ICANN73 | Semana de preparación – Actualización sobre las normas de ejemplificación e intercambio de conocimiento para la seguridad del DNS y los sistemas de nombres (KINDNS)
Miércoles, 23 de febrero de 2022 – 11:00 a 12:00 AST

ADIEL AKPLOGAN: Bienvenidos todos a esta sesión sobre la iniciativa de KINDNS. Vamos a presentarles las novedades sobre esta iniciativa KINDNS, que es una iniciativa para promover las buenas prácticas en DNS en general. Tenemos interpretación disponible en el día de hoy. Vamos a solicitarles que quienes lo necesiten utilicen la interpretación. Nuestro orador va a tratar de hablar lo más lento posible para que los intérpretes puedan cumplir con su función.

Si quieren hacer una pregunta, pueden hacerlo en el espacio de preguntas y respuestas para que nosotros la podamos tomar. Si desean hacer uso de la palabra, también pueden levantar la mano. Esto les va a permitir hacer uso de la palabra. Pasemos a la siguiente diapositiva, por favor, Steven.

Vamos a tener una presentación dividida en dos partes. Yo les voy a mostrar la introducción y les voy a presentar a Philip Regnauld, quien es el experto de este proyecto y les va a comentar en qué situación nos encontramos. Va a profundizar más en este proyecto. Tuvimos una sesión durante la reunión ICANN72 donde hicimos una introducción de la iniciativa KINDNS y les explicamos un poquito cuál era su objetivo.

Voy a comenzar directamente hablando de esta iniciativa, que es una iniciativa de intercambio de conocimiento e instauración de normas para la seguridad del DNS y la asignación de nombres. Para abreviar el nombre usamos esta sigla y hablamos de usar las mejores prácticas en la comunidad de operadores del DNS en general para que en forma voluntaria ellos se adhieran a estas buenas prácticas y también para que nosotros dentro de la ICANN promovamos las buenas prácticas en todo el mundo y nos aseguremos de trabajar juntos para que el DNS sea un espacio lo más seguro posible. Siguiente diapositiva, por favor.

Algunos de ustedes ya están familiarizados con MANRS, que es una iniciativa que tiene que ver con la seguridad del enrutamiento en línea. KINDNS también tiene que ver con eso en cierta forma. Podemos decir que podemos tener KINDNS y MANRS, que en español se traduciría como amabilidad y modales, y todo esto contribuiría a una mayor seguridad del sistema de nombres de dominio.

Aquí queremos tener buenas prácticas sencillas que los operadores puedan seguir con facilidad para asegurarnos de que la operación en el DNS sea segura. Aquí hablamos de la operación del DNS porque aquí hablamos de buenas prácticas puramente técnicas con respecto a la operación del DNS en sí mismo. Muchas veces en torno al DNS hay otros servicios y otras aplicaciones en funcionamiento pero esta iniciativa trata de hacer foco más específicamente en el aspecto técnico de la operación del DNS.

Si están familiarizados con el DNS, seguramente habrán escuchado decir que hay buenas prácticas relacionadas con DNS. Hay un documento de 2.000 páginas que habla del DNS pero aquí estamos

tratando de sacar de todo ese documento lo más importante para que todos los operadores que ejecuten cualquier componente del DNS puedan operar el DNS con seguridad. Siguiente diapositiva, por favor.

Esta iniciativa se compone de distintas partes. Tiene algunos componentes centrales, más que nada la operación del DNS a través de la identificación y la documentación de las normas de seguridad más críticas para el DNS. Básicamente nosotros compartimos en forma periódica lo que surge del trabajo de notificar las normas y obtener una devolución de parte de la comunidad.

Nos concentramos en las buenas prácticas para lanzar algo más específico sobre buenas prácticas, tener un portal dedicado de información con estas buenas prácticas y las guías de implementación. Allí podríamos tener información útil que los operadores pueden evaluar. Aquellos operadores que están comprometidos con la implementación de las buenas prácticas a través de esta iniciativa. Esto nos puede ayudar a promover la noción de las buenas prácticas. Todo lo que se publique se publicará en este portal, en este sitio web dedicado: kindns.org.

Luego vamos a trabajar para identificar algunos indicadores que nos puedan ayudar a visualizar el impacto que tiene esta iniciativa en términos de la seguridad del DNS. Queremos encontrar algunos indicadores que sean medibles a lo largo del tiempo para ver si estamos yendo en la dirección correcta o incorrecta, y hacer los ajustes que requiera el caso. En la próxima fase tendremos esta actividad.

Normalmente, cuando presentamos en el contexto de la ICANN la iniciativa, normalmente nos preguntan si esto también va a referirse a la funciones de aprovisionamiento del DNS. Es decir, los registros, los registradores, los registratarios, si habrá buenas prácticas en ese sentido también. La respuesta es no al comienzo porque aquí nos concentramos en la función central del DNS pero tal vez en una etapa posterior podemos ver cómo se puede mapear algunas de estas buenas prácticas y extenderlas al sistema de aprovisionamiento. Es decir, a los registros, los registradores, con sus buenas prácticas y sumar esto a la iniciativa. Lo hemos considerado pero en la primera fase principalmente nos vamos a centrar en la operación del DNS. Siguiente, por favor.

Tenemos la atención centrada en varias categorías. Si están operando el DNS, lo hacen en un ámbito donde hay otros componentes que contribuyen a la robustez y la operación segura del DNS en general. Como dije, inicialmente no vamos a cubrir todos los aspectos pero sí nos vamos a concentrar en particular en aquellos componentes del DNS que son los servidores autoritativos que funcionan en distintos entornos, en los TLD o en aquellos operadores que se ocupan de zonas críticas y también en la gestión de los dominios de segundo nivel en general. Tenemos TLD y zonas críticas como cualquier TLD nic.tld o .UK. Esa será la primera categoría.

Luego tendremos una segunda categoría donde nos ocuparemos de los dominios de segundo nivel y quienes los registren o los administren. Luego tendremos los operadores de resolutores recursivos en general y en esta categoría también tenemos tres

subcategorías que vamos a atender: resolutores privados y cerrados, los privados compartidos y los públicos. Vamos a promover toda esta iniciativa en torno a estas categorías.

También vamos a dar cierta orientación respecto de los sistemas de servidores y la red en general con consideraciones desde el punto de vista de la privacidad, que pueden tener un impacto en algunos aspectos de la seguridad en términos generales. Si en esta instancia algún operador quiere sumarse a KINDNS y trabajar con esta iniciativa, se va a hacer una autoevaluación de ese operador en contraposición con estas dos categorías principales que mencioné. Es decir, los servidores autoritativos y la operación de los resolutores recursivos en general. Vamos a publicar, por supuesto, guías de implementación, cómo llevar adelante determinadas tareas, listas de verificación, procesos de configuración entre otros.

Surge la pregunta con respecto a qué software vamos a tener para dar orientación. Vamos a usar el más popular, por supuesto, pero queremos considerar que se puede aplicar estos conceptos a cualquier software si se puede presentar de una manera que sea comprensible. Siguiente diapositiva, por favor. A partir de aquí le voy a dar la palabra a Philip para que nos presente los distintos elementos que tenemos en cada una de estas categorías mencionadas. Philip.

PHILIP REGNAULD: Muchísimas gracias, Adiel, por la presentación y por esta introducción. Espero que tengamos alguna devolución de parte de la comunidad con respecto a las buenas prácticas que se están presentando, cómo se

van identificando. ¿Cómo hemos dividido esto? ¿Cómo hemos categorizado a los operadores de DNS? Pensamos inicialmente en tener los dominios de primer nivel y de segundo nivel al principio pero pensamos que tal vez era un abordaje no sé si llamarlo simplista pero un poco complicado. Queríamos ver si podíamos tener operadores de nombres de dominio autoritativos u operadores de servidores de DNS que ofrecen servicios de resolutores recursivos. Para comenzar con los servidores autoritativos, lo que hicimos fue ver el tipo de zonas que existen en Internet por naturaleza jerárquica. El DNS es más crítico a medida que subimos más en la escala y llegamos a la raíz que es el nivel más crítico, la zona más crítica. No más vulnerable pero sí es el blanco más buscado si alguien quiere comprometer la seguridad del DNS. En general apuntan a ese nivel.

Los TLD tienen un papel importante pero también hemos visto otros dominios que podrían tener una operación importante. Si vemos los servidores de nombres para muchos países no es infrecuente ver en Dinamarca con DK que los nombres también se ubican en un subdominio como nic.dk. Probablemente estos niveles sean tan importantes como los de TLD.

Por eso decidimos dividir esta categoría en zonas críticas. Así las llamamos. Con los nombres de dominio de primer nivel pero también las zonas auxiliares o de soporte que ofrecen algún tipo de servicio, ya sea alojando servidores de nombres o creando determinadas dependencias. Otro que decidimos incluir en las zonas críticas no está necesariamente vinculado con la operación del DNS en sí mismo pero si lo vemos desde la perspectiva de los ccTLD, ¿cómo lo llamaríamos?

Algunos archivos de zona de los dominios de nombres podrían ser muy críticos en cuanto a sistemas de identificación de gobernanza electrónica, de ciudadanos. Hay algunos que son más importantes que otros pero aquí en Dinamarca tenemos un sistema de identidad nacional que hemos identificado como servicio crítico. Si myid.dk está caído, muchas personas no se van a poder conectar. ¿Esto puede tener un efecto sobre todo el DNS? Esto va a depender de un modelo de autoevaluación. Aquí lo que queremos hacer no es necesariamente dictaminar qué zonas son críticas o no sino más que nada estamos planteando un marco para que se pueda identificar cuáles son las zonas críticas o que una organización pueda identificar que brinda servicios críticos y establecer cuáles serían las buenas prácticas que deberían ponerse allí en juego para mantener la seguridad. También incluimos sitios de banca y de finanzas que son considerados críticos para el funcionamiento apropiado de la economía de un país. En cierta forma no diría que esto es algo arbitrario pero sí fue la manera en que decidimos estructurar nuestro trabajo. En cuanto a la vulnerabilidad y al impacto para una unidad constitutiva o para los electores o para una economía, obviamente tenemos que pensar aquí también que los ccTLD son críticos. Siguiente diapositiva, por favor.

Luego tenemos otros nombres de dominio. Todos aquellos que están por debajo del nivel superior, que también son críticos, que brindan los servicios en los sitios web, en gobierno electrónico, comercio electrónico. Todas estas cosas tienen que ser manejadas responsablemente también. Aquí, no obstante, hay menos restricciones en términos de las mejores prácticas que deseamos observar. ¿Por qué queremos tener esta operación? Para que la gente

comience con KINDNS, comience a implementar las mejores prácticas y no se sienta desalentada por la complejidad.

Quedamos en el dominio de segundo nivel y si algo anda mal no va a impactar tanto. Se puede seguir con la delegación y puede seguir sujeto a ciberataques. Se está verificando si se está haciendo la diligencia debida o implementando las mejores prácticas que permiten al menos mitigar estos incidentes. Realmente no importa cuán importante es el dominio. En este sentido todos deben hacerlo porque si el nombre ha sido secuestrado, va a generar algún tipo de perturbación. Siguiente diapositiva.

Los operadores del DNS recursivos. Esta es la otra mitad del ecosistema. Tenemos los operadores autoritativos y luego los operadores del DNS recursivos. Aquí tenemos que considerar qué clase de resolutor recursivo tenemos. En esencia, si es público o si es privado. Mirando en más detalle, habrá resolutores privados que serán los corporativos, las redes totalmente cerradas que no son accesibles desde el exterior, el acceso del tipo VPN y, por lo general, con base de direcciones privadas, que son organizaciones como compañías, seguros, bancos. La mayoría de las empresas estarán estructuradas así pero hasta cierto punto las redes hogareñas y residenciales también.

Luego un poquito más abiertos tenemos los resolutores privados compartidos. Aquí no quiero especificar necesariamente que sean los ISP o proveedores de alojamiento pero son aquellos clientes o instituciones, podemos imaginar una red universitaria, que no son accesibles desde el exterior pero que pueden ser compartidos por entidades jurídicas claramente distinguibles. Por ejemplo, múltiples

clientes que comparten un resolutor de una ISP o en el contexto de un conjunto de organizaciones federadas, con una administración técnica en común. Esta sería entonces una categoría más.

Después tenemos los resolutores públicos. Cuando pensamos en estos resolutores públicos pensamos en AAA, en Google, este tipo de servicios. En el medio tenemos los servicios de DNS cerrados con el filtrado comercial de DNS que pueden tener distintas formas. Disculpas. Voy a tratar de hablar más despacio.

Con los resolutores públicos entonces, como decía, tenemos Google y los similares. Luego tenemos los semiabiertos o los que se llaman resolutores abiertos con componentes comerciales. A través de un acuerdo de derechos o un contrato se reciben servicios adicionales de estos operadores como puede ser depuración o servicios de DNS pasivo donde el tráfico es analizado para ver si hay algún host comprometido o malware. En este caso los operadores son públicos por lo general pero tienen algún tipo de mecanismo de control de acceso. Quizá alguna tarifa que hay que pagar o un contrato para poder ingresar y usar este servicio y aprovechar, beneficiarse de estos servicios de valor agregado que van a proveer. Esas son las distintas categorías entonces.

En la sección arriba, lo que hacemos es identificar de qué manera estos resolutores… ¿Cómo hice la restricción del acceso a estos resolutores? Pueden ser certificados, pueden ser direcciones IP. Esto en realidad no importa. Lo que importa es que cada uno de estos operadores lo que tratamos de hacer es ponerlos en una categoría y luego, desde KINDNS, ver cuál es el lugar para nosotros, cuáles son las

mejores prácticas y, hasta cierto punto, que los usuarios finales y las organizaciones, por ejemplo una empresa que desea hacer una búsqueda… Estoy conectado a mi ISP y estoy utilizando su resolutor para hacer las consultas de DNS a la Internet. ¿Por qué hay que observar estas prácticas? ¿Realmente se están cumpliendo, se está siguiendo el programa? Luego, referirse al proveedor o al ISP o al departamento de TI y chequear que se estén siguiendo estas mejores prácticas para proteger la privacidad de la manera en que aquí se está describiendo. Siguiente, por favor.

Bien. Las recomendaciones para los resolutores privados. De hecho, no hemos cubierto la totalidad de las recomendaciones para los resolutores autoritativos pero no es nuestro foco. Nuestro foco son los privados. Los resolutores privados, como decía, son las redes privadas que a veces son partes de dominios de redes como active directory. Lo que hicimos fue centrarnos primordialmente en la seguridad de esas redes e identificamos una necesidad de más transparencia. Esto significa que algunas recomendaciones que pueden aplicarse a otros espacios como DoH o DoT siguen beneficiando estos servicios y aprovechando DoH o DoT, por ejemplo, para reenviar las consultas a un resolutor arriba que tiene habilitada la encriptación para por lo menos garantizar que se pueda salir en caso de que haya interferencia. Eso es lo que ocurre.

Luego la disponibilidad y la flexibilidad de los servicios. Como mencionaba, algunas de estas mejores prácticas incorporan las antiguas mejores prácticas administrativas pero en el sitio web habrá más detalles del programa que quizá deseen consultar para fortalecer

el sistema y hacer una mejor administración del sistema. Aquí algo muy importante que tenemos es la validación con DNSSEC. Olvidé mencionar que, para los autoritativos, lo que se espera, una de las principales mejores prácticas que estamos promoviendo para los operadores de zonas autoritativas es la firma con DNSSEC. Aquí, en el lado de los resolutores, vamos a alentar, de hecho, que sea un requisito para los resolutores, hacer validación con DNSSEC. Esto lamentablemente no es el caso con gran parte del software que existe pero subrayamos esta necesidad de hacer validación con DNSSEC en este momento. Creo que esto se aplica a la mayor parte del software. Siguiente diapositiva.

Los resolutores privados compartidos. Nosotros hablamos de que comprende los tipos de ISP o proveedores de servicios similares. Tienen requisitos similares pero con clientes diferentes. Tratan con un mix de usuarios de cable, residenciales, móviles, con cierto control de acceso y como estos resolutores son compartidos por distintos clientes hay cuestiones de privacidad también. Hay distintas cosas de las cuales no vamos a hablar ahora pero la idea es comprobar o asegurarse de que cuando se ofrece un servicio de DNS se haga de manera amigable para la privacidad. Lo que recomendamos aquí es habilitar DoH, DoT o ambos en el servicio del resolutor para que estos clientes se sientan más cómodos enviándoles a ustedes las consultas y no tener que ir a buscar la resolución a otra parte por una cuestión de latencia, que pueden usar las redes de ustedes con DoH o DoT, que pueden usar sus sistemas sabiendo que hay una relación de negocios con ustedes como ISP y ustedes así ofrecer DoH y DoT. Esto tiene sentido en términos de privacidad. Por supuesto, esto va en paralelo

con la tradición existente de DNS encriptado que va a existir durante un tiempo.

Disponibilidad y resiliencia del servicio del DNS. Es una de las recomendaciones que aquí también formulamos. Esto está en el sitio web y en la wiki. Hay distintas mejores prácticas de higiene y fortalecimiento y también nuevamente validación del DNSSEC. Cualquiera que tenga resolutor privado debería firmar con DNSSEC. Siguiente diapositiva, por favor.

Para los operadores de resolutores públicos, estamos hablando aquí de los más grandes como Google y otros. Por supuesto, ellos ya tienen su propia manera de hacer las cosas y muchos de ellos estoy seguro de que ya están implementando estas mejores prácticas pero nos esforzamos en considerar la incorporación de validación por DNSSEC también.

Luego la consideración de privacidad, DoH, DoT. Los grandes nombres ofrecen o DoH o DoT o ambos. Ahí se pueden enviar las consultas seguramente. Por ejemplo, Quad9 utiliza al igual que Cloudflare este servicio. También minimización de Qname. Esta minimización de Qname es para evitar la fuga de nombres de dominio totalmente calificados, no necesariamente a la raíz. Activando esta función solo se revela parte del nombre de dominio porque se quiera o no, los nombres de dominio son reveladores. Divulgan información sobre los usuarios, sus hábitos y lo que están haciendo. Eso no corresponde para el consumo público.

Lo mismo para los resolutores cerrados con DNS con filtros a través de algún tipo de control de acceso o con pago podrán también ofrecer DoH o DoT, que probablemente sea el caso en la mayoría, y minimización de Qname siempre habilitada. Es una práctica en la mayoría pero ahora lo estamos convirtiendo, por así decirlo, en un requisito. También por supuesto validación por DNSSEC. Siguiente, por favor. No sé si esto era todo lo que yo tenía que cubrir.

ADIEL AKPLOGAN: Gracias, Phil. Yo continuaré. Lo que Phil nos contó ha sido una reseña de cómo se van a estructurar las distintas mejores prácticas y tengan en cuenta que aquí el objetivo es uniformizar todo esto y centrarnos en las más importantes. Tener un número determinado de mejores prácticas a implementar. Nuestra meta es de 7 a 10 mejores prácticas en total para no generar más confusión en la gente. Ahora les voy a contar cómo se va a presentar esto, cómo se va a estructurar cuando se lance.

Como decía, estará alojado bajo kindns.org, que es un sitio web dedicado, soportado y patrocinado principalmente por la ICANN. A quienes les interese incorporarse a la iniciativa, hay distintas formas. Ahí encontrarán toda la información que necesitan. Habrá una sesión sobre las distintas categorías. Como decía Phil, el área de soporte y participación es para los operadores que quieran incorporarse a la iniciativa. Aquí se pueden registrar, ya sea como patrocinadores, como miembros, los operadores, o como embajadores de la iniciativa.

Luego tenemos una sesión de herramientas donde los operadores pueden hacer la autoevaluación a través de discusiones para ver cómo estas herramientas se van a desarrollar. Son muy sencillas y directas porque nosotros esto no lo hacemos obligatorio. Es una participación voluntaria. La mayoría de las personas se van a comprometer a implementar estas mejores prácticas en general. La herramienta de autoevaluación se va a basar sobre todo en el compromiso propio de cada uno a la hora de implementar las distintas prácticas y responder las preguntas.

Luego se desarrollará un tablero con información, como nos contaba Phil, como les conté, para poder rastrear las distintas herramientas y el impacto que tienen sobre el contexto. También las guías acerca de cómo implementar las mejores prácticas o con más informaciones sobre cada una de las mejores prácticas y sus consideraciones. Por ejemplo, en la diapositiva que mencionaba Phil, todo lo que está relacionado con el núcleo, la seguridad del sistema central, habrá cuatro mejores prácticas detalladas en las guías donde la gente puede consultarlas pero no son parte del núcleo del programa. Habrá un blog con eventos también.

A medida que vamos trabajando hacia este objetivo en el resumen y la identificación de las mejores prácticas, hemos comenzado ya a desarrollar algunas de las guías. Hemos dado a conocer recientemente un libro guía para la firma con DNSSEC en uno de nuestros documentos de la OCTO. Estos documentos serán referidos varias veces en KINDNS y pronto se darán a conocer varias otras guías. Siguiente diapositiva, por favor.

Muy bien. Tenemos aquí un contrato para que alguien nos ayude con el diseño de este sitio web. Probablemente tenga este aspecto. Todavía está en una etapa muy incipiente. Cuando tengamos la diagramación y el diseño finales, ustedes podrán verlo. Este será el próximo resultado que tendremos en este proyecto en términos generales. Siguiente, por favor.

Hemos tenido que adaptar nuestros plazos un poquito desde la última vez que hicimos la presentación por distintos motivos pero nuestro objetivo en este momento es hacer el lanzamiento para fines del primer trimestre del 2022. Es decir, fines de marzo aproximadamente. Es posible que no tengamos todas las funciones del sitio web disponibles. Vamos a hacer el lanzamiento con las más críticas para poder comenzar con esta iniciativa incorporando operadores y trabajando con ellos ya. Obviamente vamos a ir dando información actualizada a la comunidad y a través de la lista de distribución. Les recomendamos que se sumen a la lista de distribución de correo electrónico que es abierta, que nos den sus comentarios, que nos hagan sus aportes y mientras tanto hemos establecido una página wiki donde estamos publicando la mayor parte de la información con respecto a lo que estamos haciendo en este momento. Este será un repositorio temporario. Luego nos trasladaremos al sitio web formal cuando ya lo tengamos listo.

Creo que con esto llego a la última diapositiva. Les quiero agradecer a todos por su atención. Ahora quisiera saber si hay alguna pregunta, comentario o sugerencia. Para eso hicimos esta sesión. Gracias.

KINGA KOWALCZYK: Tenemos una pregunta. Adiel, ¿quiere que la lea en voz alta?

ADIEL AKPLOGAN: Sí.

KINGA KOWALCZYK: Tenemos una pregunta de Sivasubramanian: "¿KINDNS también desarrollará un compromiso común compartido no para vincular a los usuarios con un único resolutor sino con múltiples resolutores redundantes que cualquiera pueda usar? Puede haber una situación tal vez un poco lejana, no tan precisa, que una universidad bloquee a sus alumnos de utilizar resolutores externos o que el alcalde de una ciudad insista en que nadie en la ciudad utilice otro resolutor que no sea el de la ciudad. Tal vez estos compromisos compartidos pertinentes y otros se separarían de estas prácticas compartidas".

ADIEL AKPLOGAN: Creo que es un comentario muy pertinente y creo que tiene que ver con la parte de los usuarios, de los registratarios. Más que nada me parece que está relacionado con la parte de política porque hay una decisión de política en juego aquí. Cuando alguien les pide a sus clientes o a sus usuarios o a su comunidad que tienen que utilizar un determinado servicio, ese aspecto de política en realidad no está cubierto aquí porque tenemos muy poco control sobre ese tipo de cuestiones. Desde la perspectiva del registratario, por supuesto si uno se ocupa de la operación puede configurar determinados resolutores y esa es una buena práctica general para la gestión general, para la

prestación de servicios, para la resiliencia, la redundancia, los servicios del DNS pero no hemos hecho hincapié en este aspecto en particular porque tiene más que ver con los registratarios y las prácticas de los ISP que no conforman el núcleo, la parte central de esta iniciativa.

KINGA KOWALCZYK: No sé si tenemos alguna consulta más. Pueden levantar la mano. Por el momento aquí no hemos recibido más preguntas. También pueden ingresar su pregunta en el espacio de preguntas y respuestas, y yo voy a leerla en voz alta.

ADIEL AKPLOGAN: Quisiera escuchar a los participantes, su opinión con respecto a un aspecto que mencionó Phil. Creo que estaba en la diapositiva donde se hablaba de los resolutores públicos donde ponemos de relieve las consideraciones de privacidad. DoH y DoT, como sabrán, al principio fueron bastante polémicos. Planteaban ciertas inquietudes al principio pero los operadores de resolutores cada vez más lo fueron implementando y en general es una buena práctica para la privacidad.

La pregunta que tengo es: ¿Cuánto de estas consideraciones en materia de privacidad tendrían que formar parte de KINDNS? Cuando ustedes consideran las prácticas y la documentación sobre buenas prácticas generales que tenemos hasta el año pasado, las consideraciones en materia de privacidad no están puestas de relieve demasiado pero en los últimos tiempos hemos dado mucha más atención a las consideraciones de privacidad. La minimización de Qname es algo que se utiliza desde la perspectiva de los resolutores. Es

algo sencillo. Se basa en software. Creo que no genera ninguna controversia eso o no la veo por lo menos.

Sin embargo, cuando hablamos de DoT o DoH, aquí a veces hay algunos que fruncen el ceño. Nosotros no sabemos si mencionarlos como buenas prácticas o no. Nosotros en nuestra lista de distribución no hemos hecho tanto hincapié en estos dos, en particular en DoT pero quisiera saber cuál es la opinión del público desde el punto de vista de la privacidad con respecto a DoT y DoH. Veo que hay alguien que está levantando la mano. ¿Alguien le puede dar al participante la posibilidad de habilitar su micrófono? Ulrich.

ULRICH WISSER: Hola. Muchísimas gracias, Adiel, por permitirme hacer uso de la palabra. Quería decir que DoT resuelve algunas de las consideraciones en materia de privacidad porque no permite que las personas en el pase puedan escuchar su solicitud pero hay que depositar mucha confianza en el operador. Obviamente eso solamente se puede resolver con un DNS que pasa las cosas al olvido pero no sé si eso puede considerarse una práctica adecuada. DoT resuelve alguno de los problemas de privacidad pero está muy lejos de resolverlos todos.

ADIEL AKPLOGAN: Muchas gracias. Es un buen comentario desde la perspectiva de un operador. Mencionamos algo que es importante y también interesante. Hay una relación de confianza que ya existe en cierta forma entre el usuario de un resolutor y el proveedor en el contexto de los ISP. Es obvio que hay un acuerdo de servicio. Eso implica cierto

nivel de confianza. Esto puede hacer que las consideraciones en materia de privacidad se manejen de determinada manera. En una red corporativa, donde hay una política que indica que uno tiene que utilizar el resolutor correspondiente a esa empresa, el aspecto de privacidad también está manejado porque allí se utiliza una red corporativa. Hay que cumplir con determinados requerimientos. Cuando todo esto está abierto, es allí donde tal vez el tema de la privacidad se torna más crítico.

Tratamos de incluir de manera más subrayada las consideraciones de privacidad en lo que tiene que ver con los resolutores abiertos y públicos donde cualquiera decide utilizar un resolutor y allí puede haber más preocupación por la privacidad y lo que se envía a través de ese resolutor.

¿Alguien más tiene algo para compartir con respecto a los resolutores o, por supuesto, los recursivos o los autoritativos o cualquiera de los aspectos que estamos incluyendo aquí? Muy bien. Si no tenemos más preguntas o comentarios tal vez podemos interpretar que estamos bien encaminados. Les quiero agradecer a todos aquellos que ya se han incorporado a la lista de distribución y que han empezado a hacer aportes a esta iniciativa. Creo que hay una pregunta. Me la perdí. La pasé por alto.

KINGA KOWALCZYK: Sí. La pregunta es si la medición es parte del diseño de KINDNS, una forma de medición a través de la cual la comunidad tenga formas de acceder a los datos del resolutor mantenidos por varios resolutores y

un método de comparación. La pregunta es si la medición es parte del diseño de KINDNS.

ADIEL AKPLOGAN: Tenemos un identificador, un indicador que nos va a permitir ver si esto está impactando en el aspecto de seguridad de la operación de DNS. Eso es lo que tenemos planeado. ¿Cuáles serán esos indicadores? Todavía no están claramente definidos. Tal vez podemos compartirlo también a partir de otras iniciativas que ya existen como [ITHI] pero con respecto a los datos del resolutor, no sé qué datos se están mencionando aquí o cuáles es su relevancia pero cuando tratamos de medir, tratamos de pensar en medir lo que desde nuestra perspectiva se puede medir sin acceder a datos privados.

Probablemente midamos solamente aquellas cuestiones relacionadas con las buenas prácticas que nosotros hayamos identificado. Podemos decir tal vez que el número de resolutor que tiene una consideración de privacidad y que se ha visto en el último año, ver tal vez aquellos resolutores que tienen el DoT o DoH o la minimización de Qname.

No sé si refieren a acceder a los datos del resolutor porque si hablamos de acceder a los datos del resolutor, entonces entramos en un ámbito totalmente diferente. Vamos a medir lo que se pueda ver en forma pública pero solamente relacionado con las buenas prácticas que hayamos identificado.

También queremos tener tantos operadores resolutores como sea posible en nuestra iniciativa y que adopten las buenas prácticas. Si tenemos la posibilidad de cooperar y trabajar en conjunto con estos

operadores y hacer alguna medición y algún estudio, por supuesto esto va a enriquecer la iniciativa pero tratamos de que sea lo más sencillo posible, para que lo que presentemos no genere ninguna polémica, ninguna controversia ni al usuario ni a aquellos que van a aprovechar el resultado de esta iniciativa.

Muy bien. La lista de distribución está abierta. Siéntanse libres de sumarse a ella y podemos continuar con el debate allí. Pueden hacernos llegar sus sugerencias, sus consultas o pueden contactarse en forma directa con nosotros. Pueden escribir directamente a octo@icann.org si lo desean.

Veo una pregunta de Desiree. Gracias. Sí. Como mencioné, hay un componente de comunicación y de difusión externa que se aplica a la comunidad en general y si bien tenemos un programa de embajadores oculto por algún lado para promover esto, la ICANN también cuenta con algunos recursos para la comunicación y la promoción de esta iniciativa. Por supuesto, el éxito depende de la vía de promoción y cómo podemos facilitar la evaluación y el uso por parte de la comunidad.

Muy bien. Muchísimas gracias a todos por sumarse a esta sesión. Nos quedan solamente nueve minutos. No veo ninguna pregunta que haya llegado. Con gusto vamos a poder continuar la conversación a través de correo electrónico para seguir hablando del tema. ¿Algo más, Kinga, a lo que debamos prestarle atención?

KINGA KOWALCZYK: No. Hemos respondido a las preguntas. Muchísimas gracias a todos. La presentación va a estar disponible en el sitio web de la ICANN73 en un par de días. Muchísimas gracias.

ADIEL AKPLOGAN: Gracias, Kinga. Gracias, Steven. Gracias, Phil, también. Adiós a todos.

PHIL REGNAULD: Gracias.

[FIN DE LA TRANSCRIPCIÓN]