC y las prioridades para el año 2026, después de esto habrá una sesión de lluvia de ideas para la campaña de ciberespacio más segura y vamos a acabar con comentarios finales.

Antes de pasar la palabra, ¿por favor, pueden gestionar la cola de manera interna? Porque es difícil que yo vea quiénes tienen la mano levantada en la sala de Zoom y en la sala física, así que, les agradezco mucho si pueden hacer eso. Les doy la palabra a los que están en la sala para seguir la sesión.

RAM MOHAN Muchas gracias, Claire, por estar despierta a una hora tan loca, por así decirlo, muchas gracias por su dedicación. En cuanto a la gestión de la lista de oradores el staff del SSAC está aquí, me puede echar una mano, tengo acceso a la pantalla, pero no sé si voy a ser muy diligente a la hora de siempre ver lo que sale en ella.

Siempre nos complace venir aquí y hablar con ustedes en el marco del ALAC, tenemos muchas ideas compartidas que estamos poniendo en marcha, por lo que espero con impaciencia seguir con

los debates, con el comité y avanzar nuestros objetivos compartidos.

Queremos empezar con algunos miembros del SSAC, Matthias; ya lo conocen y Peter Thomassen, los dos están a mi derecha, van hablar un poco sobre DNSSEC, pero no desde la perspectiva típica técnica, sino desde la perspectiva de los usuarios finales, esto es lo queremos hacer, queremos tener una conversación con ustedes sobre esto, quizás vamos a compartir algo en directo con ustedes siempre que los dioses de las demostraciones lo permitan y podamos hablar sobre eso. Este es el modelo y le voy a dar la palabra a Matthias.

MATTHIAS HUDOBNIK Soy Matthias Hudobnik, yo soy el enlace del ALAC ante el SSAC y también soy miembro de SSAC. Mi objetivo hoy es explicarles los principios de la operación y las invitaciones que existen, para darles un poco de contexto, el DNS es el libro de números de teléfonos del internet, pero se diseñó hace mucho tiempo y hoy día tenemos que garantizar que las respuestas que nos dé este libro sean verídicas y que también podamos detectar cualquier problema que surja.

Podemos pensar en una consulta del DNS como una postal sellada y cualquier actor que esté en la ruta puede modificar esa consulta o borrarla y desviarlo a usted a otro sitio, por ejemplo, en lugar de llegar al sitio web de su banca, las extensiones de seguridad del DNS y la DNSSEC añade un sello, una firma a esa ruta, no existe un

descifrado, pero por lo menos se puede ver si se ha manipulado esa consulta.

Los dos objetivos que tengo con la presentación es que sepan que el origen se ha autenticado y el segundo aspecto tiene que ver con la integridad de los datos, es decir, saber que los datos no se han modificado a lo largo del camino. Próxima diapositiva.

Se utiliza la criptografía de la llave pública y el propietario de la zona tiene una llave privada para firmar sus registros DNS, se crea lo que se llama RRSEC, es una firma digital y un proceso de verificación, también se publica la llave pública del DNS y cuando se recibe la respuesta del DNS se utiliza la llave pública para verificar la firma, si la firma es válida los datos son auténticos y si no se rechazan.

Esta protección funciona cuando la zona está bien firmada y la validación de las DNSSEC funcionan, y sabemos que esto no es así para todo el internet hoy en día. Próxima diapositiva. Tenemos la cadena de confianza, la pregunta clave es, ¿quién o cómo podemos saber que la llave pública es legítima? Porque se puede publicar una llave falsa y aquí interviene la cadena de confianza, hay una jerarquía natural en el DNS y hay llaves de la madre, digamos, hay una cadena de delegación del firmante y hay una cadena que no interrumpe ningún sitio, por ejemplo, .COM, finalmente, llega a la zona raíz y esto es así para todo el sistema del DNS.

Dando un ejemplo negativo, el desafío de las DNSSEC es cómo gestionan las cosas que no existen, así que, en el DNS un hacker

podría crear un mensaje de no encontrado y redirigir a otro sitio, hay registros que se llaman NSEC, NSEC3, que demuestran que un nombre no existe, es decir, que no hay nada entre entrada A y entrada C.

En cuanto a la experiencia del usuario final, es muy importante porque la protección es invisible para los usuarios finales, este proceso es casi invisible, por ejemplo, no es necesario instalar una App de DNSSEC, normalmente el resolutor recursivo; ya proporcionado por parte del ISP, realiza una verificación, así que, sí devuelve una falla y puede parecer un enlace roto, pero realmente se trata de una protección, a veces las DNSSEC pueden estar desconfiguradas para un sitio web y esa es la respuesta que devuelve.

En cuanto a la última diapositiva, en pocas palabras, el DNSSEC da autenticación del origen, que es muy importante, y lo segundo es la integridad de los datos, por lo que ayuda que los cimientos del internet sean de fiar, es muy importante que se ponga en marcha y se mantenga de manera adecuada, no realiza un proceso de cifrado ni bloquea el malware y si no está bien implementada esta herramienta puede dar de baja un sitio web legítimo, así que, no es una barita mágica.

Le voy a dar la palabra ahora a Peter, que nos va a contar más información y nos va a explicar cómo las DNSSEC pueden ser un poco como el airbag de un coche.

PETER THOMASSEN

Les voy a dar algunas consideraciones prácticas. La DNSSEC no es una solución independiente de seguridad, sino que, existe en una serie más grande de medidas de seguridad, garantiza la seguridad de la información de los dominios y traduce los dominios a direcciones IP en cuanto al sistema de enrutamiento, así que, ¿qué parte del internet puede decir que se encarga de una serie de direcciones IP? El tráfico se dirige a esa parte de los dispositivos y el sistema de enrutamiento tiene que estar seguro para que las personas no puedan decir que son propietarias de una dirección IP y recibir su tráfico, eso tiene que ver con el RPKI.

Como dijo Matthias, añaden un sellado, no protegen el contenido o evitan que se inspeccione, así que, también se necesita la confidencialidad en los contenidos de la conexión, esto se llama "el cifrado" y se puede utilizar el enfoque TLS, esto se utiliza también para HTTPS. Cuando uno se conecta a un servicio web, o de chat, pasan tres cosas, se busca la dirección IP para ver si está segura, es decir, la integridad de los datos.

Entonces el primer paso sería la consulta de la dirección IP, que está asegurada con las DNSSEC, así que, tenemos la integridad de la información del dominio. El segundo paso tiene que ver con la preparación de la petición, es decir, el correo que queremos enviar, encriptarlo para el trasporte. El tercer paso consiste en enviar esta petición a algún sitio y el enrutamiento de eso se asegura con el

RPKI, estas cosas funcionan como un conjunto. Próxima diapositiva.

Aquí tenemos algunos ejemplos de los ataques contra los cuales protegen la DNSSEC, protege contra el secuestro de servidores de nombres, en 2019 hubo un ataque bastante importante, algunos lo llamaron un ataque de tortugas de mar, por algún motivo, para los registros que fueron atacados se cambiaron algunos servidores de nombres, esto afectó a agencias de inteligencia, ministerios, etc., pero también a proveedores de servicios de internet, entonces se redirige el tráfico a la infraestructura controlado por los atacadores y obtuvieron los certificados de cifrados válidos.

Hubo una alerta CISA del departamento de seguridad interna de los Estados Unidos y decía que el ataque iba a reorientar el tráfico a infraestructura controlada por los atacantes y que obtendrían un certificado de cifrado válido, y esto es porque cuando uno secuestra un dominio a nivel del DNS, se puede conseguir un certificado que se va a aceptar.

La cámara que maneja la estructura de muchos ccTLD, como podemos ver aquí, también fueron atacados, el ataque, en general, no tuvo éxito porque utilizaron las DNSSEC. Hay un video interesante en YouTube de parte de Bill Woodcock donde mostraba este link al PCH, ahí van a poder ver todos los detalles, en este caso, el servidor de nombres falso estaba instalado en el registrador, se redirigió el tráfico del DNS a allí, pero, como se utilizaba validación de las DNS, las respuestas a este servidor de

nombres falsos no eran aceptadas y, por lo tanto, la contraseña no fue hackeada.

Esto, en realidad, no fue directamente un ataque de spoofing en DNS porque, en este caso, los servidores de nombres cambiaron en la delegación. El segundo tipo de ataque que sería mitigado por parte de las DNSSEC es una ataque de Routing, en este caso, el atacante toma posesión de la dirección de IP de alguien más, por ejemplo, en el 2018 hubo un caso del servicio de DNS 53 de Amazon, esto afectó a los servicios de MYETHERWALLET.COM, terminaron atacando a los servidores, crearon un sitio web falso y robaron las criptomonedas por un total de unos $150.000 antes de resolver la cuestión.

En este caso, no se estaban utilizando las DNSSEC, pero si se hubieran utilizado los paquetes de IP para las solicitudes de DNS se hubiera terminado en el resolutor, pero, en este caso, no habría habido respuestas que hubieran sido aceptadas por los resolutores que tenían que realizar la validación. Las DNSSEC no solamente protegen de la manipulación directa, sino que, también protegen de ataques que hacen una explotación del DNS y ejecutan actividades a través de otro vector de ataque. Siguiente, por favor.

Hablé anteriormente de las tecnologías complementarias, RPKI, que protege el enrutamiento, está implementada en un 62% y los números siguen aumentando, esto es algo que no se introdujo hace mucho tiempo y la implementación aumenta porque esto es implementado por los ISP y por los registros regionales de internet,

no necesita la colaboración o intervención de los usuarios de internet, por lo tanto, no es necesario educar al público.

Para lo que es HTTPS, que protege contenido, la implementación llega a un 95% y esto es así porque después del escándalo de Snowden se comenzó a inventar la automatización; que ahora está incluida en una gran cantidad de software de servidores web, y en el caso de las DNSSEC, están implementadas en un 7%, esto es en relación a los nombres de dominios registrados y, según una lista que enumera a los 1.000 primeros, se dice que el número es bastante menor en cuanto otras tecnologías y la razón es la siguiente.

Se necesitan dos pasos para poder activar las DNSSEC, uno es que hay que firmar la zona, hay que crear las firmas y, por otro lado, el segundo paso, es que hay que ingresar información clave en el dominio principal y aquí se conecta con la cadena de confianza, como explicaba Matthias anteriormente. Siguiente diapositiva.

Cuando el registrador opera el servicio de DNS para el nombre de dominio, lo puede hacer, pero si es un registrador que difiere del proveedor de servicios de DNS, entonces el registratario tiene que también participar y, muchas veces, no están al tanto o comenten errores, entonces es un poco más complicado de automatizar, a diferencia de otras tecnologías.

Aquí les muestro algunos ejemplos de las diferencias en cuanto a los formularios, este es, en realidad, un formulario para que un

registrador introduzca un registro de DS a un nombre de dominio, esto lo pueden obtener del proveedor de DNS.

Aquí vemos otro formulario para lo mismo, parece un poco extraño, tienen que seleccionar varias cuestiones, también colocar otros componentes de registro de DNS y tiene varias instrucciones muy precisas. Siguiente, por favor.

Este es otro formulario para lo mismo y, creo que, ya entendieron lo que quería decir. Siguiente diapositiva. Las DNSSEC como un problema de accesibilidad, no es que la tecnología sea frágil, sino que, es difícil de configurar, entonces, en pos del interés de los usuarios finales, sería bueno si pudiéramos avanzar en hacer que sean más accesibles y un poco más automatizadas, no quiere decir que si uno las quiere utilizar no lo puede hacer, pero no es una cuestión de simplemente activarlas.

Hay soluciones disponibles para esta situación, si se elimina la intervención manual hay menos posibilidad de error, es más accesible y funciona de la siguiente manera. El operador del DNS del nombre de dominio le dice al registro que quiere activar las DNSSEC y puede probar que es una solicitud auténtica, lo muestro a nivel general en un ejemplo de cómo funciona.

Realizamos un seminario web con EURALO y otro grupo, hace un tiempo, donde mostramos una demo en vivo y, en realidad, tuvimos que esperar como una hora para que se actualizarán los archivos de zona en el TLD, aquí vamos a mostrar algunas capturas de pantalla, entonces ustedes pueden también consultar el

seminario web de EURALO y .CZ, en este caso, podemos hacer una consulta de decir: “Aquí está mi solicitud para activar las DNSSEC”, no lo tienen que hacer manualmente.

Una vez que se envía la solicitud del principal al secundario, el registro de .CZ lo va a observar, verifica la validez de la solicitud y lo pondrá en el registro de DS. Siguiente.

Este es el estado que aparece en el dispositivo analizador del DNS, esto es antes de registrar el seminario web como EURALO.CZ, en este caso, la zona .CZ devuelve el nombre de domino NX, una vez que registramos el nombre de dominio hay información adicional que tiene que ver con las firmas disponibles, pero falta el registro de DS; que es la cruz roja que vemos en pantalla, así que, inicialmente el dominio está registrado, pero no hay DNS sin interacción del usuario cuando se activa la automatización, esto es como una especie de airbag en un auto.

Hay cuestiones que se realizan en el background, entre el operador del DNS y el nombre de dominio principal, me parece que esto sería una buena manera de habilitar o permitir esta funcionalidad para aquellos registradores que no quieren lidiar manualmente con estas situaciones. Siguiente diapositiva.

El estado es el siguiente. Se utiliza en algunos ccTLD, yo mencioné como ejemplo a .CZ, pero también tenemos otros ejemplos como los ccTLD de Suiza, Suecia, Uzbekistán, Costa Rica, Liechtenstein, entre otros, lo importante es que debemos saber que los gTLD no son elegibles para este tipo de tecnología porque, como ustedes

saben, siempre el diablo habita en los detalles y hay algunas diferencias de implementación que existen.

Por ejemplo, cuando la registración tiene un bloqueo actualizado no queda claro si se puede habilitar la automatización de las DNSSEC, entonces hay cierta inconsistencia en la implementación que, primero, hay que abordar para que las cosas funcionen de la misma manera para los gTLD, así que, por el momento no se puede esperar que funcionen de la misma manera.

Existe un documento del IETF con recomendaciones sobre cómo efectuar todo esto, esto es un RFC, sería muy bueno si la automatización de las DNSSEC pudieran estar disponibles para todos los TLD que lo quieran implementar, esto podría maximizar nuestra interoperabilidad, hacer que las DNSSEC sean más accesibles, minimizar los errores, las sorpresas y también esto es parte de las recomendaciones que se hicieron con el SAC126, esto estaría en línea con ese documento.

Creo que, esto es un pantallazo general de cómo funciona y de la posibilidad. Con gusto voy a responder preguntas.

CLAIRE CRAIG

Muchas gracias, Peter. Quisiera aprovechar esta oportunidad de hacer una pregunta, usted habló de la dificultad de implementar las DNSSEC y me pregunto, ¿en los mercados pequeños las DNSSEC podrían implementarse a nivel de los puntos de intercambio de internet?

PETER THOMASSEN Los puntos de intercambio de internet, en realidad, se encargan de enviar y recibir paquetes de datos, conectan al que envía y al que recibe, esto está dentro de lo que es el área del enrutamiento donde se aplica la tecnología de seguridad de RPKI, allí sería la tecnología más adecuada, los nombres de dominios no están al nivel del punto de intercambio de internet, tampoco las DNSSEC.

CLAIRE CRAIG Muchas gracias. ¿Alguna otra pregunta?

RAM MOHAN Veo que Nath tiene una pregunta y Maarten también, así que, adelante.

MR. NATH Se mencionó que algunos ccTLD ya utilizan la automatización, ¿cuáles son los desafíos que se ven para otros ccTLD cuando esto se implemente y cómo se pueden promocionar o hacer que otros ccTLD lo implementen?

PETER THOMASSEN Yo no estuve participando en esta cuestión de hacer que otro ccTLD lo implemente, no sé exactamente esto cuando comenzó, creo que fue por el 2020, en ese entonces algunos elementos operativos como, por ejemplo, los bloqueos no habían sido aclarados.

¿Cuáles eran los desafíos? Es una buena pregunta. En el taller del DNS que, creo que, se va a realizar el miércoles, Olli Schacher dará un informe exactamente sobre ese tema, así que, sugiero que escuchen su contribución.

RAM MOHAN Muchas gracias. Amrita.

AMRITA CHOUDHURY Mi pregunta es la siguiente. Hemos visto que se ha realizado mucha capacitación en materia de los DNSSEC, lo han hecho los RIR, la ICANN, ¿esto tiene que ver con un cambio de consciencia de los ISP para la implementación? Porque desde la perspectivas de los usuarios finales no hay ningún rol, pero quizás desde el punto de vista de los ISP y otros, esto sí se hacía, entonces ¿es necesario algún enfoque descendente? Porque, muchas veces, estas cuestiones se tienen que ver desde el punto de vista del costo y la implementación, además, desde la estructura.

PETER THOMASSEN Sí, seguramente. Hay un tema de firma y de validación, en esto hay costos asociados, a veces ni las entidades ni las personas están dispuestas a pagar esos costos hasta que algo sucede, entonces el incidente de suplantación de identidad del servidor de nombres que sucedió en 2019, como mencioné, fue un punto importante, esto apuntaba a algunas organizaciones en el Medio Oriente y si observamos las estadísticas de implementación de las DNSSEC en

Arabia Saudita, bueno, antes de esto era el 20% y después llegó al 99%, entonces, por supuesto, hay cosas que tenemos que tener en cuenta.

SETONDJI HOUNZANDJI Voy a hablar en francés. Tengo una pregunta a título personal, soy ingeniero en informática y yo ya he implementado las DNSSEC en ciertos nombres de dominios y siempre me pregunto por qué no lo hemos hecho antes. Hoy cuando uno quiere configurar un servidor web, además de los certificados, se puede utilizar un código de escritura latino, hay que lanzar el código de escritura y el sistema nos indicará cómo hacer la configuración, entonces me pregunto por qué no lo hicimos también para las DNSSEC.

Mi pregunta tiene que ver con lo que usted hace. Tenemos en África ccTLD también, entonces ¿cómo se podría avanzar para asegurar que eso también se utilice o se implemente en África? Nuestro ccTLD es .BG y cuando quiero implementar las DNSSEC a nivel de los servidores tengo que crear claves, tengo que enviar la información a .BG, entonces con esto se tendría una actualización automática, me pregunto si esto podría tener un mayor impacto en los ccTLD de África. Gracias.

PETER THOMASSEN No estoy al tanto de ningún proceso en particular, pero el grado de dificultad va a depender mucho del software que se utilice, hay software que no es DNS o hay software que utilizan los registros,

FRED, por ejemplo, utiliza CZNIC, que es de código abierto, y también hay tecnologías de automatización para aquellos registros que las utilizan, no es muy difícil, hay que hacer la configuración, pero no la puede implementar uno mismo, entonces no sé exactamente cuál es el software que utiliza .BG, pero quizás yo o el resto de mi equipo podamos brindar asesoramiento, pero no hay un proceso en particular. No sé si respondí a su pregunta.

RAM MOHAN: No sé si alguien más quiere hablar. ¿Maarten?

MAARTEN AERTSEN: Es una respuesta corta para la pregunta que se hizo al principio de la sesión. No creo que haya nada que restrinja la implementación de las tecnologías de las cuales ha hablado Peter en mercados más pequeños, creo que, se centró en los puntos de intercambio en el DNS, pero si pasamos para esa parte nos podemos centrar en otras cuestiones, hay mercados pequeños y hay ccTLD que ya existen en mercados pequeños.

PETER THOMASSEN: Hace tiempo que existen las DNSSEC, pero la automatización es algo bastante reciente y es bastante difícil, se han dado muchas fallas, muchas configuraciones erróneas, apagones y quizás es un problema que tiene que ver con la imagen, hasta cierto punto hay un problema de imagen y de narrativa, algunas de las cosas han

cambiado porque la automatización puede hacerse de manera técnica hoy en día.

Hay un artículo de Bárbara que está aquí sobre esta cuestión y los animo a que lean ese artículo.

RAM MOHAN: Gracias por ayudarnos con la lista de oradores. Primero, Sébastien, Billy y luego Matthias, creo que, podemos acabar allí con la lista de oradores.

SÉBASTIEN BACHOLLET: Muchas gracias. ¿Cómo puedo garantizar que tenga las DNSSEC o no? ¿Qué puedo hacer desde la perspectiva de un usuario final del DNS?

PETER THOMASSEN: Maarten quiere responder.

MAARTEN AERTSEN: Si he entendido bien, la pregunta es cómo podemos verificar si todo está bien configurado, ¿o quiere añadir algo, Matthias? No. Hay herramientas que son fáciles de utilizar para comprobar si el dominio está bien configurado, una viene de mi país, se llama INTERNET.NL y permite realizar verificaciones, se puede poner el nombre y nos dice si las DNSSEC están configuradas para un nombre de dominio. También puede consultar si su ISP tiene la

habilitación configurada, así que, existen estas herramientas, hay muchas y una de las cuales es INTERNET.NL.

PETER THOMASSEN Desde una perspectiva práctica si compra un dominio hay un panel de administración y allí puede ver si Let's Encrypt está activado, puede ingresar en esa cuenta y lo puede activar, o no, creo que, muchos registradores ofrecen ese servicio, así que, se trata de marcar una casilla.

RAM MOHAN Gracias. Billy.

VASYL "BILLY" BRATCHENKO Dijo que cuando recibe errores es una tentativa de intercepción, o es que algo está mal configurado, ¿hay una manera técnica de saber si realmente se trata de una tentativa o si es una falla de configuración?

PETER THOMASSEN Es muy difícil detectar esto. Como dijo Matthias, las DNSSEC es el guardaespaldas silencioso y si se equivoca el guardaespaldas porque recibe instrucciones equivocadas, se bloquea el acceso, pero automatizar estos procesos es lo que debe prevenir esto. Los certificados HTTPS son procesos parecidos con esto y cuando se puso en marcha Let's Encrypt veíamos muchos certificados caducados, pero hoy en día ya es mucho más raro.

MATTHIAS HUDOBNIK Sí, si está interesado puede consultar el seminario web que realizamos con EURALO porque participaron muchas personas de Cloudflare, de CORE, de .PT y Bárbara también hizo una presentación, por lo que si tiene interés dura hora y media y puede aprender mucho de esa sesión, voy a ver si puedo poner el enlace en el chat. Gracias.

RAM MOHAN Creo que, hay una pregunta entre el público.

AVIRAL KAINTURA Gracias a Peter y Matthias por explicar las DNSSEC. Desde la perspectiva del usuario final cuando falla una validación de las DNSSEC y vemos que sale un error del servidor genérico, sabemos que los problemas subyacentes pueden ser varios, entonces puede significar que hay muchos problemas subyacentes, puede ser un problema de seguridad o una mala configuración, así que, ¿desde la perspectiva del usuario final puede haber una manera de tener más transparencia acerca de qué está sucediendo? Gracias.

PETER THOMASSEN Perdón, estaba distraído, ¿puede repetir la pregunta?

AVIRAL KAINTURA Cuando falla una validación de las DNSSEC, sale un error, un error genérico, por lo que puede significar muchas cosas, quizás una

mala configuración o una cuestión relacionada con la seguridad, quería preguntar entonces, ¿desde la perspectiva del usuario final existe la posibilidad de tener más transparencia para saber qué está sucediendo?

PETER THOMASSEN

Sí y no, es cierto que el código de error es bastante genérico para cualquier tipo de error, hay varias extensiones para el DNS, por ejemplo, los códigos de errores extendidos, no sé exactamente cómo es el nombre, y permite que el resolutor incluya un dato en la respuesta para decir qué ha pasado, qué ha fallado, por ejemplo, la llave o la firma estaba caducada. Aunque se tenga esto, esta información no se muestra en el navegador porque de normal el navegador pide al ISP una dirección IP y eso es lo que recibe, por lo que no se puede mostrar a nivel del navegador, el IETF está trabajando para cambiar eso y quizás en el futuro los navegadores pueden mostrar información más avanzada y explicar por qué no se puede llegar a un sitio, por ejemplo, porque hay un filtreo del DNS.

Sé que hay trabajo en curso, pero me parece que aún quedan unos años para que esto se pueda poner en práctica. Y la pregunta más interesante aquí no es cómo puede terminar el usuario final, cuál es el problema, sino que, aquí lo importante es que el operador sepa qué pasa para que lo pueda resolver, los resolutores pueden transmitir la información al operador una vez que se observa el error y así arreglar, por ejemplo, las malas configuraciones.

RAM MOHAN

Voy a cerrar ya la lista de oradores porque me parece que es un tema muy interesante y hay muchas preguntas al respecto. En línea está Mourad.

MOURAD MELLITI

Buenos días a todos, quería volver a esta cuestión de la seguridad, ¿es suficiente tener las DNSSEC en la zona raíz? ¿O no? Intervienen muchas partes interesadas en la seguridad de un dominio, no solo el registrador o un registro, sino que, los proveedores de servicios también intervienen y ofrecen las DNSSEC a los usuarios finales, y aquí existe una diferencia en lo que se refiere a esta cadena para que el dominio esté firmado y seguro no es suficiente con proteger la zona raíz.

Me encargo de .TN, que está seguro desde 2014, pero hay registradores que no ofrecen las DNSSEC, utilizamos el nombre de dominio DNSSEC.TN, entonces la activación de las DNSSEC para los ccTLD o los gTLD no siempre es la mejor solución para que se active de manera automática, quiere decir que los registradores también tienen que ofrecérselo a los usuarios finales.

Y quería volver a esta cuestión porque me parece importante implicar a todas las partes interesadas.

PETER THOMASSEN

Efectivamente es un problema que implica a todas las partes, pero a fin de cuentas cuando activamos las DNSSEC a nivel de dominio

y a nivel principal el registro DNS está configurado y esto se tiene que transmitir al operador del nivel secundario, el registrador es un intermediario, pero es así. Y si encontramos la manera de que llegue esta información, por ejemplo, si hablamos con Cloudflare, si se lo pedimos, puede activar las DNSSEC directamente y es posible también que el registrador active el proceso automatizado, es una cuestión de política, parece que sería más fácil si el registro asumiera el trabajo, en lugar de los registradores.

Si tiene más interés en las consideraciones detalladas sobre esta cuestión en una parte del documento de recomendaciones operativas está… Está el enlace a este documento aquí en el centro, el registrador puede implicarse, pero no tiene por qué.

RAM MOHAN Sí, gracias, Peter. Robert.

ROBERT GUERRA Quería volver atrás un nivel, hemos hablado de los problemas que surgen, pero no perdamos de vista que esto tiene que ver con la autenticidad y la integridad de los datos, cómo ayudó la implementación del HTTPS, Let's Encrypt, también se trata de hacer pedagogía, es importante que todos sepan que existe esta elección, los registradores pueden tener la opción de activar las DNSSEC y así puede haber un mecanismo más eficaz de autenticidad.

La elección recae sobre el usuario, pero es una elección bastante importante, hay cada vez más ataques contra la infraestructura y otras cuestiones, así que, elegir el registrador adecuado que tenga características que nos pueda ayudar, sin duda, es importante para los usuarios, así que, no perdamos de vista esto ni en callarnos en otras cuestiones, hay registradores que sí lo están implementando y esto va a ir cada vez a mejor, los códigos de errores que salen van a ser mejor en el futuro y quizás si se da un error podemos buscar si el registrador proporciona esta información.

Muchas personas piensan que es una elección entre registradores que tiene que ver con el costo, pero no es solo eso, tenemos los códigos de errores, los mensajes y esto me parece bueno que se implemente, va a ser, tal vez, más fácil.

RAM MOHAN: Gracias, Robert. Casi estamos llegando al final de esta parte de la sesión y Frederic tiene la palabra.

FREDERIC TAES: Gracias, ha sido muy interesante. Organizamos una mesa redonda sobre las DNSSEC y fue muy bien, el feedback que recibimos fue muy positivo, entre el 80% y 100% se convenció para implementar las DNSSEC tras eso, es algo bastante complejo, abstracto y explicamos cómo las DNSSEC constituyen un valor añadido. En cuanto a las preguntas sobre los usuarios finales, EURALO ha desarrollado una extensión para navegadores para mejorar la

fiabilidad del DNS y los nombres de dominios, es gratis, pueden acudir a Trustworthiness.org y está disponible también en el sitio web.

Así los usuarios pueden ver si las DNSSEC están implementadas para tal nombre de dominio porque no es fácil encontrar esa información sin esta extensión, además, se proporciona otra información acerca de los nombres de dominios. Muchas gracias.

RAM MOHAN Muchas gracias por ese feedback y gracias por compartir con nosotros que la sesión fue buena, esto refleja el trabajo que realizan los equipos que son capaces de entender la jerga técnica y explicárselo a las personas en un lenguaje más sencillo.

FREDERIC TAES No solo había personas de la comunidad de la ICANN, sino que, acudieron empresas, expertos en seguridad de internet. Gracias.

RAM MOHAN Muchas gracias. Adelante.

JONATHAN ZUCK Sí, fue una sesión grabada quizás podemos extraer esos segmentos que son útiles para dar explicaciones y ponerlo a disposición de los demás, creo que, es una buena costumbre que podemos tener, si no les importa.

FREDERIC TAES Sí, muchas gracias, Jonathan. Estamos mejorando nuestra faceta de comunicación en LinkedIn, en nuestras plataformas, así que, queremos publicitar esto entre todos.

JONATHAN ZUCK Sí, tiene una diosa de las redes sociales al lado.

NATALIA FILINA Muchas gracias por haber organizado esta mesa redonda sobre las DNSSEC, Joly MacFie de ISOC ayudó muchísimo, estuvo muy bien estructurada, hubo resúmenes cortos, grabaciones… Así que, voy a poner el enlace en el chat para compartir esta información, muchas gracias, de nuevo.

RAM MOHAN Creo que, el SSAC y el ALAC nos podemos quedar con lo siguiente. Decimos que, es bueno automatizar, hace que las cosas sean más fáciles y estas herramientas permiten que haya menos errores y que la complejidad de este tema se puede tapar con un proceso automatizado, entonces estamos trabajando sobre esto también dentro de la ICANN, SSAC publicó un informe sobre la automatización hace tiempo. También animamos a los gTLD a que empiecen a automatizar procesos estandarizados, así que, cuando se dé una discusión política sobre esto nos gustaría que nos

ayudaran con lo que hacemos nosotros, que es la parte más técnica.

Nos queda poco tiempo, así que, lo que vamos a ir directamente al tema de la campaña de ciberseguridad y, en este caso, Jonathan nos va a contar hacia dónde queremos ir, para quienes no conocen del tema el SSAC y el ALAC en los últimos tiempos han participado en diferentes conversaciones productivas y han materializado esas conversaciones a través de contenido y el ALAC tomó ese contenido y lo transformó en material educativo muy interesante, excepcional diría, donde hay texto explicativo, es decir, sacaron todas las partes técnicas, por ejemplo, qué pasa o qué tiene que hacer uno cuando sufre phishing y lo transformó en material muy adecuado y útil para los usuarios finales.

Entonces queremos compartir con ustedes cosas que estamos haciendo con otras partes de la comunidad, lo queremos compartir con ustedes y, por supuesto, después queremos hacer una tormenta de ideas para ver qué más podemos hacer.

JONATHAN ZUCK Ah, o sea que se están viendo con otras personas también.

RAM MOHAN Sí, no sabía, pero sí. Pasemos a la siguiente diapositiva.

A comienzo de este año comenzamos a colaborar con la ISPCP y ahora hemos anunciado coordinación con la ISPCP una serie de seminarios webs en las reuniones de la ICANN sobre varios temas,

cada uno de estos temas son temas en los cuales el SSAC tiene interés, pero también sobre los cuales hemos brindado contenido y material, lo que estamos haciendo con los ISP es lo siguiente.

Ellos brindan la sede, la red de distribución y nosotros brindamos los expertos técnicos para que den las disertaciones, estuvimos presentes en febrero… No sé si quiere contar brevemente quién estuvo allí, cómo fue, etc., y luego cuento el resto.

ORADOR NO IDENTIFICADO Creo que, eran 107 personas y tuvimos un debate muy interesante sobre la automatización del DNS, la prevención del uso indebido y la mitigación, hubo también algunas preguntas relacionadas con la Inteligencia Artificial, que es algo que está muy candente en nuestro grupo, y también tuvimos diferentes actividades.

RAM MOHAN Bueno, verán en la pantalla que hay algunas que son más relevantes para los proveedores de hosting en un ISP y esto, creo que, es como un punto de partida para preguntarnos qué más podemos hacer, Jonathan.

JONATHAN ZUCK Nosotros formamos dentro de ALAC un subgrupo, que se llama ACES, y es un grupo que está creando el curso de phishing, pero también buscamos otros medio de información, seguramente habrán escuchado de las RALO, de las ALS y las ALS que tienen sus propios miembros, entonces la idea es cómo hacer llegar esa

información hasta allí, hay diferentes métodos, podría ser una campaña de Twitter (X), o también podría ser una llamada telefónica, podría ser un seminario web, un seminario general, etc.

Una de las cuestiones que consideramos fue una campaña vía Twitter (X) que tiene relación con la Aceptación Universal, pensamos lo siguiente. Buscar una marca global que no haya implementado todavía la Aceptación Universal y ver cuántos tuits podíamos enviar a esa marca global. La ICANN está trabajando muy intensamente para contactarlas, pero no sé si había una encuesta y no sé si hay algo automatizado que se pueda hacer, pero tiene que haber una manera en que la gente pueda recibir la información de una campaña del DNS.

Sébastien habló sobre la pregunta de la automatización y el usuario final, entonces si saben que un ISP no lo tiene hay alguna manera en que nosotros podamos ayudarlos, por ejemplo, quizás le podemos contar, pero si nosotros utilizamos nuestra red para comunicarnos con grupos más grandes, a modo de experimento, ver si podemos crear consciencia y también fomentar la implementación o la automatización, bueno, quizás todo esto pueda ser posible si pensamos en formas de identificar a quién le tiene que llegar el mensaje.

Entonces, probablemente, podamos movilizar nuestra red para que lo efectúe, finalmente, ¿qué le parece?

RAM MOHAN

Yo voy a hablar a título personal. Desde hace muchos años en la comunidad de la ICANN, si tomamos a las DNSSEC, por ejemplo, las tratamos como un tema técnico y dedicamos mucho tiempo a explicar la tecnología y a desmitificarla, pero cuanto más lo intentábamos más mística se volvió y después teníamos las implementaciones de las DNSSEC, había algunos errores de implementación, ciertos problemas, había informes que decían: "Este TLD puntual tuvo un problema a raíz de las DNSSEC".

Entonces en el SSAC lo que hacemos son dos cosas, por un lado, tomamos la tecnología y la explicamos de una manera que sea más accesible y amigable para el usuario. Por otro lado, tenemos un grupo de trabajo que, se supone, va a terminar su trabajo a finales de este año y que trabaja sobre las consideraciones operativas para las DNSSEC. Uno de los temas no tratados, por así decirlo, es que las DNSSEC son complejas desde el punto de vista operativo y por eso hay ciertas organizaciones que pueden decidir que no las tienen que aplicar.

En algún momento Warren mencionó, por ejemplo, el tema de las propiedades o sitios más visitados de internet, muchos de estos no tienen implementada las DNSSEC y no es una cuestión de capacidad, sino que, hay otras razones por las cuales no las implementan. Si se quiere implementar las DNSSEC, ¿qué es lo que tenemos que hacer para prepararnos? No solamente para implementarlas, sino para también mantenerlas, es decir,

implementarlas y continuar trabajando de una manera que sea segura y operativa.

JONATHAN ZUCK Entonces, ¿cuál es el mensaje que se quiere dar?

RAM MOHAN Bueno, es exactamente eso, creo que, en el caso de las DNSSEC, vamos a tener que pensar. Si el usuario final no tiene acceso a las herramientas y ni siquiera comprende el valor o el beneficio de las DNSSEC deberíamos, por ejemplo, centrar nuestra energía en los intermediarios y después explicar el valor a los consumidores, en lugar de tratar de involucrarlos directamente, lo podemos pensar.

JONATHAN ZUCK Cuando hablamos de los usuarios finales esto es un poco más sofisticado, si uno es parte de una ALS seguramente haya un capítulo de ISOC o alguna empresa relacionada con la seguridad, por ejemplo, Donna en Massachusetts, entonces ellos tratan de operar en beneficio o en pos del beneficio de los usuarios finales. Creo que, muchos no tienen la sofisticación necesaria para poder implementarlas, pero sí se puede llevar el mensaje y si saben a quién llevar el mensaje eso seguramente pueda ayudar, tenemos que determinar quién es la audiencia para que nuestros miembros puedan llevar el mensaje y ayudar a esos usuarios o a esas personas a implementarlo. Eso, creo que, es el camino a tener en cuenta.

RAM MOHAN Tenemos a Russ y después a Hervé, Amrita y Sébastien que quieren tomar la palabra.

RUSS MUNDY Yo quiero responder a la pregunta de Jonathan en relación a con quién hay que hablar. En muchos casos, las personas que están en el campo de trabajo, por así decirlo, tienen un mejor conocimiento de a quién se deben dirigir y es mayor que el conocimiento que tiene el SSAC en ese sentido, es decir, a lo largo de los años en muchas oportunidades hemos escuchado de varios proveedores y registradores en particular que no hay demanda para las DNSSEC, nadie las pide, entonces cualquier interacción que se pudiese tener, ya sea con los ISP o con los registradores, o los registros, donde se les pida apoyo para el servicio de DNSSEC es algo importante de hacer.

Creo que, la mayoría de las personas en ALAC o en las ALS están al tanto de la importancia de las DNSSEC y de la necesidad de utilizarlas, creo que, son los más adecuados para llevar el mensaje. Yo puedo decir, por ejemplo, que se puede cambiar el registrador porque hay otros registradores que están utilizando un servicio que no soporta las DNSSEC, entonces ir a otro registrador es otro nivel, no en todos los casos, pero en muchos casos sí. Gracias.

RAM MOHAN Muchas gracias. Setondji.

SETONDJI HOUNZANDJI Me gustaría traer esperanza, hablamos de la Inteligencia Artificial de los inconvenientes relacionados con el uso indebido del DN, pero debo decir también que hay muchos beneficios en relación a la Inteligencia Artificial que permitirían una mejor implementación de las DNSSEC. Todo el mundo teme o no sabe cómo crear una llave, sé que hay respuestas, también sé y espero que cada vez más los nombres de dominios implementen las DNSSEC.

RAM MOHAN Muchas gracias. Sí, creo que, también mantener la esperanza muchas veces nos aleja de la felicidad. Amrita.

AMRITA CHOUDHURY Dos puntos. Uno es una pregunta, ¿queremos promover las DNSSEC? Porque, como se mencionó, hay varias compañías que eligen no implementarlas y entender esto es una parte del trabajo. Y dos, para Jonathan, obviamente necesitamos ayuda, pero si observamos el mundo de los ISP vemos que hay diferentes ISP, hay ISP que están en países en desarrollo y otros que son gestionados por una o dos personas, hay categorías, hay niveles educativos en cuanto a la gestión e incluso el conocimiento de lo que sucede a nivel global es diferente, entonces, para mí, la creación de capacidades es importante para todos.

Jonathan, en caso de que estemos pensando en una campaña, bueno, hay que considerar este tipo de cuestiones, ver qué es lo

que tenemos que hacer y luego relacionarla con alguna página que tenga el SSAC o la ICANN con información de recursos que puedan consultar porque tener la información correcta, a veces, es complejo, es difícil y, a veces, no es así, entonces si podemos tener este tipo de información tenemos que pensar qué tipo de campaña podemos hacer y desde At-Large lo podemos hacer para las RALO.

Si hay una empresa un poco más grande en la que queramos pensar, podemos entonces identificar una, preguntarles si están listas para la implementación de las DNSSEC por cuestiones de seguridad y luego ver. Eso sería también algo que podríamos hacer y son las ideas que me surgen en este momento.

RAM MOHAN Adelante, Sébastien.

SÉBASTIEN BACHOLLET Muchos de los temas que ustedes pusieron aquí quizás también sean de interés para nosotros como usuarios finales, probablemente tengamos que pensar de qué manera podemos trabajar con la ISPCP y con At-Large, pero hay dos temas para la reunión ICANN86 que a mí en lo personal me parece de mucha importancia porque el post quantum no es eso y no es mañana, tenemos que discutir de qué manera lo podemos abordar como usuarios finales y quizás tener un programa un poco más amplio.

RAM MOHAN Seguramente con gusto podemos trabajar conjuntamente y, como dije, esto lo puse como simplemente un punto de partida para la conversación. Maarten, adelante.

MAARTEN AERTSEN Yo quisiera saber si ALAC quiere que Peter vuelva una vez que terminemos con estas cuestiones de la automatización porque, como se mencionó anteriormente, hay trabajo en curso, pero bueno, quizás cuando esto termine me parece que sería bueno comenzar a hablar de las campañas y todo ese tipo de cuestiones.

SÉBASTIEN BACHOLLET Perdón. Hablemos de At-Large, nuestros 15 miembros de ALAC lo necesitamos, pero también los millones de usuarios necesitamos más todavía.

RAM MOHAN Perdón, ¿tiene una pregunta?

KARAN Mi pregunta es la siguiente. Si el uso indebido del DNS es un tema tan importante y las DNSSEC parecen tener tantas limitaciones, ¿esta iniciativa qué respuesta nos da con respecto a estas limitaciones? Porque tenemos la campaña de ciberseguridad, que es una.

RAM MOHAN

A ver, el uso indebido del DNS particularmente dentro del contexto de la ICANN… Bueno, en este caso, las DNSSEC son una parte muy pequeña, hay otras cuestiones que surgen, si préstamos atención, en la GNSO hay un PDP sobre uso indebido del DNS que tiene relación con os nombres de dominios asociados, entonces hay trabajo que se está realizando en este sentido.

Las DNSSEC no son la solución definitiva para el problema del uso indebido del DNS, en el SSAC acabamos de comenzar con un grupo de trabajo que se encarga de estudiar el impacto de la Inteligencia Artificial en el uso indebido del DNS, acabamos de empezar ese trabajo también en esta área, así que, esto es para estar atentos porque seguramente haya más trabajo por delante.

JONATHAN ZUCK

Sí, hay un PDP nuevo sobre las consultas de nombres de dominios, hay otro PDP que tiene que ver con las registraciones masivas y la IA, hay programas de identificadores fiables, hay también cambios a los contratos que requieren una mitigación inmediata. OCTO, como parte de la ICANN, ha empezado a construir más herramientas para al menos entender de dónde sale, de dónde procede el uso indebido del DNS, así que, va a haber muchos caminos para abordar este problema que nunca se va a resolver del todo, pero están pasando muchas cosas al respecto.

RAM MOHAN: Muy bien, creo que, ya podemos cerrar la sesión, muchas gracias, Jonathan y Claire, por acogernos, siempre es un placer venir aquí, la calidad y profundidad de las conversaciones que hemos tenido hoy refleja la relación que estamos construyendo, pero también refleja la calidad y el interés que hay por lo que estamos haciendo conjuntamente.

JONATHAN ZUCK: Muchas gracias, siempre es un placer que vengan a hablar con nosotros, ya lo dije, hacen mucho trabajo excelente y no queremos que ese trabajo acabe como una tesis doctoral, que acabe en una biblioteca, sino que, tiene que llegar al público adecuado. Muchas gracias.

**[FIN DE LA TRANSCRIPCIÓN]**