ICANN76 | Foro de la comunidad – Programa de Becas de la ICANN: introducción de la OCTO de la ICANN y KINDNS
Domingo, 12 de marzo de 2023 – 10:30 a 12:00 CUN

SIRANUSH VARDANYAN: Tomen asiento, por favor. Vengan más cerca. Esta es una sala bien grande y queremos verlos a todos. Tomen asiento. Vengan aquí, frente a este escenario. Gracias.

Los miembros de NextGen y los becarios que están sentados por ahí, vengan aquí delante, a sentarse aquí delante. Aquí hay asientos. Vengan y siéntense aquí. Quiero verles las caras a todos. Quiero ver sus sonrisas también.

Vamos a comenzar la sesión. Por favor, inicien la grabación. Gracias. Hola a todos. Bienvenidos a este segundo día de ICANN76. Espero que todos lo hayan pasado bien ayer, que les haya gustado. Mi nombre es Siranush Vardanyan y quiero darles la bienvenida a esta sesión con nuestro equipo técnico, el equipo de IANA. Ellos les van a contar un poco más sobre todas estas abreviaturas.

Antes quiero hacer un breve anuncio. Voy a ser la coordinadora de la participación remota para esta sesión y esta sesión será grabada y se rige por los estándares esperados de conducta de la ICANN. Durante esta sesión, las preguntas y los comentarios presentados en el chat se leerán en voz alta si se presentan en el formato correcto, como se indica en el chat. Si quieren hablar durante esta sesión, por favor, levanten la mano y cuando mencionen su nombre los participantes

virtuales activarán su micrófono en Zoom y los participantes presentes utilizarán un micrófono físico. Tenemos dos micrófonos volantes aquí.

Para el beneficio de todos los participantes les pedimos que digan su nombre para los registros y hablen a una velocidad razonable. Tenemos hoy interpretación en seis idiomas y quiero alentarlos a todos a que antes de sentarse tomen los receptores y utilicen la interpretación. Tenemos excelentes intérpretes que están trabajando con nosotros hoy.

Con esto quisiera presentar a nuestros oradores hoy. Vamos a comenzar con John Crain, que es el CTO. Es el director de la Oficina de Tecnología. También Kim Davies, quien nos hablará sobre IANA. Vamos a comenzar con John. Adelante, John. Tiene la palabra.

JOHN CRAIN: Funciona bien. Muy bien. Gracias. Estoy muy contento de verlos a todos aquí hoy. Como ustedes saben, los becarios y los NextGen son mis grupos favoritos en la ICANN porque todos tienen ideas nuevas, son caras nuevas y es muy bueno poder estar aquí. Mi nombre es John Crain. Soy vicepresidente sénior y CTO en la ICANN. Estoy en la ICANN desde hace un par de décadas. Ha pasado un tiempo ya. Soy parte de los muebles casi.

Yo llevo adelante un grupo que se llama IROS. Seguramente no lo conocen. Es una distinción interna que tenemos. Nosotros somos un grupo de siglas. Nos encantan las siglas. IROS significa identificadores, es decir, nombres de dominio, direcciones de IP, todo investigación

sobre identificadores, operaciones y seguridad. Todo se trata de identificadores y lo que ocurre con estos identificadores.

Podemos dividir todo esto en algo así como tres módulos. Tenemos un grupo denominado IANA, que es la autoridad de asignación de nombres de Internet que está gestionada por Kim Davies, que es el caballero aquí a mi lado. Luego tenemos un grupo que está muy concentrado en los compromisos de las cuestiones técnicas y que está gestionado por mi amigo Adiel. Tenemos también a David, que está aquí a mi derecha.

Gran parte de la investigación y dos de los gestores que trabajan conmigo, veo a uno de ellos que se está escondiendo entre la comunidad… Di hola, Samaneh. Podrías venir. No veo a Matt pero sé que Matt puede venir o puede quedarse un poco por ahí atrás, así con un poco de timidez. Eso es lo que hacemos. Hacemos investigación sobre todas las cuestiones que afectan a los identificadores. El equipo de la IANA gestiona todos estos identificadores desde una perspectiva operativa. Vamos a hablar de todos estos asuntos.

No quiero dedicar mucho tiempo a contarles sobre esto. Lo que quiero es contarles un poco de lo que hacemos. Me voy a ocupar de quizá lo más importante que hace la ICANN, que todos escucharon que es la gestión de políticas, la formulación de políticas. Las políticas son importantes solamente si podemos establecerlas y podemos gestionar todos estos identificadores. ¿Por qué no nos cuentas, Kim, sobre el rol de IANA?

KIM DAVIES: Voy a ser breve porque tengo una presentación. El rol de la IANA esencialmente es ser un repositorio de todos los identificadores. Seguramente todos ustedes conocen los nombres de dominio cuando hablamos de identificadores pero no son los únicos, de ninguna manera. Las direcciones IP son seguramente algo familiar para ustedes pero literalmente hay miles de identificadores que permiten la comunicación en Internet que ustedes seguramente no conocen. Para que Internet funcione tiene que haber algún lugar centralizado donde todos esos identificadores se asignan. Esto se tiene que hacer con consistencia en todo el mundo. Esto está en el centro de lo que hace la IANA. Vamos a hablar de eso en un momento pero esto es un resumen de lo que vamos a hablar después.

JOHN CRAIN: La R significa research, investigación. Cuando hablamos sobre las cuestiones básicas de lo que hace su grupo, ¿por qué no nos cuenta lo que hace su grupo?

SAMANEH TAJALIZADEHKHOOB: Soy Samaneh y lidero un grupo de investigación sobre seguridad, estabilidad y flexibilidad dentro de la oficina del CTO. Los temas de los que nos ocupamos tienen fundamentalmente que ver directa o indirectamente con la seguridad del DNS. Se podría tratar de algunos de los asuntos que ustedes escuchan mucho dentro de la reunión de la ICANN que es el uso indebido del DNS y también la configuración de seguridad del DNS, todas las cuestiones indirectas que afectan a los nombres de dominio, que afectan el uso indebido

como el phishing, el malware, botnet, comando y control, eventos de seguridad, protocolos de seguridad, etc. Le voy a dar ahora la palabra a Matt.

MATT LARSON: Soy Matt Larson. También lidero un equipo de investigación. A veces hacemos seguridad pero no siempre está concentrada como lo hace el equipo de Samaneh. Trabajamos mucho. Somos muy afortunados de tener acceso a los datos de los servidores de raíz de la ICANN. Hacemos investigación en eso y también hacemos investigación sobre la base de los contenidos del DNS. Accedemos a los archivos de los ccTLD y estos son algunos de los conjuntos de datos más importantes. También somos muy activos en el IETF. Hacemos clarificación de protocolo, mejoras y documentos relativos a todo lo que es lo operacional.

JOHN CRAIN: David, ¿por qué no nos habla del trabajo de operación?

DAVID HUBERMAN: Hola. Buenos días a todos. Soy David Huberman y trabajo en lo que denominamos el compromiso técnico. Somos básicamente ingenieros en el mundo que trabajamos con la comunidad técnica y no técnica para generar capacidades, habilidades sobre DNSSEC, el ruteo seguro, el ángulo RPKI, los RIR. Trabajamos especialmente con las comunidades no técnicas sobre temas que tienen que ver con la ICANN para que todos puedan comprender muy bien la ingeniería que está por detrás de la infraestructura de Internet y cómo está construida esta

Internet. También nos asociamos con muchos de nuestros amigos y colegas aquí en la ICANN en esfuerzos dentro de los gobiernos, la comunidad no técnica, para poder garantizar que todos estén hablando el mismo idioma en cuanto a cómo funciona Internet.

JOHN CRAIN: Fue un muy buen resumen. Vamos a ir a las preguntas en un momento. Escuché ya bastante pero el equipo de IROS, que se pare por favor. El equipo es mucho más grande que esto pero trajimos un pequeño contingente a la reunión para que podamos interactuar con la comunidad y trabajar aquí. Es importante que les escuchemos a ustedes. Le voy a pasar la palabra a mi colega para ver si hay preguntas.

SIRANUSH VARDANYAN: Gracias, John. Esta sesión está planificada para los NextGenners y los becarios. Por eso quiero alentarlos a todos a que hagan preguntas, porque esta es una oportunidad única para todos ustedes. Muchos no son técnicos pero es muy importante poder entender de qué manera desde el punto de vista técnico funciona la ICANN. No tengan vergüenza. Como dije, durante la sesión anterior nunca hay preguntas tontas. Hagan preguntas entonces. Podemos empezar ahora mismo incluso. Lo que les resulte interesante lo pueden preguntar. Tenemos aquí micrófonos. Quizá puedo pedir que haya micrófonos en este costado. Levanten la mano. Muy bien. Ahí vienen los micrófonos. Dos segundos, por favor. ¿Puede tomar el micrófono, por favor? Vamos a comenzar aquí.

HARISH CHOWDHARY: Hola a todos. Soy Harish Chowdhary. Soy becario. También soy investigador en una universidad de India. Mi investigación se basa en la seguridad del DNS. Al equipo de investigación, mi pregunta es cómo puedo contribuir. Específicamente estoy trabajando en el ccTLD .IN, en la seguridad de este ccTLD y en las mediciones. ¿Cómo puedo entonces contribuir a este trabajo? ¿Cómo podemos generar nuevas tecnologías para el equipo, para poder trabajar con ambos equipos?

JOHN CRAIN: Samaneh, ¿quieres responder?

SAMANEH TAJALIZADEHKHOOB: Gracias, John. Gracias por esta pregunta. Me alegra tenerlos a todos aquí en la sala. No sé si ustedes conocen el proyecto DAAR, que ICANN tiene ya desde hace dos años. Es una herramienta de actividad de informes de dominios y somos parte de este trabajo. Tenemos una colaboración con el .IN. Me gustaría saber en qué asuntos trabaja usted y si podemos quizá trabajar en conjunto, así podemos darles datos que les resulten útiles. Quizá lo puedo guiar hacia el punto indicado. Hacemos mucho trabajo en cuanto a la seguridad de los TLD. Estas son áreas en las que les puedo resultar quizá útil.

JOHN CRAIN: Si me permiten, también publicamos muchos documentos en algo que denominamos la serie OCTO. Si las ven y les resulta interesante y les

parece que eso está bien o les parece que es horrendo, esperemos que no, nos pueden escribir comentarios. Tómense el tiempo para hablar con Samaneh o con cualquier parte del equipo aquí. Siempre estamos abiertos a colaborar y a ver si hacemos la investigación correcta o si la podemos mejorar.

SIRANUSH VARDANYAN: Nicolas, tiene la palabra.

NICOLAS FIUMARELLI: Hola, equipo OCTO de ICANN. El ruteo de la ICANN no es parte de los objetivos de la ICANN pero ustedes acaban de hablar del RPKI y la importancia de la seguridad. ¿Puede aclarar de qué manera la seguridad del ruteo funciona en el trabajo de la ICANN? Además, si la seguridad de ruteo está dentro de la investigación de la ICANN, me da curiosidad conocer la resiliencia y la infraestructura de las grandes empresas y las aplicaciones conocidas. Hace algunos años por ejemplo hubo un incidente que involucró a Meta, que antes era Facebook, que también involucraba al DNS y quisiera saber si nos podían contar de qué manera empresas como META tratan la seguridad de ruteo y cuál es la infraestructura y su resiliencia. Gracias por su tiempo y sus respuestas.

JOHN CRAIN: Son muchas preguntas. Voy a tratar de responder. La primera es simple. ¿El ruteo está dentro del alcance de la ICANN? ICANN no se ocupa del DNS sino de los identificadores. El ruteo es a las direcciones

IP lo que la resolución es al DNS. Si consideramos eso, tenemos un punto de vista interesante. Con el DNS lo que tenemos es un socio porque ICANN es parte de una comunidad que tiene registros, registradores, proveedores de resolutores y el mundo de las direcciones IP es parte de esta investigación. En general tiene que ver con los RIR, que son los registros regionales de Internet, etc. Es un área diferente del DNS pero no hacemos solamente DNS. Le voy a dar ahora la palabra a David para que nos hable un poco de todas estas cuestiones.

DAVID HUBERMAN: Es una muy buena pregunta. Es una pregunta que a veces nos hacemos internamente porque no queremos salirnos de nuestro mandato. El RPKI, y esta muy buena idea de rutear la seguridad, mientras que los proveedores de servicios de Internet y todos los participantes en el ruteo de Internet pasan tráfico y pasan anuncios sobre quiénes son, esta es mi red, estos son los servicios que tengo, si quieren llegar ahí, llegan a través de estos anuncios de ruteo. Desde hace 30 o 40 años esto es inseguro y ahora los estamos asegurando a través de una infraestructura que puede, esperamos, prevenir gran parte de los accidentes y gran parte del uso indebido que a veces leemos. Como industria no queremos que ustedes lean esto porque no queremos que esto ocurra. Queremos que la infraestructura subyacente simplemente funcione para que cuando ustedes tomen su dispositivo puedan ir a cualquier sitio web y que funcione y que no lo tengan que pensar.

Tenemos esta capa de seguridad que estamos armando y tenemos que asegurarnos de que esté bien hecha. A la vez, tenemos que ser

conscientes del hecho de que todos los nombres y las infraestructuras que están dentro de nuestro alcance estén detrás de la infraestructura de Internet, detrás de esta capa de seguridad. Si no se hace bien y no podemos acceder a los servidores de nombres, a los resolutores, si no podemos tener acceso a los distintos componentes, esto es un problema. Prestamos mucha atención a esto.

Usted pregunta específicamente sobre META. En octubre de 2021 Facebook estuvo indisponible durante un día entero. La razón fue el DNS. Es un meme en el mundo de Internet que si algo deja de funcionar es la culpa del DNS. Aquí había una configuración muy interesante donde el acceso físico a los edificios, por ejemplo, entrar a un centro de datos, a una oficina de Facebook, utilizan tarjetas como en cualquier otra empresa pero todo el sistema estaba vinculado al sistema de DNS para poder autenticar quiénes somos y utilizar el DNS para encontrar los repositorios donde está toda esa información, pero hubo una falla interna que hizo que el DNS no esté disponible, no solo al mundo sino todos los sistemas dentro de META.

Quiere decir que cuando uno quería entrar a través de una puerta para autenticar se tenía que utilizar el DNS y no tenía acceso al DNS. Esta es una forma muy creativa de hacer que las cosas no funcionen. Esto le enseñó no solo a META sino a todos a pensar en que cuando construimos la infraestructura, sea IT corporativo o cuestiones muy grandes que la gente necesita, tenemos que pensar en el ruteo, la autorización, la autenticación y el DNS, y no crear islas, vallas, que pueden hacer que se genere una isla y que las cosas no funcionen. Creo que todos aprendieron de ese incidente.

JOHN CRAIN: Si miran esta reunión, va a haber gente de META. Fue la red de ellos y el problema de ellos. Quizá ellos pueden responder esta pregunta.

SIRANUSH VARDANYAN: Para la interpretación, por favor, les pedimos que hablen a una velocidad razonable. Tenemos aquí una pregunta remota de Shanelle McPherson, que es NextGen de ICANN76. A último momento no pudo venir pero su pregunta es para el equipo de John Crain. "¿De qué manera se implementa el DNSSEC y cómo puede un ISP de un país involucrarse para implementarlo?"

JOHN CRAIN: Primero que nada, Shanelle, lamento que no pudiste venir. Esperamos poder reunirnos en el futuro. Te pedimos que sigas solicitante venir a las reuniones de la ICANN. Primero le voy a pasar esta pregunta a Kim para que nos cuente cómo se pone esto en la raíz y le voy a pedir a David que nos cuente sobre el trabajo que hacemos en cuanto a la participación en DNSSEC. ¿Por qué no nos cuenta sobre la raíz?

KIM DAVIES: Muchas gracias, John. Una de las funciones de la IANA, de la que no hemos hablado todavía, es gestionar la zona raíz del DNS. Esta es la pieza más crítica del DNS, es el primer sitio para las computadoras que acceden a este sitio. Contiene los registros autoritativos de los

dominios que existen y es donde están los servidores que se encargan de esos TLD.

Una parte de nuestra responsabilidad a la hora de gestionar esta zona raíz incluye gestionar las llaves criptográficas que aseguran esta zona para el DNSSEC. Es una parte muy importante de nuestras operaciones. Dedicamos muchos recursos a esa función dentro de la IANA. Esto es porque DNSSEC funciona a través de una clave única central de la cual dependen todos para comenzar este proceso. Es crítico que se mantenga segura esta clave, que se reconozca por parte de la comunidad y que no suponga riesgos de acceso no autorizado.

Hacemos esto al asegurar esta clave. Tenemos instalaciones muy seguras para esto y cada tres meses accedemos a esta clave para hacer uso de ella. Hacemos ceremonias de la clave e incluimos a la comunidad. Se emite por Internet. Lo hacemos para que los expertos en seguridad puedan monitorizar y ver lo que estamos haciendo, y que digan si efectivamente ICANN sigue el procedimiento correcto, no existe riesgo de que se utilice esta clave de otra manera que no sea segura y todos están satisfechos.

Como dije, esta es una parte clave de nuestros procesos operativos. Podría hablar durante una hora sobre esto. Es un tema interesante pero esta es una de las responsabilidades más fundamentales de ICANN y la IANA en cuanto a la seguridad del DNSSEC. Sé que han hablado del ISP. Ahora le voy a pasar la palabra a mi compañero.

DAVID HUBERMAN: Después de que el equipo de Kim ha hecho un gran trabajo para que funcione esta clave en la zona raíz, tenemos que usarla. ¿Cómo se hace? Pasamos un nivel más abajo. Es decir, el TLD. .COM, .MUSEO, etc. Aquí quiero centrarme en los códigos de país. Estamos en México. .MX. Si queremos hacer el DNSSEC aquí en México vamos al registro, vamos al operador del registro de .MX y ese operador firma su propia zona y ofrece validación y firma DNSSEC para todos los dominios que estén por debajo.

Estoy mirando al público. Veo a Nicolás Antoniello. Él vive en Uruguay. Lo que hace es que va a los diferentes ISP y a los operadores de registros de TLD. Trabaja con ellos para establecer la firma del DNSSEC. Les enseña todo sobre cómo funciona y cómo utilizar estas herramientas. Sobre todo trabaja con los ISP para saber que están validando, que están resolviendo los DNSSEC. La ICANN funciona a nivel de raíz para que todo se pueda validar y autenticar con las claves. Trabajamos también con los ISP y los registradores para que tengan las herramientas y el conocimiento. También el apoyo que necesitan para ofrecer el DNSSEC a otros niveles.

SIRANUSH VARDANYAN: Muchas gracias. Setondji, me parece que tienes la mano levantada. Gracias, Betty, por ayudarme. Después Oliver.

SETONDJI HOUNZANDJI: Me gustaría hablar en francés. Muchas gracias. Me llamo Setondji. Soy administrador de sistemas. Gestiono el servidor Linux. Soy de Benín

pero vivo en Francia. Mi pregunta tiene que ver con los ccTLD. Me interesa mucho todo lo que tenga que ver con el DNS. Yo trabajo en cómo asegurar los servidores del DNS. Mi pregunta tiene que ver con los ccTLD porque, como ya saben, en muchos países los registros de los ccTLD se eligen por parte de un gobierno y nos hemos dado cuenta de que a menudo los ccTLD no están bien configurados, no se gestionan ni se administran bien.

Mi problema consiste en descubrir si es posible que la ICANN haga una auditoría de todos los ccTLD para publicar normas acerca de lo que se tiene que hacer. Saben que hoy en día muchos ccTLD no hay implementado en el DNSSEC. ¿Qué puede hacer la ICANN? Me gustaría que la ICANN obligara a las personas. Por ejemplo, podrían lanzar una auditoría sobre algunos ccTLD y les dicen que no están al día y que no pueden seguir trabajando con ellos. Se puede enviar a un auditor y ciertos procesos para que se pongan al día. Si los ccTLD americanos y europeos están asegurados pero los africanos no, esto es un problema. Hemos hablado de un mundo, una Internet. No puede ser un mundo y muchos internets, gracias.

JOHN CRAIN: Muy bien. Gracias. Voy a dividir esto en dos partes. Una parte tiene que ver con el estado del entorno ccTLD y el estado técnico. Ha hecho algunos comentarios interesantes pero quizá podemos hablar de eso en otro momento porque me gustaría saber qué datos tienen porque nos interesan mucho los datos. Ha hablado de la calidad de la infraestructura y si tienes datos sobre esto, me gustaría tener una discusión sobre esto, de lo que se ve, de lo que no se ve. Hemos oído

que muchos ccTLD no tienen la firma. Esto es un juicio. Es importante tener los datos.

La otra parte no tiene que ver con una cuestión técnica sino con una cuestión más bien política acerca de cómo se gestionan los ccTLD. No se establece la política para los ccTLD por parte de ICANN. Son códigos de país y utilizan otro mecanismo. No existe un mecanismo para que ICANN obligue a imponerse ciertas políticas en esta área. Nosotros no hacemos eso. Colaboramos mucho, muchísimo con los ccTLD. David puede hablar de esto.

Estos foros de ICANN son lugares donde puedes venir a hablar de esto. En la ccNSO se reúnen muchos ccTLD para hablar. Tienen un día técnico en casi todas las reuniones de ICANN en el que hablan de estos temas. Existe mucha colaboración entre los ccTLD con la ICANN y algunos miembros del personal con el fin de mejorar las cosas.

Yo creo que una auditoría tendría que implicar al titular de ese proceso político y eso no es competencia de ICANN. Yo creo que en un futuro próximo no vamos a ver una situación en la que ICANN pueda entrar en un registro de ccTLD y hacer una auditoría. Quizá muchos dirían que no lo tendría que hacer tampoco porque no recae sobre nuestra responsabilidad.

KIM DAVIES: Ha sido un buen resumen. Quizá tendríamos que recalcar ciertas cosas. Quizá no saben la diferencia entre un TLD genérico y un ccTLD, es decir, un código de país. Muchas de las conversaciones políticas en una

reunión de ICANN se centran en hablar de los parámetros en los que funcionan. Una vez que se decide qué normas se van a acordar, hay que decir cómo se implementan y cómo se monitorean. Hay un departamento de cumplimiento en ICANN y cada operador de los gTLD tiene que cumplir con ciertos requisitos para seguir operando y si no lo hacen en un tiempo determinado hay remedios que existen para eso.

Parece que estás buscando algún arreglo así quizá para los ccTLD pero es otra historia. Volvemos a los años 80, al principio de los DNS. Se tomó una decisión que se ha mantenido hasta ahora y es que los ccTLD pertenecen a los países. El papel de ICANN es bastante limitado. Encontrar a la persona encargada en ese país para que operen en el beneficio público dentro de ese país. Todos los mecanismos de supervisión tienen que estar en marcha en ese país para que haya un cumplimiento. Es un mundo complejo y muchos países tienen mecanismos distintos. Unos son mejores que otros, eso está claro, pero lo que puede hacer la ICANN a través de una actividad de participación técnica es promover las buenas prácticas, la creación de capacidades, hablar sobre las obligaciones y cómo cumplirlas. Es un componente tan importante de los ccTLD el hecho de que se operen dentro del país y por eso los operadores tienen no todo el control pero sí que tienen la mayor parte de la responsabilidad. Eso quiere decir que nosotros no tenemos tampoco mucho que hacer con ese respecto. Muchas gracias.

SIRANUSH VARDANYAN: Vamos a escuchar una pregunta más y luego una remota. Después Kim va a dar su presentación.

OLIVER RISTESKI: Hola. Me llamo Oliver. Soy de Macedonia. Trabajo en el Ministerio del Interior. Formo parte del Centro de Investigación de Seguridad. Tengo una pregunta. Hace poco recibimos correos con bombas falsas en aeropuertos, escuelas, centros de transporte. Nos costó bastante dinero arreglarlo. Es muy poco eficiente investigar estos delitos. En la región de los Balcanes, esto ocurre mucho. Me gustaría saber si hay posibilidades de investigar más en profundidad estas cuestiones.

JOHN CRAIN: Parece que estás hablando del phishing, del malware. Son abominables y forman parte de nuestro día a día en el Internet. Claro que podemos hacer investigación cuando esto tiene que ver con el sistema de nombres. No sé si mi compañera quiere hablar un poco de esto.

SAMANEH TAJALIZADEHKHOOB: Muchas gracias por esta pregunta, Oliver. Como ha dicho John, esto ocurre todos los días. Casi todos los usuarios de Internet experimentan este problema en nuestro grupo de SSR estamos haciendo investigaciones que se van a publicar dentro de poco sobre los métodos de identificación y clasificación de los correos de phishing, spam, malware, etc. No dejes de mirar nuestras publicaciones de OCTO. Vamos a publicar el método. Estamos haciendo una investigación académica. Una vez que se apruebe a ver si se puede utilizar en otras áreas, quizá para los operadores, etc.

JOHN CRAIN: Además hay otras cosas en las que puedes pensar. Si hay un certificado nacional, asegúrate de que forman parte de este certificado. Te puedes involucrar en esa comunidad y que las personas que responden a los incidentes estén al día porque este problema no es único. Además, a la larga se puede invertir en las universidades para crear las capacidades, el talento dentro del mismo país para entender esto, que sea investigación, respuesta a los incidentes, la creación de redes técnicas, por ejemplo.

Si tiene mucho interés en el aspecto de la seguridad pública, de cómo se utiliza Internet y quiere saber cómo se puede involucrar en eso, hay un comité asesor de los gobiernos. Es una parte importante. Hay un grupo de trabajo que se centra en la seguridad pública. Si su gobierno participa en el GAC, el Comité Asesor Gubernamental, y tienen un interés específico en esta área podrían involucrarse.

En la ICANN hablamos de lo que se llama el uso indebido técnico o las amenazas de seguridad. No todas las amenazas con las que nos encontramos en Internet, y de hecho muchas de ellas, no tienen que ver con el trabajo que realizamos nosotros. Ese tema en concreto es un tema muy importante. Ahora mismo se están haciendo varias cosas dentro de la comunidad. Hay negociaciones de contratos acerca de lo que quiere decir ser un registrador, un registro y qué hacer con respecto al uso indebido. El hecho de recibir informes, investigarlos, no son las palabras exactas pero tampoco soy yo abogado. Lo que falta en nuestro lenguaje contractual es que estas personas tienen que mitigar estos usos indebidos. Estamos trabajando a petición de las partes

contratadas. Los registros, los registradores nos dijeron que querían añadir esto a sus contratos para tener esta obligación contractual de mitigar este uso indebido.

Se está realizando esta conversación ahora. Impartimos mucha formación. Hay publicaciones, investigaciones. Estamos muy interesados en este tema. Si hay cuerpos de seguridad, por ejemplo, que quieran hablar sobre la formación, la participación, estaríamos encantados de hablar con estas fuerzas de seguridad. Lo hace mucho nuestro staff. Solemos explicarles cómo funciona el ecosistema. A veces es para presentarlos a otros actores del ecosistema. Crear confianza, por así decirlo, porque esto es clave a la hora de realizar nuestro trabajo. Puedes hablar con nosotros. Podemos hablar de tú a tú para ver qué puede hacer tu ministro y cómo puede involucrarse.

SIRANUSH VARDANYAN: Muchas gracias. ¿Podemos poner ya la presentación de la IANA? Mientras tanto vamos a ir a la pregunta de Romulo Chacin, NextGen de ICANN76. Le gustaría saber cómo los proyectos de mitigación de las amenazas interactúan entre ellos.

JOHN CRAIN: ¿Cuánto tiempo tenemos? Si miramos las competencias principales de ICANN, si miramos los estatutos, el propósito pone claramente que nos tenemos que preocupar de la seguridad, la estabilidad y la resiliencia de Internet y también de los sistemas de identificadores. No estamos hablando de las páginas web. Hola, vecinos. Estoy yendo voces.

De alguna manera es clave a todo lo que hacemos. Todo tiene que ver con la seguridad. Como personal de ICANN y también como comunidad cuando estudiamos algo siempre tenemos en mente el cómo esto afecta a la seguridad, a la estabilidad. Hay interacciones por todas partes. Dentro de IROS la IANA hace bien su trabajo, como siempre. Esto es crítico para la estabilidad del sistema, lo que se refiere al registro de los identificadores. También realizamos investigación, hacemos participación, difusión externa. Como ha dicho Kim, también está el cumplimiento contractual. Tenemos negociaciones contractuales. Permitimos estas discusiones políticas y todo esto afecta a la seguridad y la estabilidad de los sistemas de identificadores. Este es nuestro trabajo.

SIRANUSH VARDANYAN: Gracias. Kim, te voy a dar la palabra para que nos hables sobre IANA.

KIM DAVIES: Esta es una buena oportunidad mientras tenemos esta conversación de hacer un tour rápido sobre cuáles son las funciones de la IANA, algo que seguramente ustedes escucharon mucho durante alguna reunión de la ICANN. Seguramente ustedes ya saben qué significa la palabra IANA. La idea aquí es ser breve sobre las funciones de la IANA. Esperamos que esto les resulte útil. Vamos a tener preguntas después. Si surge algo, les vamos a pedir que nos lo digan.

Hablamos un poco sobre esto ya. La autoridad de asignación de nombres de dominio, más allá del nombre, hacemos más que

números. Hacemos parámetros de protocolo. Hacemos otro tipo de identificadores también. En esencia, se trata de una de las instituciones más antiguas de Internet. Al principio de los primeros años de Internet, cuando era un proyecto de investigación, esos primeros nodos estaban conectados, y en los 60 y en los 70 alguien tenía que tener un registro de qué estaba conectado a qué y este rol fue jugado por Jon Postel, que es la persona que está a la derecha, al lado de Vint Cerf. Jon Postel fue la personificación de la IANA desde el principio. Después IANA recibió su nombre y recibió ese nombre precisamente en los años 80.

IANA empezó a ser más de que una persona. Se convirtió en un equipo. En última instancia, este fue el propósito original. Sigue siendo el propósito hoy. Para qué se utilizan los archivos de la IANA y si hay una autoridad de registrar estos identificadores y qué es lo que esto ha generado.

En los años 90 se reconoció que las funciones de la IANA en particular y la gestión de la zona raíz requerían de una estructura un poco más formal y no solamente una persona académica, Jon Postel trabajaba en la universidad, más allá de lo que él podía hacer individualmente y con su equipo. En los 90 esto se formalizó. Se reconoció la comercialización de Internet, el crecimiento y la creciente demanda de la función de IANA. ICANN se creó para gestionar la IANA. Esa fue su función principal.

El primer nombre fue la nueva IANA. Hoy ICANN existe por este propósito central. ICANN tiene otros alcances más allá de la IANA pero sigue siendo central en la función de la IANA. Hoy IANA es un

departamento en la ICANN. Hablamos de los identificadores únicos de Internet. Cada uno de estos registros tiene una política distinta. Parte del trabajo de este equipo es aplicar estas políticas dependiendo del tipo de identificador y de la situación.

Cuando escuchen IANA se va a referir a esta función de asignación, este registrador dentro de la ICANN. ¿Por qué necesitamos a haya alguien que lleve adelante los registros? ¿Internet no está libre de un control centralizado? Las computadoras se hablan entre sí utilizando protocolos técnicos. No todos son lo mismo. Las computadoras se entienden entre sí. El contenido se transmite a través de esos protocolos. Hay protocolos centrales como TCP/IP. Este es un ejemplo.

Tienen que funcionar en todos los dispositivos para que la red funcione. Gran parte del trabajo que hacemos entonces en la IANA no solamente se trata de los protocolos como los nombres de dominio sino también lo que funciona a niveles más bajos en la computadora para garantizar que la transmisión entre los distintos dispositivos en Internet funciona, sea preciso y que ese adjunto sea recibido en el formato correcto, que cuando uno se conecte a un servicio no reciba una llamada de teléfono en lugar de un sitio web. Todos estos identificadores tienen un propósito específico para poder ayudar en esa comunicación. Los proveedores de software utilizan las asignaciones de IANA para que su software funcione con los de otros en Internet.

Las funciones hoy se llevan adelante por el equipo de IANA. Hay distintos contratos. Hay toda una cantidad de contratos mezclados. Otro término que ustedes pueden escuchar esta semana es la PTI. PTI

es una afiliada de la ICANN. Piénsenla como una subsidiaria de la ICANN que realiza efectivamente las funciones de la IANA. La PTI no es una distinción importante que tengamos que tener en cuenta. Una de las salvaguardas que implementamos en el año 2016, cuando la transición de múltiples partes interesadas ocurrió, las funciones de la IANA se pusieron en una organización diferente de la ICANN pero una organización que la ICANN de todos modos controla y esa es la PTI. Si escuchan ustedes el término PTI no se preocupen. Sepan que es el nombre anterior de la entidad que opera las funciones de la IANA. Es una operación diaria como en cualquier otro departamento de la ICANN. Somos 16 personas. Esto es lo que hacemos como trabajo.

¿Cuáles son entonces las funciones de la IANA, un poco más en detalle? En general, las dividimos en tres secciones: parámetros de protocolo, recursos de número y nombres de dominio. Esta distinción es un poco arbitraria. Hay un poco de superposición pero, en general, funciona bien dividirlo en estas tres áreas.

Me voy a centrar primero en los parámetros de protocolo. Básicamente son el aspecto central de lo que hacemos. Los parámetros de protocolo, hay miles de tipos de parámetros de protocolo. Hay cientos de miles sino millones de asignaciones de parámetros de protocolo. Son muchas. Hay muchas de las que nunca escucharon hablar. Hay un porcentaje que yo ni escuché. Muchas se utilizan en aplicaciones específicas y salvo que estén creando ustedes software para una cuestión muy específica, no van a necesitar nunca estos registros pero para las 5, 10 o 50 personas que trabajan en la industria que implementan software en torno a estos identificadores, el trabajo que

hace la IANA tiene mucho valor. Hay un índice en iana.org/protocols. Ahí pueden ver la lista completa.

Para los parámetros de protocolo, la IANA tiene un rol central en la implementación para desarrolladores de protocolo, proveedores de software, que vienen y hablan directamente con IANA, reciben las asignaciones que necesitan a partir de nosotros directamente. Esto es lo que distingue a nombres de dominio y a recursos de número. En general, la gente no viene a la IANA para recibir un nombre de dominio ni un recurso de número. Sin embargo, lo que tienen en lugar de esto es un sistema de asignación jerárquica donde hay un intermediario con distintos tipos de responsabilidades. La IANA es una parte muy pequeña de esa asignación. Parte de la razón es que hay una política que se debe aplicar para los recursos de número y los nombres de dominio.

¿De dónde provienen entonces estos registros? La gran mayoría se desarrollan en el IETF, el grupo de trabajo de ingeniería de Internet. Este es el organismo de estandarización principal de Internet, que es donde la mayor parte de la estandarización o normalización ocurre. Cuando se generan normas de Internet dentro del IETF un componente de esto se genera en los registros de la IANA que van junto con estos estándares. Seguramente escucharon hablar de los RFC. Son una serie de documentos donde se publican los estándares de Internet. Muchas RFC crean, modifican e incluyen instrucciones sobre lo que la IANA tiene que hacer y lo que debe aplicar.

Vamos ahora a hablar de los recursos de número. Para los que no están familiarizados, estos recursos de número en general se refieren a tres

cuestiones principales. Las direcciones de protocolo IPv4, las IPv6 y los números AS. Los que no conocen las direcciones IP, hay dos versiones. La versión 4 y la versión 6. Estos son números únicos que se asignan a cada dispositivo en Internet. Tu computadora tiene uno, los dispositivos en casa tienen otro, la TV seguramente tiene otro. Cada vez más hay distintas cosas en el mundo que las tienen. Este es el identificador único que se utiliza para transmitir datos de un dispositivo a otro. La transmisión se hace a través de Internet. Cada transmisión se conoce como un paquete que tiene que tener una dirección, que son direcciones IP.

Como hay millones de estas direcciones lo que necesitamos es una forma de poder agregarlas en un set para que sea más fácil de manejar y que los ingenieros no tengan que escribir cada dirección de IP individualmente. Esto se hace con sistemas AS o sistemas autónomos de número. Son como códigos postales de Internet. Los proveedores de red agrupan conjuntos de direcciones IP en un solo número AS y cuando hablan sobre cómo enviar tráfico en Internet utilizan los números AS para que sea mucho más fácil.

Ya les hablé sobre qué son. Voy a decir que las direcciones de IP versión 4 se acabaron. Asignamos las últimas direcciones IPv4 disponibles hace algunos años. A los Registros Regionales de Internet les quedan muy pocas direcciones de IPv4. Hay muchas iniciativas para pasar a IPv6, que tiene mucha más capacidad de crecimiento.

Los Registros Regionales de Internet se los voy a mencionar brevemente, para los que no lo conocen. Uno no viene directamente a la IANA para pedir una dirección IP. Lo que hace es que, como usuario

final, automáticamente se le asigna una dirección de IP, la asigna el proveedor de Internet. Estos son los protocolos en los que trabaja la IANA. DHCP asigna la dirección IP en un dispositivo y cada proveedor de red, sea un ISP o una red de conferencia en un hotel, tiene un conjunto de direcciones IP que comparte entre las personas en la red. ¿De dónde reciben estos bloques? Los reciben de los registros regionales de Internet. Hay cinco RIR. LACNIC es el de México aquí y cada uno de ellos son los que asignan las direcciones IP y los números AS dentro de la región. Los RIR a su vez dan asignaciones de IANA.

Por último, los nombres de dominio. ¿Cuál es el rol de los nombres de dominio? Vamos a saltearlo. En cuanto a la jerarquía de DNS, la parte central del espacio de nombres de dominio es la zona raíz. Esta es una parte central, esencial de lo que hacemos en la IANA. Aquí ven que por debajo de la raíz tenemos los TLD. A la vez asignan etiquetas en el primer nivel, en el segundo nivel, etc. Nuestra responsabilidad principal dentro de la IANA es la administración de la zona raíz del DNS y de nuevo este es el registro autoritativo de cuál es un TLD. Luego está toda la información técnica y también la información administrativa, como quiénes son los puntos de contacto, cuál es la empresa que opera ese TLD, este tipo de cuestiones. Nosotros somos una entidad que guarda estos registros. Recibimos actualizaciones, cambios administrativos a los TLD. También hacemos debida diligencia en algunos tipos de pedidos. La IANA, una vez que está satisfecha con los cambios adecuados a la raíz, enviamos la implementación a los servidores de zona raíz en Internet.

Esto lo mencioné antes. Nosotros tenemos la clave de la firma de la llave, que es la que asegura el DNS también. Hacemos una ceremonia de firma de clave y lo hacemos de esta manera para promover la confianza. Lo hacemos de esta forma tan pública. Podemos hacer todo ese trabajo para el DNSSEC en privado y podríamos decir que somos ICANN y confíen en nosotros. Pero una mejor manera de hacerlo es incorporarlos a todos ustedes en el proceso y darle a la comunidad acceso, visibilidad. Creemos que esto promueve la confianza, porque todo el mundo puede ver con sus propios ojos lo que hacemos, los expertos de seguridad en el mundo ven lo que hacemos y colectivamente lo pueden ver y decir: “Esto se está haciendo de un modo seguro y podemos confiar en el sistema”.

Otras funciones que tenemos en el espacio de dominios. Operamos el .INT, uno de los TLD. Estos son organizaciones de tratado intergubernamental. También operamos el .ARPA. Este es un dominio que ustedes seguramente no verán directamente pero es importante para las operaciones directas. También tenemos un repositorio de reglas de generación de etiquetas. Estos son nombres de dominio internacionalizados que comparten las mejores prácticas.

Esto de alguna manera resume las operaciones de la IANA. Sé que es una descripción muy general pero no quería terminar con la seguridad. Voy a saltear esta diapositiva. Hay otros aspectos de la IANA que están por detrás de todo lo que hacemos, que es la imparcialidad y la neutralidad. Estamos aquí para implementar las políticas escritas. Lo podemos hacer de un modo neutral. Esto es parte de lo que hacemos y de nuestros compromisos esta semana. Tenemos un foco muy central

en el desempeño. Hay muchos SLA en lo que hacemos. Estamos midiendo todo el tiempo lo que hacemos. Esto es clave. Queremos continuar mejorando. Esta es otra parte de nuestro trabajo y de nuestra mejora. Parte de esto es tener terceros externos. Tenemos rendición de cuentas ante la comunidad. Hay muchos comités de control dentro de la IANA que vamos a aprender en el espacio de la ICANN.

En resumen, la IANA mantiene registros de sistemas de números únicos. La Internet tiene que poder estar interoperando. La mayor parte de los registros son bastante directos, la gente va directamente a la IANA. Seguramente nunca escucharon hablar de eso. Son fáciles pero hay algunos muy complejos. Hablamos de la zona raíz, de la clave que protege la zona raíz. La IANA es como la raíz global para todos estos sistemas de nombre. Esta es la vista general de la IANA.

SIRANUSH VARDANYAN: Gracias. Esto ha sido muy informativo. Esta presentación de PowerPoint está subida a nuestro sitio web de la ICANN76 en esta sesión en particular. Si quieren descargarlo y utilizarlo, lo pueden hacerlo. Podemos ahora recibir unas cuentas preguntas más. Tenemos aún 30 minutos asignados para eso. No sean tímidos. Adelante. Veo aquí también a David.

FIRUZ AZIMOV: Hola. Soy Firuz. Soy becario de la ICANN. Tengo dos preguntas. La primera es sobre algo que mencionaron antes en cuanto al problema

de META. Recuerdo que también hubo un problema con META que había sido anunciado por otro ISP. Esto pasa incluso en nuestro país. Hemos tenido este problema de que nuestra subred asignada para el DNS fue anunciada por otro ISP y así perdimos Internet no solamente para esta subred sino también para todos nuestros usuarios. Mi pregunta es si se puede tener una solución para evitar este tipo de problema y si cada router tiene que tener una verificación RPKI y de qué modo podemos lograr que haya una estabilidad como usted dijo en las capas más bajas, por ejemplo en la capa tres.

JOHN CRAIN: Esta es otra discusión sobre cómo aseguramos el ruteo. En general esto se denomina un BGP hijacker. Le voy a pedir a David que nos hable de esto.

DAVID HUBERMAN: El RPKI ayuda en este tema en cierta medida. Lo que resulta interesante es que lo que usted acaba de describir ocurre todos los días en Internet y a veces múltiples veces por día. Nuestros amigos en la Sociedad de Internet han generado un observatorio para mirar estos eventos y están midiendo entre 500 y 1.000 de estos eventos cada año. Esto ocurre desde los años 90. No es nada nuevo. Parte de esto es malicioso. Parte es para generar cierto misterio y buena parte es accidental.

Durante muchos años, los ingenieros que armaron la Internet escribieron a mano configuraciones entre los ruteos y los humanos

generan errores. Si uno hace un error en un ruteador, puede ser muy malo. El RPKI está diseñado para ayudar con buena parte de esto, especialmente con este segundo escenario. Especialmente en los problemas humanos RPKI ayuda mucho.

RPKI no requiere que todos los ruteadores que tienen BGP validen los anuncios. Lo que ocurre es que solamente requiere que todas las grandes redes de tránsito en el mundo lo hagan porque cuando compartimos información de ruteo de un ministerio o de un ISP, de aquí de la reunión de la ICANN en Cancún hacia Facebook en California hacia algo en Venezuela, todos estos paquetes atraviesan unos 800 proveedores de Internet supervisados y si esos 800 proveedores validan, firman, todo lo que es inválido se cae y el tráfico no va a donde no tiene que ir.

Una de las historias de éxito de RPKI en los últimos años es que hay un 100% de adopción a estos 800 ISP en el mundo para que puedan validar los paquetes. Si uno opera una red o si regula una serie de redes, es muy importante que esas redes emitan los certificados, las autorizaciones para sus prefijos de ruteo, para que todo el mundo pueda validarlos. Para asegurar el canal, la comunicación, necesitamos no solamente el RPKI sino que también tenemos que poder validar la ruta, el camino que cuando llega a destino pueda volver también porque hay una serie de intermediarios. Ese camino tiene que estar validado todo el tiempo para que lo que llamamos el intermediario pueda tomar ese paquete y llevarlo cuando no lo autorizamos a hacerlo. El IETF, la comunidad de ingeniería, tiene algunas soluciones y seguimos trabajando para desarrollar mejores soluciones que todo el

mundo pueda implementar. Esa va a ser la próxima etapa de nuestra seguridad.

SIRANUSH VARDANYAN: Muchas gracias, David. Después Nicolás. Sé que tiene usted una pregunta sobre la IANA.

DANIEL MONDRAGÓN: Hola a todos. Soy Daniel, de Costa Rica. Soy ingeniero de redes. NIC Costa Rica se encarga de los TLD en Costa Rica. Tengo dos preguntas. La primera: ¿ICANN o la IANA están haciendo esfuerzos para obligar a políticas o a tecnologías para que se utilice el DNS TLS en lugar del DNS sobre HTTPS? Esto podría ser un problema. La segunda pregunta es qué opina ICANN acerca de esto desde la perspectiva del ruteo y de seguridad, etc.

JOHN CRAIN: La primera es fácil. No, porque no es competencia nuestra. Estudiamos estas cosas. Las medimos. Se habla mucho en otras áreas sobre el efecto de esto. Si uno hace investigaciones sobre los paquetes del DNS y quiere mirarlos, no se puede. Podemos hablar de si esto es bueno o malo. No tengo la respuesta. Yo hablo desde la perspectiva personal. Siempre existe una tensión entre la seguridad y la privacidad cuando se trata de estas tecnologías. Por lo tanto, no tenemos una postura oficial. Sí que hemos investigado un poco. Matt no ha dicho mucho. No sé si está despierto y nos quiere comentar algo.

MATT LARSON: Sí, sí. Estoy despierto. Hemos investigado un poco estas cuestiones. De hecho Paul Hoffman ha contribuido a estos esfuerzos en lo que se refiere a las normas. Hemos ayudado a desarrollar estas normas. Hay un interés creciente en la privacidad y creo que será inevitable que se utilicen más estos otros protocolos. Son más intensivos desde la perspectiva de la computación y de la red porque el DNS es un paquete para la petición y un paquete para la respuesta. Quizá esto pasa con otros paquetes pero cuando se añade la criptografía estamos hablando de interacciones muy complejas, con más paquetes. Los proveedores que responden a muchas peticiones, los operadores, no solo estamos hablando de un paquete sino que se tiene que establecer una conexión. Tiene que haber una validación de la criptografía y esto es muy intensivo y cuando hay una operación a gran escala, esto plantea muchas preguntas. Creo que es el rumbo general que estamos viendo y quizá se van a empezar a usar más estos protocolos.

SIRANUSH VARDANYAN: Pido disculpas. Creo que me he equivocado con su nombre. Nicolas tiene otra pregunta. Luego David nos va a dar otra presentación.

NICOLAS FIUMARELLI: Hola. Yo participé de manera virtual en la ceremonia de la KSK. Es una pregunta que tiene que ver con esto pero también con el DNSSEC. ¿Hay esfuerzos en curso dentro del IETF para incorporar la criptografía? Como se quieren incluir estos algoritmos nuevos, ¿qué anticipa el PTI a

la hora de implementar estos nuevos algoritmos dentro del DNSSEC y cómo van a afrontar estos problemas, estos desafíos con respecto a la seguridad del sistema?

KIM DAVIES: Muchas gracias por la pregunta. De momento la criptografía poscuántica, no estamos trabajando en ninguna iniciativa con respecto a esto pero sí que estamos preparando el terreno para cambiar el algoritmo criptográfico en la zona raíz. Ahora usamos un algoritmo que llevamos utilizando muchos años. No sabemos si esto va a ser fácil de cambiar o no. Hemos creado un equipo de diseño de la comunidad en las últimas semanas. Se van a reunir dentro de dos semanas para hablar largo y tendido sobre esto. El propósito de este equipo es averiguar cómo se cambia el algoritmo en la zona raíz, si es la criptografía poscuántica o quizá otro tipo de técnica. No sabemos cuáles van a ser los resultados. Estamos en una fase muy temprana. Aún no podemos hablar de la criptografía poscuántica. Sí que somos conscientes de ella pero en cuanto a la actividad que existe ahora, voy a pasarle la palabra a Matt para que hable de la investigación porque me parece una actividad que tiene que ver más con la investigación.

MATT LARSON: Muchas gracias. Esta es una oportunidad para hablar de la serie de documentos de OCTO que se ha mencionado anteriormente. Hemos escrito un documento sobre esto. No estoy en la sala de Zoom así que no puedo poner el enlace pero el documento se llama OCTO-031. La criptografía poscuántica recibe mucha atención y por eso OCTO

solicitó una investigación sobre esto. Están escribiendo un paper sobre esto, un artículo. Este artículo ya existe. Lo hemos cogido y hemos hecho un resumen para que fuera más fácil de entender. Allí se habla de los desafíos. Yo creo que aún estamos muy lejos de tener que preocuparnos por estos algoritmos poscuánticos porque aún no existe una computadora que pueda suponer una amenaza para los algoritmos de hoy en día.

Se habla mucho en la industria, en el sector, y si uno lee las publicaciones igual piensa que es inminente. El mundo se va a colapsar. Pero no es así. Aún quedan décadas. Esa es nuestra postura. Nos parece que es demasiado pronto como para estudiarlo. Aún tenemos muchísimo tiempo porque aún no hay computadoras cuánticas que puedan suponer una amenaza para la criptografía de hoy.

SIRANUSH VARDANYAN: Se ha puesto el enlace en el chat en Zoom. Pueden abrirlo y leer el documento en profundidad. Le voy a dar la palabra a David para que nos hable del proyecto KINDNS.

DAVID HUBERMAN: Muchas gracias. Voy a cambiar un poco el tema para el tiempo que nos queda. Estamos aquí para hablar de una cosa que estamos haciendo en la ICANN para mejorar la postura técnica de Internet. Ayer fui a cenar. Fui con un amigo y me lo pasé muy bien. Mientras nos traían la cena el mesero hizo algo que es el escenario de pesadilla para el

mesero. Se le cayó mi consumición, mi bebida y me empapó. Cuando pasa eso podemos reaccionar de dos o tres maneras. Podemos enfadarnos y decir: "¡Pero qué hace usted!" y montar un pollo, por así decirlo, pero eso es incómodo para todos. Nos podemos quedar ahí sin reaccionar o podemos adoptar un enfoque mejor. Podemos reírnos, sonreír y decir: "No pasa nada. Todo el mundo se equivoca". Podemos hacer algo bueno de una situación un poco mala. Eso es lo que hicimos. Estaba bien el mesero. Ahora somos amigos. Todo bien.

¿Por qué estoy hablando yo de esto? Podemos hacer lo mismo con respecto al DNS. Podemos ser amables. Podemos hacer que la vida sea mejor para todos tomando acciones de amabilidad para todos. Hemos creado un programa que se llama KINDNS. Es decir, amabilidad. Tenemos una página web: kindns.org. El propósito de esto es que todos los operadores del DNS, pequeños, grandes, Facebook, Google o un ISP nuevo en Macedonia, muy pequeño, que haya pasos que pueda tomar para ser más amables. Si todo el mundo es amable, el DNS puede ser fortalecido y tener una postura técnica mejor.

En este proyecto los operadores se clasifican. Pueden ser pequeños, con un servidor autoritativo, que responde a las consultas. Quizá es un operador resolutor. A través de este proyecto puede hacer una autoevaluación para saber cómo le va con respecto a una serie de normas que la comunidad de ICANN y del DNS acordaron. Es una serie de normas básicas que tienen que seguir todos y si todos siguen estas normas funcionaría mejor el DNS. Sería más seguro y más estable.

El operador puede comparar con estas normas, recibir el resultado y ver dónde están las brechas, dónde están las diferencias. Este esfuerzo

se basa en algo que hicieron nuestros amigos de la Sociedad de Internet. Ellos hablan de las buenas maneras y nosotros hablamos de la amabilidad. Estas iniciativas sirven para mejorar las cosas para todos. Son pasos pequeños que no cuestan dinero y tampoco cuestan mucho tiempo. Ayuda a los operadores a entender dónde está la red y cómo puede mejorar la infraestructura del DNS. Esto es la amabilidad y si tienen tiempo, por favor, miren la página web. Pueden ver allí en palabras muy sencillas algunas de estas normas aceptadas por la comunidad a las que seguimos. Eso es lo que quería compartir. Muchas gracias.

SIRANUSH VARDANYAN: Tenemos una pregunta de un participante remoto, de Mohamed Elnour Abdelhafez Fadul, de Sudán del Sur. “La validación de las rutas es importante para la seguridad del ruteo global. La extensión del BGPsec se introduce para resolver este problema pero no es fácil de implementar debido a la cantidad importante de recursos que consume el BGPsec. ¿Qué papel tiene ICANN a la hora de ponerlo en marcha?”

JOHN CRAIN: Hay dos roles que podemos desempeñar. Uno es la participación y otra es participar en la investigación. David, no sé si quiere usted hablar de esto.

DAVID HUBERMAN: Es una pregunta muy buena. Muchas gracias. Como decía, las dos rutas a una infraestructura segura son el RPKI y la validación de la ruta. Sabemos que implementar el BGPsec no es fácil. No romperíamos el Internet. Haríamos algo peor. Haríamos que fuera más lento. En ICANN nuestra participación en la investigación, en la búsqueda de soluciones es en cierto modo lo que hace el equipo de Matt y lo que hacen otros equipos con respecto a los procesos de desarrollo de los protocolos. Estoy hablando sobre todo del IETF. Cuando salen soluciones podemos medir el impacto de manera científica, formal, de manera empírica, a través de nuestras conversaciones con miembros de la comunidad. Además, podemos ser facilitadores para las conversaciones más centradas en la comunidad de ICANN para ver cuáles son los impulsores, cuáles son los motivos y cómo estas tecnologías pueden mejorar la situación sobre el terreno.

JOHN CRAIN: Muchas gracias. Me gustaría saber cuántas personas en esta sala han participado en el grupo de trabajo de ingeniería de Internet. Si trabajan en esto y les interesan los protocolos, es buen sitio. Si no son frikis de esto, quizá no es el mejor sitio. Para los que sí lo somos es buen sitio. Yo creo que les va a sorprender mucho pero ICANN no gestiona Internet. No desarrolla Internet. Es una asociación, una comunidad de ingenieros y de personas que utilizan Internet. Es bueno ver a las personas en el IETF. No sé si tenemos más preguntas.

SIRANUSH VARDANYAN: Quizá podemos oír una pregunta más. Afifa.

AFIFA ABBAS: Hola. Me llamo Afifa. Soy mentora de los becarios. Hace dos años que hago esto. Una pregunta que me suelen hacer los becarios es dónde en la ICANN en lo que se refiere a ciberseguridad, dónde pueden involucrarse los becarios. Como mentora me cuesta bastante contestar a esta pregunta. Si pueden citar alguna plataforma en la que puedan involucrarse, estaría bien. Como mentora, yo sé que hay muchas personas que llegan y que les interesa mucho la ciberseguridad. Queremos que llegue gente nueva y seguro que eso también es lo que quiere la ICANN. ¿Cómo podemos aprovechar este talento?

JOHN CRAIN: Muchas gracias, Afifa. Siempre es un placer ver a los becarios, sobre todo cuando se convierten en mentores. Es una pregunta muy interesante. La ICANN no es un foro de ciberseguridad. No es lo que hacemos. No obstante hay una vía de ciberseguridad. Esto sale en la agenda. Si quieren consejos acerca de cómo pueden involucrarse más en las cuestiones de ciberseguridad, dentro de ICANN hay un comité que se llama SSAC. Pueden solicitar la membresía. Quieren sobre todo profesionales de la seguridad con experiencia. Si entran como alguien así, con experiencia, es buen sitio para mirar.

Hay días técnicos. La ccNSO realiza días técnicos en los que se habla mucho de la seguridad y también pueden venir a nosotros y hablar con nosotros para que encontremos otro sitios para hablar de estos temas. En ICANN es importante no solo lo que pasa en las discusiones de políticas. Estamos hablando de las políticas de los identificadores. No

solo se trata de la seguridad y la ciberseguridad. Lo importante de aquí es interactuar, hablar con las personas en los pasillos. Si han visto a alguien al que quieran conocer que tenga que ver con la ciberseguridad o con otra área, no duden en hablar con su mentor o con un miembro del personal de ICANN o con cualquier persona de la comunidad y decirle: "Me interesa el tema X. He encontrado a alguien que entiende de esto. ¿Me lo pueden presentar?"

Se trata de trabajar de abajo arriba juntos y formar una comunidad. Este es el mejor consejo que les puedo dar. Hay una vía de seguridad. Miren también los días técnicos, el ccTLD. Hablen con las personas de SSAC, RSSAC. ¿Alguien de algún ccTLD aquí en la sala? Sí. ¿Trabaja con la seguridad? ¿Está en la lista de seguridad del ccTLD? La ccNSO también trabaja en esto. Pueden hablar con nosotros, con los demás. Hablaremos de este tema y a ver si podemos encontrar algo. Ha hablado de la ciberseguridad, que es un término que tiene muchas acepciones para diferentes personas. Creo que Samaneh quiere decir algo.

SAMANEH TAJALIZADEHKHOOB: Algo para agregar a lo que dijo John. Es una pregunta interesante porque a veces lo discutimos pero no de forma sistemática. Hicimos proyectos más grandes y más pequeños. No lo hablamos internamente pero, como equipo de investigación, tenemos proyectos y recibimos ideas externas u operaciones dentro de nuestro grupo hacia fuera. Si los mentoreados que ustedes tienen están interesados en los proyectos de investigación, pueden enviarlos a nosotros y podemos ver cómo podemos proceder en ese sentido.

SIRANUSH VARDANYAN: Gracias. Con esto quiero agradecerles a todos nuestros presentadores, Matt, Samaneh, David, John y Kim, por su tiempo. Sé que tienen un programa muy abultado. Gracias por haber venido a hablar aquí con los becarios, con los NextGenners. Todos ellos están interesados en aprender más y los participantes aquí ahora conocen estas caras. Cuando las vean en los pasillos y quieran hacerles preguntas, siéntanse en libertad de contactarlos y formulárselas. Para concluir esta sesión quiero decirles que sean amables unos con otros. Muchas gracias. Termina aquí esta sesión. Podemos terminar la grabación. Muchas gracias.

ORADOR DESCONOCIDO: Vamos a estar aquí unos minutos más. Si quieren venir a hablar con nosotros, vamos a estar aquí. Pueden venir a buscarnos. A los NextGenners y a los fellows les pido que no se vayan de esta sala porque tenemos que hablar. Gracias. Por favor, tengan en cuenta que tenemos un ensayo en esta sala a las 12:30. Tienen que irse.

ORADOR DESCONOCIDO: A los NextGenners y a los becarios les pedimos por favor que vengan aquí, de este lado.

[FIN DE LA TRANSCRIPCIÓN]