ICANN79 | Foro de la comunidad – Cómo funciona - Sesión 3: cómo proteger sus prácticas operativas de DNS
(todo sobre KINDNS)
Domingo, 3 de marzo de 2024 – 3:00 a 4:00 SJU

NICOLAS ANTONIELLO: Hola y bienvenidos todos a la sesión sobre cómo funciona todo acerca de KINDNS. Yo seré el coordinador de participación remota para esta sesión. Tengan en cuenta que esta sesión está siendo grabada y se rige por los estándares de comportamiento esperado de la ICANN. Durante la sesión, solo se leerán en voz alta las preguntas y comentarios si se presentan en la ventana de preguntas y respuestas. Si desean tomar la palabra durante la sesión, levanten la mano en Zoom, y cuando lo llamen por su nombre, tendrán la posibilidad de habilitar su micrófono en Zoom. Los participantes presenciales utilizarán un micrófono de sala para hablar. La interpretación para esta sesión incluye inglés, francés, árabe y español. Por favor digan su nombre para los registros y el idioma en el van a hablar si es que no hablan en inglés. Y por favor hablen a un ritmo razonable. Habiendo dicho esto, le doy la palabra a Adiel Akplogan.

ADIEL AKPLOGAN: Gracias, Nico, y bienvenidos todos a esta sesión acerca de KINDNS. KINDNS es una iniciativa que comenzó la ICANN hace unos pocos meses y que se lanzó hace un año y medio exactamente. Es una iniciativa que constituye una herramienta adicional para lo que venimos haciendo

desde hace varios años, que es promover las mejores prácticas en la operación del DNS considerando los diferentes componentes del DNS. Y nuestro objetivo es simplificar esas prácticas para los operadores de forma tal que de manera simple y sencilla puedan implementarlo en sus marcos operativos.

Entonces, KINDNS es un intercambio de conocimientos e instauración de normas para la seguridad del DNS y de la asignación de nombres. Se trata de conocimientos compartidos que tratamos de enmarcar dentro de un único acceso. Hay un sitio web que ofrece más información sobre el programa y que brinda datos detallados acerca del marco, cómo participar y, lo que es más importante, ofrece una herramienta de auto evaluación que desarrollamos, de modo que ustedes ya pueden empezar a mirar el sitio web.

Tal como dije, si están muy familiarizados con el DNS o no, quizás estén familiarizados con el proyecto que trata de identificar todos los aspectos relacionados con el DNS. Y son muchos. Si ustedes son operadores de DNS, ya sea resolutores o autoritativos, y quieren estar al tanto de toda la información relacionada con el DNS y tienen que operarlo, tienen que dedicar mucho tiempo a esto. Y esto implica realmente mucho tiempo, ya sea que se traten de un operador grande o pequeño, implica mucho tiempo. Los operadores grandes pueden dedicar todo un equipo a este trabajo, pero los más pequeños a veces quedan perdidos aquí.

Entonces, la idea era trabajar con la comunidad, obtener retroalimentación de los operadores que están en el campo y generar

un marco muy simple y claro que cualquiera pueda seguir, que cualquiera pueda tener como objetivo también. KINDNS no implica solamente decirle a la gente que lo haga ya, sino darles un objetivo al cual llegar. Apuntamos a llegar a ese nivel de madurez de la operación del DNS siguiendo este marco. Ese es el objetivo. Trabajamos con la comunidad durante un año a través de la lista de correo electrónico de KINDNS, recibimos aporte de operadores para poder llegar a las mejores prácticas más importantes para enmarcarlas y para publicarlas para que la gente se pueda autoevaluar y también para poder participar como embajadores o promotores de las mejores prácticas.

A lo largo de todo este proceso de debate y de recepción de aportes, llegamos a cinco categorías diferentes de mejores prácticas. Dos son específicas para los operadores de servidores autoritativos. Y aquí también las dividimos en dos. Operadores de zonas críticos u operadores de TLD, porque pensamos que estas empresas están a cargo de servidores autoritativos clave que quizás tengan estándares un poco más elevados en sus prácticas. Y luego tenemos los operadores de SLD, que son operadores. de segundo nivel. Eso implica cualquiera que tenga un nombre de dominio que tiene la responsabilidad en relación con ese dominio de segundo nivel.

Y estos dos requieren una serie de mejores prácticas específicas. Y luego tenemos los operadores de servidores resolutores también, que también desempeñan un papel importante en el ecosistema del DNS. También tienen diferentes prácticas que deben implementar o las que deben apuntar. Y aquí tenemos tres categorías diferentes. Tenemos los operadores de resolutores cerrados y privados, es decir, aquellos que se

utilizan en un entorno muy controlado. Tenemos privado compartido, que en general son operados por los ISP en nombre de sus clientes y los comparten con aquellos con los que deciden compartirlo. Entonces, no es totalmente público, como lo que vemos en un entorno corporativo, por ejemplo. Es privado, pero con un cierto grado de uso compartido.

Y luego tenemos los resolutores públicos, que son aquellos que están abiertos a cualquiera. Tenemos algunos que son muy conocidos, como el 8.8.8, que es operado por Google. Y en estas tres categorías de resolutores tenemos una serie de mejores prácticas que recomendamos implementar. Y como una especie de práctica transversal, tenemos el refuerzo del sistema, porque podemos implementar todas las mejores prácticas a nivel del DNS. Pero si nuestro sistema, propiamente dicho, no cumple con algunas prácticas básicas de seguridad, podemos hacer cualquier cosa a nivel del DNS, pero el sistema va a seguir siendo débil. Y esa debilidad también puede trasladarse a las operaciones del DNS. Entonces, también tenemos algunas recomendaciones con respecto a cómo reforzar el sistema central.

Si aplican la autoevaluación a sus prácticas de KINDNS dentro de sus operaciones DNS, también deberán autoevaluarse. También deberán evaluar cómo operan ustedes sus propios sistemas. Y tienen que ver si hay algo allí que podría afectar las operaciones del DNS. Entonces, el programa tiene dos aspectos: el primero es el aspecto de autoevaluación. Allí pueden usar la herramienta que nosotros ofrecemos para ver en qué punto están ustedes en cuanto a la seguridad de la operación del DNS. Y luego pueden decidir si quieren unirse al marco de KINDNS. ¿Qué significa eso? Significa que ustedes dicen

públicamente que sí, yo cumplo con estas mejores prácticas, están implementadas en mis operaciones cotidianas y también podemos promover estas prácticas entre mis clientes, entre todos aquellos que utilizan mi sistema.

Y, además, si ustedes quieren capacitación con respecto a esas mejores prácticas, también podremos ayudarlos para darles la información que necesitan para promover esas prácticas. Son simples, ya que el objetivo de KINDNS es hacer algo simple para que los operadores lo puedan implementar. La siguiente, por favor. Entonces, ya mencioné la autoevaluación. Pueden hacer la autoevaluación en línea. Entran al sitio web, eligen la opción de autoevaluación y deben responder una serie de preguntas acerca de cómo operan el DNS. Es un marco voluntario, de modo que ustedes brindan la información real. Si ustedes son honestos, entonces el sistema va a reflejar la realidad y les va a indicar qué deben hacer. Recibirán un informe y la autoevaluación, por supuesto, es anónima. Nosotros no recabamos ninguna información con respecto a quién hace la autoevaluación. Ustedes la hacen. Ustedes brindan la información con respecto a cómo operan sus redes o su operación del DNS. Y, finalmente, se genera un informe.

Lo interesante de ese informe es que no solo les dice cómo están ustedes, en qué punto están ustedes, sino que también les da una guía, una orientación con respecto a cómo mejorar en los puntos en los que no están bien. Quizás hay siete prácticas y hay una que ustedes no están haciendo. El informe generado después de la autoevaluación les va a decir: bueno, acá usted tiene un cero o un diez, un cero de diez porque usted dijo que no está implementado. Esta es la razón por la cual es

importante que usted lo implemente y esta es la forma de hacerlo. Y ustedes, por supuesto, pueden descargar ese informe y usarlo como guía para mejorar su sistema. Y también pueden utilizarlo para convencer a los decisores que tienen que invertir más en las operaciones del DNS para saber exactamente qué tienen que hacer y poder hacer una buena planificación.

La participación en KINDNS es voluntaria. No es algo que la ICANN obligue a hacer a los operadores. Es un marco que está disponible. La información que se ofrece también se ofrece de forma voluntaria. Y tratamos de generar una relación de confianza entre el marco de KINDNS y el operador que lo utiliza. Cuando participan, es decir, cuando se unen a la iniciativa KINDNS, Cuando se convierten en promotores de esas mejores prácticas, esto va a ser de público conocimiento. Entonces tenemos una plataforma de autoevaluación, tenemos el sitio web creado hace aproximadamente un año y medio.

Hay mucho interés en el uso de esta autoevaluación. Hasta ahora hay unas 1500 personas que están utilizando la herramienta de autoevaluación. Y lo que mostramos acá son algunos resultados interesantes que se recaban en forma anónima a través de las respuestas de la autoevaluación, por ejemplo, ¿por qué a la gente le interesa el marco KINDNS? Y no les sorprenderá ver que la mayoría de las personas que hacen la autoevaluación quieren saber en qué punto están en cuanto a esas mejores prácticas. Quieren saber si están implementando las mejores prácticas o no. Un 22% finalmente se unió a la iniciativa KINDNS y eso les ayudó a mejorar el sistema para poder implementar formalmente el programa, porque cuando uno se

incorpora al programa, debe responder algunas preguntas más detalladas.

La autoevaluación es entre ustedes y la herramienta de autoevaluación y el uso del informe de autoevaluación es personal. Nosotros no vemos esa información, pero cuando ustedes deciden incorporarse y ser participantes en el marco KINDNS, entonces deberán responder la misma información, pero con un nivel un poco más detallado. Tienen que explicar cómo están implementando las distintas prácticas específicas y les vamos a hacer preguntas adicionales para que ustedes lo entiendan, porque una vez que ustedes digan yo estoy practicando KINDNS, esto será una afirmación pública y nosotros queremos asegurarnos de que cumplan con todos los requisitos.

Además, también algunos utilizan la autoevaluación para prepararse para cumplir con todas las mejores prácticas. Y hay un interés que también observamos, que el 40% de las personas que hicieron la autoevaluación lo hicieron para convencer a los gerentes de hacer lo correcto. Esto significa que la gente tiene algunas dificultades para obtener más recursos, por ejemplo, para implementar las mejores prácticas. Entonces, completar la autoevaluación los ayuda para mostrar. Estamos observando esto, necesitamos más apoyo. Y este fue un hallazgo interesante para nosotros y para aquellos que hacen la autoevaluación por diferentes razones. Y también obtuvimos información adicional. La mayoría de los que completaron la autoevaluación tienen servidores resolutores autoritativos. Eso pasa en el mundo de los operadores: uno opera el autoritativo para uno mismo,

para su propio nombre de dominio, pero también ofrece resolutores a los clientes.

La mayoría mencionó que opera ambos. El 29% opera solamente servidores autoritativos. Y entre aquellos que operan servidores autoritativos, el 29% opera TLD de los que hicieron la evaluación. El 44 tiene dominio en segundo nivel. Y solo el 27% opera ambos. Entonces, la mayoría, y esto también es un buen reflejo de lo que ocurre, la mayoría de los que utilizan nombres de dominio son operadores de SLD o registratarios que utilizan el dominio para sí mismos. Y eso tiene sentido. Muchos de los que completaron la evaluación son administradores de TLD. Y también nos interesan mucho esos administradores de TLD porque operan en un aspecto muy crítico del sistema de nombres de dominio.

Estas son más estadísticas acerca de las prácticas. Esto es lo que las personas dicen acerca de los operadores, de los resolutores públicos. En el caso de los resolutores públicos, tenemos ocho prácticas para los operadores de estos resolutores. Y la práctica menos implementada es la que tiene que ver con DNS sobre TLS o DNS sobre HTTPS, que implementa encriptado entre el usuario y el operador de resolutores. Solo el 46% de las personas que hicieron la evaluación implementaron esa práctica a pesar de que hay varias personas que ya las implementaron.

En el lado de DNSSEC, en el que hemos estado trabajando durante mucho tiempo, estamos viendo un aumento importante entre los operadores de servidores autoritativos que tienen la validación de

DNSSEC activada. Y aquí la mayoría, el 66%, tienen activada la validación de DNSSEC. Entonces, esto también nos da una idea desde el punto de vista técnico, en el equipo de participación técnica, donde debemos centrar nuestros esfuerzos en cuanto al desarrollo de capacidades, ver dónde están las fortalezas de los operadores y cuál es la información que nos están mandando los operadores. La próxima diapositiva.

Entonces, pueden incorporarse a la lista de distribución de KINDNS, que es donde se debatió el tema de las prácticas, pero la idea es utilizar esa lista de distribución de manera más activa para mantener a la comunidad trabajando y activa con respecto a las mejores prácticas, pero también para debatir la evolución de las prácticas. Ya hemos recibido algunos comentarios adicionales con respecto a las prácticas y estamos integrando estos comentarios al marco para poder llegar a más operadores. La lista de distribución, entonces, es una herramienta importante para lograr nuestro objetivo, porque queremos recibir cada vez más aportes y comentarios de la comunidad. Queremos que la comunidad participe de esto y que esto sea gestionado por la comunidad, liderado por la comunidad.

También tenemos actividades de relacionamiento para promover esto en todas las regiones. El equipo de relacionamiento técnico con el equipo de GSE, Participación Global de Partes Interesadas, organizó algunas reuniones sobre este tema en las diferentes regiones trabajando con los operadores para que conozcan este marco de mejores prácticas y lo puedan implementar. Esta semana vamos a llevar a cabo un programa sobre el KINDNS, una clínica sobre el KINDNS.

Pueden pedir una reunión con la gente del equipo técnico para hablar sobre su caso específico de la operación de DNS. Por lo tanto, tendrían un soporte dedicado, una persona dedicada, que les ayudaría a ver el tema de implementación de KINDNS, cómo hacer la autoevaluación, y después podría ayudarles a llevar a cabo todo lo necesario. Y también esta persona podría seguir en contacto con ustedes después de esta reunión. El programa está evolucionando en cuanto a la parte del backend. La autoevaluación va a ser un poco más técnica en el futuro.

Hay algunos aspectos que irán más allá de responder la pregunta y brindar cierta información. Les vamos a dar a ustedes herramientas para que ustedes puedan evaluar sus operaciones de DNS y les vamos a dar los resultados de esta autoevaluación para que ustedes puedan ver mejor cómo implementar las prácticas. También vamos a tener un zone master. Los operadores de servidores autoritativos trabajan con un zone master para desarrollar una serie de elementos para evaluar lo que están haciendo dentro del marco de KINDNS. Entonces, el resultado del zone master será específico para la operación de cada operador en relación a KINDNS. También empezamos a trabajar de alguna manera con Manners, porque esto es parecido a lo que hacen Manners para el enrutamiento. Vamos a promover esto juntos. Y en la práctica de KINDNS, el centro, hablamos de las prácticas de Manners, porque algunas de las prácticas de Manners sirven para fortalecer el centro, el núcleo.

Ya organizamos algunos talleres con Manners en forma conjunta para promover las mejores prácticas de DNS y las de enrutamiento, porque en algún punto se conectan. Y la idea es asegurarnos de cubrir todo el

ecosistema. También activamente trabajamos con un grupo de investigadores para ver cómo medir la implementación de estas prácticas y ver cómo evolucionan cuando avanzamos con nuestro programa de difusión y relacionamiento. Es entonces un campo muy activo, va evolucionando continuamente y queremos incorporar a más personas, más operadores para mejorar todo esto y también para que más personas lo adopten. Eso ha sido todo lo que yo tenía para compartir para la primera parte de la presentación. La segunda parte de la presentación la va a dar Nicholas, que les va a mostrar el sitio web y la herramienta de autoevaluación. Les va a mostrar cuál es el resultado de esta autoevaluación. Pero antes de llegar a este punto, quiero saber si hay alguna pregunta, si la podemos responder rápidamente. No sé si hay preguntas.

NICOLAS ANTONIELLO: No veo ninguna pregunta ni en la ventana de chat ni en la de preguntas y respuestas. Por favor, diga su nombre.

ABDALMONEM GALILA: Creo que debo leer un poco más sobre KINDNS. Es la primera vez que participo de una sesión como esta. Si tenemos tiempo, ¿podríamos ver cuál es la evaluación para los ccTLD? Estoy un poco confundido. Estoy pensando que KINDNS es un marco para DNS o para los operadores de DNS, que eso puede ser útil para los resolutores o los administradores de DNS para mejorar la seguridad. Sé que tengo que informarme más sobre esto. Igual les pido disculpas.

ADIEL AKPLOGAN: Sí. Puede hacer la autoevaluación que habla más bien de las operaciones. Por ejemplo, todo operador sabe lo que está haciendo en sus operaciones. Entonces es individual. El operador hace su autoevaluación que se aplica a sus operaciones. Pero el marco les da una idea de lo que deberían hacer. Podrían seguir el marco para mejorar sus operaciones. La idea es tener un ecosistema más seguro, más flexible. Entonces, para los operadores de TLD, las mejores prácticas están en DNSSEC. Son prácticas para que la operación sea segura. No es que si tienen DNSSEC ya está totalmente seguro. No, DNSSEC es una de las cosas que pueden hacer para tener una operación segura. Y activar una validación del lado de los resolutores es otro elemento. Y hay más elementos que se pueden agregar.

Lo van a ver ahora en la demostración que hará Nicolás.

NICOLAS ANTONIELLO: Gracias por la pregunta. Sí, vamos a ver algunos de los temas sobre los que usted preguntó. Yo soy gerente de relacionamiento técnico para América Latina y el Caribe. Y, además de eso, soy parte del equipo de participación liderado por Adiel en la estructura de la ICANN. Estamos bajo la oficina del director de tecnología. O sea, formamos parte de la oficina del OCTO en la ICANN. La idea ahora es ver un poco el sitio web. Esto es un poco más técnico, pero voy a tratar de usar un lenguaje que todo el mundo pueda entender, sepan mucho acerca del DNS o nada. Por supuesto, este programa está dirigido a los operadores del DNS. ¿Quién es un operador de DNS? Es alguien que opera un servidor DNS.

Nada más que eso. Uno puede ser un operador si gestiona su propio resolutor. O también en su casa también puede ser un operador si opera un centro de redes en un ISP o en una empresa. Todos los que operan un servidor de DNS podemos operar un resolutor o un servidor autoritativo.

Este programa ha sido diseñado para todos esos operadores. Todo tipo de operadores de servidores de DNS. Ahora voy a resumir algunos de los conceptos que mencionó Adiel. En primer lugar, hablemos un poco de las categorías de operadores. Entonces tenemos lo siguiente. Voy a retroceder. Como dijo Adiel, hemos separado esto en cinco tipos de operaciones. Esos cinco tipos de operaciones caen en dos grupos: el primer grupo… A ver, voy a empezar de esta manera. Voy a empezar con los operadores de servidores recursivos. El primer grupo está integrado por los operadores de servidores recursivos. Y aquí tenemos tres tipos de servidores recursivos. Tenemos los que llamamos resolutores privados. Para el programa un resolutor privado es un servidor recursivo que solo tiene por fin ser utilizado por quien lo opera; por ejemplo, yo tengo una organización, mi organización tiene un equipo de sistemas que administra un resolutor y ese resolutor solo es utilizado por los dispositivos dentro de mi organización y mi empresa. No será un resolutor público, no lo van a utilizar los clientes de la organización, solo lo utilizará la organización y su personal. Los dispositivos de la organización. Eso es un resolutor privado.

Después tenemos un segundo tipo de servidores recursivos que son los resolutores privados compartidos, que son los resolutores para ser utilizados por los clientes de una empresa u organización; por ejemplo,

si ustedes son un ISP, en general, los ISP les brindan a todos sus clientes un resolutor de DNS. Eso sería un resolutor privado compartido.

Es privado porque no puede acceder cualquier integrante de internet; o sea, no es un resolutor público pero será utilizado no solo por la empresa o la organización, sino también por los clientes de la misma. O sea, es un resolutor privado compartido. Después tenemos un tercer tipo de resolutor que llamamos público, que son resolutores manejados por ciertas organizaciones para ser utilizados por cualquier usuario de internet. Todos pueden tener acceso y los pueden utilizar. Como ejemplos tenemos los conocidos que manejan Google. 8.8.8.8., que tiene esa dirección de IPv4, el 1111, el 9999, los de Google, los de otras organizaciones. No hay cientos, pero muchos. Y que cualquier persona que se conecte a internet puede utilizar como resolutor porque son resolutores abiertos.

¿Por qué hacemos esta distinción entre privados, privados compartidos y públicos? Porque las operaciones incluyen algunas mejores prácticas comunes a estos tres tipos de resolutores, pero hay algunas diferencias a nivel operativo. Por ejemplo, si operamos un resolutor público al que cualquiera puede acceder, seguramente deberán revisar las políticas de seguridad, las medidas de seguridad, porque los servidores están expuestos a la totalidad de los usuarios de internet y pueden ser utilizados para fines positivos o negativos y es necesario que se protejan de las actividades maliciosas que podrían utilizar un resolutor de DNS para llevar a cabo un ataque.

No estamos hablando solamente de ataques dirigidos al resolutor en sí mismo, sino también ataques que utilizan el resolutor para atacar a un tercero. Entonces, básicamente, en un lenguaje más común, bueno, hay tipos de ataques de DNS que podrían utilizar estos resolutores abiertos como arma para atacar a un tercero. Así que es necesario protegerse de esto. Si ustedes gestionan un resolutor privado, como suele ser utilizado por dispositivos dentro de la organización, probablemente no tengan ese problema porque ustedes controlan la organización, tienen prácticas de seguridad implementadas. Entonces, si alguien utiliza el DNS para atacar a un tercero o atacar a su servidor DNS, seguramente sea alguien que ya pertenece a la organización, no un tercero externo.

Entonces, sería más fácil de identificar y controlar esto. Entonces, hay diferencias en la operación. Por eso tenemos estas tres categorías de operaciones de servidores recursivos. También tenemos a los operadores de servidores autoritativos. Y aquí tenemos dos subcategorías: una es lo que el programa llama TLD y zonas críticas. Entonces, estos son los operadores de servidores autoritativos a cargo de TLD, dominios de alto nivel, ya sea que estén administrando un TLD o un ccTLD, un dominio de alto nivel con código de país. O, como ya dije antes, un dominio de alto nivel genérico, un servidor autoritativo DNS para estos dominios y zonas críticas. Zonas críticas es un término más amplio.

¿Qué es una zona crítica? Puede ser lo que el operador considere crítico, sea lo que fuere. Por ejemplo, para algunos países a nivel gubernamental, la operación y la continuidad de las operaciones, los servidores autoritativos que brindan el hosting de los dominios de los

servicios gubernamentales son críticos, porque, si dejan de funcionar, la población no va a poder acceder a esos servicios públicos, así que son zonas críticas, estén o no en el nivel superior DNS. Podrían estar en el segundo nivel, pero podrían seguir siendo zonas críticas. Por ejemplo, en otros casos, los dominios del área de educación, aquellos que se asignan a organizaciones educativas, pueden ser zonas críticas, etcétera, etcétera.

También los dominios relacionados con los servicios de salud entran en esta categoría. Los dominios relacionados con servicios financieros aquí se incluyen en la categoría de zona crítica estén en el primero, segundo o tercer nivel y después tenemos todos los demás. Tenemos otros dominios del segundo nivel. Entonces cualquier otro servidor autoritativo entraría en esta categoría de otra otras zonas de SLD.

ADIEL AKPLOGAN: Si tenemos un sitio web y hacen clic en la categoría de operadores, Verán lo que está explicando Nicolás y tendrán una categoría diferente.

NICOLAS ANTONIELLO: Gracias, Adiel. Esta es la clasificación para el programa. Si ustedes van a formar parte de este programa, tendrán que atravesar los pasos adecuados en función de la operación, ya sea operación de servidor recursivo, autoritativo. Y tendrán que seguir estas cinco clasificaciones. Luego tenemos esta sección que se llama Fortalecimiento de la Plataforma. Y esto va más allá de la clasificación de la que hablamos

antes. Se trata de dar pasos adicionales para aumentar la seguridad y la flexibilidad de sus operaciones de DNS. Aquí hay muchas prácticas que conviene implementar si uno quiere reforzar la infraestructura, la plataforma. Y estas prácticas van desde algunas que son recomendables, simples, comunes, hasta algunas que son más avanzadas y que deberían considerar implementarlas cuando están implementando una plataforma.

Verán que en algunos casos dice debe; es decir, aquí se recomienda enfáticamente. Si dice se debe, significa que se recomienda enfáticamente y algunas no se recomiendan tan enfáticamente, pero sí se recomiendan o es algo que ustedes podrían implementar, pero que no deben implementar. Sí, se sugieren. Por supuesto que todo esto es opcional. No es obligatorio implementar nada de lo que hay acá. Solo que son prácticas comunes que se recomiendan y sugieren. Luego tenemos esta sección de herramientas y guías o pautas. Este es uno de los elementos clave del programa. Primero tenemos evaluación y herramientas. Y esta herramienta de auto evaluación es la parte clave del programa, es lo que mencionó antes Adiel. Yo voy a entrar en mayor detalle.

Como dijo Adiel, esta auto evaluación es opcional. Y quienes hacen la auto evaluación pueden ofrecer información en nombre de la empresa, en nombre de la organización que hace la autoevaluación. Y si no quieren brindar esa información, no hay problema. Igual pueden hacer la auto evaluación sin revelar ningún tipo de información acerca de quién está haciendo esa autoevaluación.

La autoevaluación. Vamos a tratar de hacer la auto evaluación. Durante la autoevaluación a ustedes les aparecerán una serie de preguntas. Aquí va el nombre de la organización, es opcional. Yo puedo escribir Nico o puedo dejarlo en blanco. Sería lo mismo. Igual uno puede continuar para completar la autoevaluación. Y después el sistema me pregunta por qué va a hacer usted esta autoevaluación. Tengo que elegir alguna de estas opciones para saber dónde estoy desde el punto de vista de la implementación de las mejores prácticas operativas para el DNS. Y después tengo que elegir qué tipo de operación del DNS tengo yo.

Si tengo un servidor autoritativo, un servidor recursivo o ambos. Si mi infraestructura de DNS es administrada por un tercero o si yo administro mi propia práctica. Digamos que soy un ISP y yo tengo un servidor recursivo que opero para ofrecerle esta opción a mis clientes. Entonces sería operación de un servidor recursivo. Y luego el tipo de operación. Como dije en este ejemplo, yo soy un ISP. Entonces tengo un resolutor recursivo privado compartido. Y luego acá está la evaluación. Acá están todas las preguntas que ustedes deberán responder para completar esta autoevaluación. Son una serie de prácticas. Se les ofrecen seis prácticas posibles y ustedes tienen que decir cuáles son las que están implementando actualmente. Por ejemplo, la práctica número uno dice: yo tengo activada la validación de DNSSEC para mis resolutores; es decir, mis resolutores tienen la capacidad para validar la información de DNSSEC que viene de los servidores autoritativos. Yo tengo DNSSEC, entonces tildo esta opción.

La práctica número dos dice: yo utilizo las listas de acceso para limitar o restringir quién puede utilizar mi resolutor recursivo. Este es un

resolutor privado compartido y yo quiero que solo mis clientes lo puedan utilizar. Entonces debería tener un sistema de seguridad o un método de seguridad que en general se llama lista de acceso que le impide a cualquiera que no es cliente mío acceder a este servidor. Entonces yo digo sí, yo tengo esto. Es una práctica común. Si quiero que mi servidor no sea público. Si no tenemos un resolutor que sea público, entonces tenemos que tildar la opción número tres. Yo tengo minimización de QNAME y resulta que ni sé lo que es QNAME, entonces lo dejo en blanco. Práctica cuatro: mis resolutores no se ejecutan en el mismo servidor. No, mi resolutor se ejecuta en el mismo servidor que uso para mis servicios autoritativos porque no tengo mucho dinero, porque no tengo otro servidor, tengo un servidor físico. Pongo ahí una máquina virtual, creo dos servidores virtuales. Y en uno de esos servidores virtuales yo tengo el servidor autoritativo y en el otro tengo recursivo. O aún peor, tengo una máquina, un sistema operativo y tengo los dos servidores ahí: el autoritativo y el recursivo en la misma máquina. En ese caso, si fuera así, no estaría cumpliendo con esta práctica, entonces no la tildo.

Práctica número cinco: mis servicios de recursión son flexibles. Utilizan al menos dos servidores diferentes que toman en cuenta la diversidad. No, yo no uso esto. Y la práctica número seis es, ¿la infraestructura que utilizo con mis servicios de DNS está siendo monitoreada? Sí. ¿Cumplo con este requisito? Entonces lo marco como cumplido. Hago clic en siguiente o next. ¿Usted tiene un portal interno o un portal para el público para que los clientes que acceden y administren sus servicios de

DNS? No, porque no lo necesito en mi caso con un servidor recursivo. Y eso es todo. Ya terminé con la autoevaluación.

Podría continuar y hacer una segunda una segunda evaluación que va a entrar en mayor detalle acerca de las prácticas de seguridad. Estas prácticas de seguridad no son solamente para los servidores DNS, son prácticas de seguridad que se usan para muchos otros servidores, incluidas las operaciones de los servidores del DNS. Por ejemplo, Adiel mencionó un programa de mejores prácticas no para DNS, sino para enrutamiento. Como dijo Adiel, este programa KINDNS es como una especie de hijo de Manners. Tomamos la misma idea de ese programa desarrollado originariamente por la ISOC para las mejores prácticas de enrutamiento, y a partir de ese programa nosotros creamos el programa KINDNS. Entonces tiene muchos otros indicadores o medidas de seguridad que deberían implementar, algunas cosas tienen que ver con el enrutamiento, otras tienen que ver con mejorar la seguridad de la infraestructura del DNS en particular, pero no vamos a hacer esta evaluación ahora.

ADIEL AKPLOGAN: La conexión con Manners es clave porque todos los servidores tienen una dirección IP. Entonces, en general buscamos la operación del DNS, pero tenemos que mejorar la seguridad del DNS y de la dirección IP. Esto también es crítico. Entonces ahí vemos que hay un vínculo directo con Manners.

NICOLAS ANTONIELLO: Para agregar a lo que dijo Adiel, a veces, con más frecuencia de lo que nos gustaría, hay capacitaciones sobre cosas que tienen que ver con las redes, con Internet, etc. Y nos centramos en un tema específico como ahora nos centramos en el DNS y corremos el riesgo de perder de vista la totalidad de la situación. Como dijo Adiel, el DNS no es algo aislado; necesita direcciones de IP, necesita toda una red, necesita enrutadores, que es el equipo que se utiliza para llevar la información de un lugar a otro. Necesitamos protocolos de enrutamiento, necesitamos muchas cosas: equipo de seguridad, medidas de seguridad, etcétera. Esa es la idea de esta parte del programa, conectar las operaciones del DNS con el resto de las operaciones de la red, como parte de todo un ecosistema. Una vez más, no vamos a hacer esto ahora porque nos llevaría demasiado tiempo, pero ustedes pueden hacerlo también. Y acá el sistema me va a dar una especie de puntaje. Dice: su puntaje total para esta evaluación es 50%, es decir, ¿usted está implementando el 50% de qué? El 50% de lo que este programa considera que son las mejores prácticas operativas acordadas para el tipo de operación del DNS que usted seleccionó.

Recuerden que yo elegí solamente operación de resolutores y dentro de resolutores operaciones de resolutores privado compartido. De las seis prácticas que había, mi puntaje es el 50%. Y luego tengo estas dos opciones: una es descargar el informe. Hago clic acá y el sistema me va a generar un PDF con toda la información. Con más información de lo que yo les mostré me va a dar una clara idea de dónde estoy en términos de la operación del DNS. Me va a decir, bueno, usted debería implementar esto, esto y lo otro que usted todavía no implementó. Y

dentro del programa también hay recursos que yo puedo usar para ir e implementar esas mejores prácticas que todavía no estoy implementando.

Si no descargo el informe y cierro la página, y posteriormente quiero descargar el informe, voy a tener que otra vez completar toda la evaluación porque esta página web no conserva ninguna información acerca de la autoevaluación después de este punto. Entonces, yo debería descargar el informe. No lo voy a hacer ahora, pero debería descargar el informe. Y luego puedo, por supuesto, volver a hacer la autoevaluación. Si recordé lo que era la minimización, entonces voy, lo hago nuevamente y luego puedo descargar el informe. Esto es solo para ustedes. Nadie más va a ver esto si ustedes no quieren. De forma tal que no tiene ningún sentido mentir en esta evaluación, porque lo que les va a decir es dónde están ustedes parados en términos de las mejores prácticas. De lo contrario, será como si no hicieran nada, a menos que, por supuesto, estén cumpliendo con todas las mejores prácticas. Bueno, este es el fin de la parte de autoevaluación. Y recuerden que hay una autoevaluación para las distintas operaciones.

Vamos a descargarlo para ver el informe, generamos un archivo. Voy a compartir el PDF generado. Este es el informe que yo acabo de descargar. Como pueden ver acá, me dice qué clase de autoevaluación hice, cuáles son las principales prácticas operativas. Me dice que opero un resolutor privado compartido solamente. Estas son las prácticas de seguridad relacionadas con la seguridad del DNS. 1, 2 y 3. Yo la 1 y la 2 las tengo implementadas y la 3 no porque no sé lo que es la minimización de QNAME. Bueno, sé lo que es, pero hacemos de cuenta

que no lo sé. Seguramente muchos de ustedes ya saben qué es, pero esto es solo un ejemplo. Pero puede ocurrir que alguien que opera un servidor del DNS no sepa qué es y está bien, no hay ningún problema con eso.

Y luego tenemos las prácticas operativas relacionadas con la disponibilidad y flexibilidad de los servidores del DNS, que son las prácticas 4, 5 y 6. Yo solo implementé la práctica 6, entonces en el caso de las otras dos prácticas tengo un valor de cero. Ese es el puntaje del 50%. Y después me dice, en el caso de la práctica 3, que es aquella que yo no tildé porque no la tengo implementada, me explica qué es y me da un vínculo con una serie de pautas que me explican cómo podría implementarlo.

El programa también tiene ejemplos de configuraciones básicas, o algunos de los servidores más comunes. Por ejemplo, si uno opera un resolutor, podría estar utilizando el software de Bind o el Outbound, que son los dos principales, que más se usan en todo el mundo. Y les va a mostrar ejemplos de cómo configurar la minimización de QNAME en ambos tipos de software. Entonces explica qué es, de qué se trata esa práctica que uno no implementó y nos da enlaces a fuentes de información que explican cómo implementarlo. Lo mismo con respecto a las prácticas 4 y la práctica 5, en donde mi puntaje fue cero.

Si yo leo todo esto y veo que podría implementarlo, voy, lo implemento, vuelvo a hacer la autoevaluación y ahí mi puntaje va a ser el 100% si implemento todo. Esta es la idea general del programa: crear algo útil, un único lugar que agrupa toda la información y que ofrece enlaces a

información. El programa no produce estándares, no generamos estándares, no generamos mejores prácticas, simplemente las recopilamos en un único lugar. ¿Por qué? Porque tal como dijo Adiel, si ustedes son un experto técnico nuevo, por ejemplo, y quieren implementar un servidor del DNS, ya sea autoritativo o recursivo, van a tener que leer más de 150 estándares y mejores prácticas. Si uno leyó al menos uno de esos estándares o mejores prácticas, sabrá que cada uno implica 100 o 150 páginas que hay que leer. Y es mucha información. Entonces, si hablamos de estándares para algo en particular, uno puede ir al grupo del IETF. Ahora, si hablamos de mejores prácticas, en general, no están en un único lugar. Están dispersas por todas partes. Entonces, hay que recurrir a la fuente más confiable de mejores prácticas, etc.

Lo que tratamos de hacer acá es, de nuevo, lo mismo. Recopilamos todas las mejores prácticas y las ponemos en el lugar que es más fácil leer, pero para las operaciones y actividades del DNS. Voy a dejar de compartir. Creo que cerré el navegador. Ya lo encontré. Lo voy a compartir de nuevo con ustedes. Bueno, esto está en el sitio web de KINDNS. Este es el informe que ustedes pueden descargar acá. Y después tenemos… Vamos a ir a la home page. Después tenemos estas herramientas y pautas. Ya vimos la evaluación y herramientas. Tenemos un tablero de control con algunos datos estadísticos que ya les mostró Adiel y después tenemos aquí pautas o guías. Este es un buen recurso, una buena fuente de información para aquellos que quieren obtener más información sobre las prácticas que no implementaron o las prácticas que sí implementaron, pero quieren saber más o actualizar información con respecto a qué son, de qué se tratan. Así que acá hay

mucha más información según el tipo de operación que ustedes lleven a cabo.

Y luego tenemos aquí estos recursos de seguridad que una vez más les da una fuente de datos estadísticos, mejores prácticas, estándares. En este caso, algunos están clasificados según la organización que generó esa recomendación o ese documento. Y tenemos una serie de documentos, en este caso generados por la ICANN, una serie de estándares generados por el IETF, recursos con información producidos por distintas organizaciones como DNS-OARC, RIPE, APNIC, NANOC, grupos de operadores de redes de diferentes partes del mundo. NANO es el grupo de operadores de red para América del Norte, pero cada región tiene un grupo de operaciones de red y hay subregiones como el Caribe que tiene su propio grupo de operadores de red, como CaribNOG, que también tiene muchas fuentes de información.

Y algunas empresas privadas como Google, ISC u otras empresas que generan información, documentación y recomendaciones acerca de cómo configurar su servicio. Bueno, ya llegamos al final de nuestra hora. Vamos a tener una pausa de 15 minutos y luego usaremos algunos minutos de la próxima sesión. Hacemos un receso ahora. Podemos pausar la grabación y volvemos en 15 minutos.

[FIN DE LA TRANSCRIPCIÓN]