MARRAKECH – Sesión de desarrollo de capacidades de At-Large: temas actuales sobre ciberseguridad
Miércoles, 26 de junio de 2019 – 12:15 a 13:15 WET
ICANN65 | Marrakech, Marruecos

JOANNA KULESZA: Hola a todos. Buenas tardes. Gracias nuevamente por participar. Mi nombre es Joanna Kulesza. Soy miembro individual de EURALO y también participo en ALAC. También soy copresidenta del grupo de trabajo de At-Large de creación de capacidades junto con Alfredo Calderón quien, desafortunadamente, no pudo asistir a la reunión de Marrakech.

Quiero darles la bienvenida a los miembros de At-Large pero también a los miembros de otras comunidades y unidades constitutivas. Nosotros consideramos este taller como parte de un esfuerzo colaborativo con el GAC en materia de creación de capacidades. Espero que haya también algunos miembros del GAC que puedan participar en esta sesión del día de hoy. Por supuesto, también les doy la bienvenida a todos los demás miembros del resto de las unidades constitutivas que estén presentes.

El tema de nuestra presentación el día de hoy es un tema muy actual que es la ciberseguridad. Como mencioné anteriormente, durante la sesión del GAC, At-Large está dando prioridad a temas

de privacidad y seguridad que tienen que ver con los aspectos que se tratan dentro del EPDP en materia de seguridad y privacidad. Aquí la idea es poder tener un mayor entendimiento de los temas actuales de seguridad o ciberseguridad y privacidad. Para eso se llevó a cabo una serie de seminarios web para los participantes de la conferencia ATLAS III que se va a llevar a cabo en Montreal a finales de año.

Como mencioné anteriormente, se llevó a cabo una serie de cinco seminarios que brindaron información multilingüe a los posibles participantes del ATLAS III pero también los seminarios web eran abiertos a todas aquellas personas que desearan participar y siguen estando disponibles en línea. Uno de los seminarios web que provocó cierto interés en particular y que también llamó la atención de la comunidad fue uno muy similar al que Patrick nos va a brindar hoy que abordó temas actuales en materia de ciberseguridad. Nosotros agradecemos el aporte de Patrick porque aborda tanto los aspectos técnicos como los de política.

Nuestro invitado del día de hoy es Patrick Jones, quien forma parte del Equipo de Participación Global de Partes interesadas de la ICANN. A mí me gusta el ángulo que toma Patrick porque tiene un ángulo más bien técnico y ha participado con los diferentes grupos como los gobiernos y la sociedad civil y partes interesadas. Con gusto ahora, Patrick, le doy la palabra para que

haga su presentación. Le agradezco por su tiempo y también por brindarnos este seminario web. Todos los materiales van a estar disponibles. Ya se encuentran disponibles en realidad en la wiki de la ICANN. Nosotros vamos a publicar también los enlaces en Twitter y en Facebook para que estén disponibles. También están disponibles en la agenda. Contamos con una hora para esta sesión. Él va a darnos suficiente tiempo para hacer preguntas. Nuestro objetivo es ese. Tengan en cuenta que esta es una sesión de creación de capacidades. Lo que queremos es que se lleven la mejor comprensión posible de este tipo de cuestiones y que esto sea una especie de punto de partida para comenzar a pensar en nuestras cuestiones de ciberseguridad. Veo que todo el mundo ya ha tomado su almuerzo. Con esto le voy a dar la palabra a Patrick Jones. Le agradezco nuevamente por su participación y le cedo la palabra.

PATRICK JONES: Muchas gracias, Joanna. Gracias por darme la oportunidad de participar en At-Large y en la comunidad en general. Esto es más bien una especie de actualización con respecto al seminario web que David dio hace unos meses. Aquí lo que incluimos es nueva información. Como ustedes saben, siempre hay alguna amenaza dando vueltas. Siempre hay algún ataque. Aquí van a ver algunos de los últimos ataques en materia de actualización respecto de estos ataques. Hubo un simposio del DNS en Bangkok y también

hay otros anuncios que vamos a poder ver y cuestiones que se publicaron en Twitter en las últimas semanas. Siguiente diapositiva, por favor.

Les cuento un poco sobre mi persona. Yo soy parte del equipo de participación de partes interesadas global pero ya hace unos 13 años que participo en la ICANN. Tuve diferentes puestos. También participé del equipo de seguridad de la ICANN. También hago algunas capacitaciones en materia del DNS. En las últimas semanas estuve en Rumanía, Letonia y Lituania. También en Polonia. Trabajamos con la oficina del CTO presentándoles algunos ejemplos.

Lamentablemente, las imágenes son un poco más grandes que la pantalla. Como ustedes pueden ver, todas las semanas recibimos algunas noticias sobre ataques que se están llevando a cabo. En este caso en particular, esto fue del 2017 sobre un botnet donde había un algoritmo que generaba nombres de dominio que afectó a todo el mundo. En ese entonces fue el ataque de DDoS más importante que afectó a las plataformas. Fue creado en 2016 por tres estudiantes universitarios y el propósito de este botnet era atacar a los servidores. En realidad fue una serie de ataques asociados con este botnet. Tuvieron un efecto colateral en los sistemas de la nube que tenían cientos de dominios en todo el mundo. Hay una estadística de marzo de 2019 que indica que el tiempo de inactividad de este ataque

costó aproximadamente unos 20 millones de dólares por hora. Pueden pensar con esto la importancia que tiene en este tipo de ataques para los usuarios en todo el mundo.

Esto se llevó a cabo esta semana mientras estábamos en Marrakech. Quizá hayan escuchado al respecto. La NASA fue hackeada. Alguien lo hizo utilizando una computadora Raspberry Partes interesadas. Afectó sus redes. Esto sucede con mucha frecuencia, todo el tiempo. Esto está dentro de un contexto de la ICANN pero simplemente es un ejemplo para que ustedes sepan cuál es el impacto que estas cuestiones tienen para los investigadores, para las universidades y para los gobiernos.

En la siguiente diapositiva vemos otro ejemplo de febrero de este año que describe una serie de ataques relacionados con el DNS que afectó a una serie de registros y proveedores de hosting. Incluso algunas otras plataformas fueron afectadas. Estas organizaciones hablaron con mucha franqueza con respecto a este ataque que tuvieron en el simposio del DNS que se llevó a cabo en Tailandia. El Centro de Protección de Marcas Comerciales también explicó lo que hizo para protegerse y recuperarse.

En la siguiente diapositiva vemos otro título que menciona la ICANN. Ustedes seguramente ya habrán leído este anuncio que

se hizo en febrero que proviene del equipo del CTO de la ICANN donde se hace una advertencia con respecto a las diferentes amenazas. Aquí se advierte a la comunidad global de Internet sobre estos ataques al DNS.

Este es otro ejemplo muy reciente. Mientras yo me encontraba en Europa, ICANN publicó este tweet con un post donde se nos pedía estar atentos a ciertas situaciones de suplantación de identidad o phishing. La ICANN hizo este anuncio con enlaces como este donde se quería llamar la atención de la comunidad para informarles de que este tipo de cuestiones sí suceden.

Esto es importante porque tenemos que tener en cuenta cuánta confianza uno pone en Internet. Hay entre 30.000 y 40.000 millones de dispositivos conectados a Internet. Todos ellos intercambian información, datos entre sí. Todos estos son objetivos muy atractivos para los ataques.

En la próxima diapositiva podemos ver un mensaje muy clave a tener en cuenta y es que cada vez hay más datos que se intercambian entre las máquinas y los dispositivos y esto es atractivo para los ataques. El SSAC publicó su documento SAC105. Existe un tutorial donde se describe la relación de Internet de las Cosas y el DNS. Si no han leído el documento, los invito a que lo hagan. También va a haber una sesión en esta reunión para la comunidad donde se explicará este documento y

los miembros del SSAC van a brindar una actualización a la comunidad. Sé que ellos a menudo vienen a hablar con ustedes y probablemente les puedan hacer más preguntas sobre ese documento.

Cuando nosotros hablamos de los elementos comunes que existen en una red de una empresa o una red gubernamental o de una universidad, todos ellos tienen este tipo de elementos. Cada organización tiene un correo electrónico, tienen calendarios, tienen contactos. Todos estos se almacenan en servidores de bases de datos donde también hay información de los empleados, de los clientes. Es decir, esto incluye por ejemplo información impositiva, información sustantiva o importante para la organización con respecto a sus clientes. También tienen información financiera donde también guardan secretos comerciales o secretos que tienen que ver con los procedimientos comerciales que realizan. Cuando estos elementos se ponen en peligro, tenemos que ver cuáles son los elementos que socavan estas cuestiones. Tenemos la gestión de la entidad, cuestiones de retención de datos, el almacenamiento de datos, política de seguridad, la forma en que se guardan estos documentos. Confían en el DNS como organización y todos los días estos elementos y sistemas son sometidos a ataques o son objetivos de ataques. Los atacantes o hackers lo que quieren

hacer es atacar esta información, vulnerar estos sistemas para obtener información.

Dentro del contexto de la ICANN, les voy a dar algunas definiciones para que sepan qué significa cada uno de los términos. Cuando hablamos de phishing o suplantación de identidad hablamos de una práctica fraudulenta que consiste en enviar correos electrónicos que parecen provenir de una empresa u organización con reputación para inducir a cierto individuo a revelar información personal, ya sea una contraseña, información sobre tarjeta de crédito, ciertos números y demás información.

El malware es un software que se diseña específicamente para dañar ciertas redes o para obtener acceso no autorizado a un sistema informático. Seguramente estén familiarizados con algunas noticias que aparecieron últimamente en relación a ataques a los hospitales. Por ejemplo, el ataque de Florida en los Estados Unidos donde hubo un ransomware que se esparció. También hay otras organizaciones que tienen que tomar la decisión de tener que pagar esta especie de rescate para poder obtener nuevamente la información que fue suprimida.

También tenemos los botnets. Estos son un conjunto o una red de computadoras privadas que son infectadas con software malicioso y son controladas por un grupo sin que lo sepan los

propietarios. Esto también puede ser a través de una plataforma donde intervengan varios actores.

Dentro de la ICANN se debate mucho a qué se llama uso indebido del DNS. No hay una definición globalmente aceptada de este concepto. Se debate dentro del grupo de trabajo del GAC y en otros ámbitos de la ICANN. Esto incluye cuestiones que tienen que ver con el ciberdelito, conducta maliciosa, hackeo. Son en realidad las amenazas al DNS las que generalmente están dentro de categorías como por ejemplo corrupción de datos, denegación de servicio y violaciones a la privacidad. Estos atacantes lo que tratan de hacer es atacar al sistema para obtener información.

Algunos otros detalles. Obviamente el CTO habla con mucha frecuencia al respecto y hace una diferencia entre el uso indebido del DNS, en este caso nos referimos a los ataques o usos indebidos de la infraestructura del DNS, en contraste con el mal uso del DNS que se refiere a explotar los protocolos de DNS o nombres de dominio o procesos de registración con un fin malicioso.

Esta diapositiva la tomé de una presentación que se hizo la semana pasada. Lo hizo nuestro coordinador de enlace ante el SSAC. Merike Kaeo trató de hacer una diferenciación entre los diferentes tipos de uso indebido del DNS que existen. Hay

ataques que se dan en los protocolos o en los servidores, como se ve aquí. También pueden encontrar esta presentación, esta diapositiva en la sesión de At-Large. No quiero dedicar mucho tiempo a describir este cuadro pero aquí básicamente se describen los diferentes tipos de ataques.

¿Cuál es el rol de la ICANN en todo esto? A veces el rol resulta bastante limitado porque somos un punto de conexión entre las diferentes organizaciones y comunidades. Cuando este tipo de ataques ocurren generalmente involucran a gobiernos o empresas multinacionales, agencias de cumplimiento de la ley internacional. Esta mañana, por ejemplo, debatimos con el grupo de trabajo de seguridad pública del GAC y los miembros del SSAC y algunos otros miembros de la comunidad este tipo de cuestiones, si hay un rol que tenga que tener la comunidad o la organización de la ICANN durante este tipo de ataques y después de los mismos.

En la reunión de ICANN que se realizó en Kobe, los miembros del SSAC hicieron una presentación sobre el secuestro o hijacking de la registración de nombres de dominio. Esto es información que tomé de la presentación del SSAC. Alguna se repite. En los ataques que se llevaron a cabo y que todavía están en curso, tenemos el DNS Espionage y Sea Turtle. La investigación en curso, como ustedes saben, se está llevando a cabo pero atribuir los ataques es difícil. Determinar quién está detrás de estos

ataques resulta dificultoso. Hay otras organizaciones que también están tratando de identificar los actores que originaron el ataque. No podemos decir que haya sido uno u otro pero básicamente estos son algunos ejemplos. Por ejemplo, preposicionamiento de ciberdefensa o ciberofensa militar. Esto implica reunir la inteligencia necesaria para lanzar un ataque militar a nivel cibernético. Esto afectó a 40 organizaciones. También a aerolíneas en países ubicados en América del Norte y Oriente Medio. Este es un ejemplo claro de los ataques que se están llevando a cabo.

Este ataque afecta a los registradores, a los proveedores de servicios de Internet. Ya mencioné algunas de las organizaciones que fueron impactadas. Creo que también hubo algún ccTLD que sufrió el efecto. No sé si Armenia. Esto nos da una idea de dónde sucedieron geográficamente estos ataques. Aquí las partes afectadas o involucradas tuvieron la posibilidad de modificar los registros al momento de la registración. Hubo credenciales de logueo. También los atacantes cambiaron los nombres de los servidores e hicieron que apuntaran a los servidores de los atacantes. Una vez que las zonas fueron redireccionadas a los servidores personales, pudieron extraer toda la información.

Esta información también se planteó en la reunión de Kobe. Este ataque fue identificado por el equipo de seguridad de Cisco Talos. Era una campaña continua que apuntaba a ciertos

dominios de Líbano, de los Emiratos Árabes y a ciertas organizaciones. También se hizo un informe en enero de 2019. Otro que se emitió en febrero. También se llevaron a cabo algunas sesiones en la reunión de Kobe en las cuales el SSAC habló al respecto. Siguiente diapositiva.

Vamos a hablar un poco sobre el rol de la ICANN antes y después. En nuestros estatutos se enfatiza esta cuestión de que la misión de la ICANN es mantener o garantizar una operación estable y segura de los sistemas de identificadores únicos de Internet. La oficina del CTO hay un entrenamiento continuo al respecto no solo entre sí sino también con las comunidades que pueden ser impactadas.

Esto ya ha sido aprobado por la junta directiva. La seguridad es un punto importante. Es el primer objetivo para los próximos cinco años. Fortalecer la seguridad del sistema de nombres de dominio y también del sistema de servidores raíz y evolucionar el sistema de identificadores únicos en colaboración con las partes pertinentes.

En nuestras reuniones, aquí hay una serie de grupos que se encuentran trabajando en materia de seguridad y estabilidad. Yo mencioné el grupo de trabajo sobre seguridad pública del GAC. En este caso, este grupo se focaliza en los aspectos de políticas y procedimientos de la ICANN que están relacionados con la

mitigación del uso indebido del DNS y el ciberdelito. También tenemos el comité asesor de seguridad y estabilidad que también trabaja en cuestiones que tienen que ver con la evaluación de las amenazas y el análisis de riesgos. Asesoran a la junta directiva de la ICANN pero también a la comunidad en general. También tenemos el Comité Asesor del Sistema de Servidores Raíz que brinda asesoramiento a la junta directiva de la ICANN y a la comunidad sobre cuestiones relacionadas con la operación o administración del sistema de servidores raíz. Hay un comentario público abierto sobre la evaluación del sistema de identificadores únicos.

Siguiente diapositiva. Esto nos ayuda a poner en contexto lo siguiente. Existen varias relaciones entre las partes de la ICANN. Tenemos un acuerdo entre la ICANN y los operadores de registro de nombres de dominio genéricos. Ellos también tienen acuerdos entre sí y los registradores, a quienes les ofrecen los dominios que administran. La ICANN tiene un acuerdo de acreditación de registradores con todos los registradores acreditados. Estos registradores pueden tener revendedores y a su vez tienen acuerdos entre ellos.

Los registradores y los revendedores pueden, a su vez, y de hecho lo hacen, tener un acuerdo entre sí y de los registratarios. La ICANN no tiene una relación contractual directa con los registratarios que registran los nombres pero esto muestra de

alguna manera la conexión que tienen las diferentes partes interesadas.

En nuestros contratos, hay ciertas herramientas de importancia que están relacionadas con la seguridad y la estabilidad. El acuerdo de acreditación de registradores impone la obligación de investigar el uso indebido. La última actualización del acuerdo de acreditación tiene disposiciones similares, lo cual incluye que los operadores de registros prohíban a los titulares de nombres de dominio distribuir malware o llevar a cabo actividades de phishing, hacer piratería, infringir derechos de propuesta de marca, contrabando y otro tipo de actividades que podrían infringir la ley.

La ICANN también cuenta con la entidad de la PTI que es responsable de los aspectos operativos, asigna recursos a los registros regionales de Internet. También mantiene la zona raíz y administra las extensiones de seguridad del DNS. No voy a dedicar mucho tiempo a esta diapositiva pero espero que puedan comprender que cuando se desarrolló el DNS, cuando los ingenieros lo crearon, la seguridad no estaba incorporada dentro de los protocolos y las DNSSEC, las extensiones de seguridad del sistema de nombres de dominio, se desarrollaron después de haber realizado cierta investigación en la cual se detectó que los dominios y los titulares o usuarios de los nombres de dominio podrían ser direccionados erróneamente.

Esto permite que la información que se dé cuando uno accede a una página sea la página real a la cual se quiere acceder. Permite a los registratarios firmar sus datos dentro del DNS y también les permite a los operadores del DNS validar todos los datos de su organización. Si un buscador está habilitado para DNSSEC van a ver que aparece un símbolo verde que les permite confirmar esta información.

Cuando hay un incidente de ciberseguridad, es importante comprender que la ICANN tiene un equipo que es básicamente el punto primario de contacto para muchas organizaciones y que coordina las respuestas que se brindan a estas organizaciones. Este grupo tiene ya una larga trayectoria en coordinar con diferentes partes y actores, y también trabaja con las diferentes comunidades. Comparten su experiencia y su conocimiento para poder abordar estos ataques.

Cuando sucede un ciberataque, esto requiere acciones o respuestas coordinadas. La ICANN cuenta con equipos de respuesta a incidentes. Son equipos de respuesta de emergencia y también cuenta con otros profesionales de seguridad que comparten información. También están las listas de TLD que se iniciaron entre los operadores de TLD y que se ponen en marcha cuando ocurre un ataque.

La organización de la ICANN, el personal y la comunidad a menudo realizan esfuerzos conjuntos para explicar a las organizaciones estas cuestiones que impactan al DNS y a los identificadores únicos y lo hacen a través de seminarios web, de sesiones de trabajo en las reuniones de la ICANN. Se organizan, por ejemplo, seminarios técnicos como el simposio del DNS. En este caso vemos un ejemplo. Se llevó a cabo a comienzos de año en esta región. Es un esfuerzo para compartir información y mejores prácticas, para concientizar sobre el tema y también para brindar información a las regiones. En este ejemplo en particular, algunos miembros de nuestro equipo están trabajando muy de cerca con un grupo de Pakistán en un taller que se hizo de creación de capacidades para informar sobre el uso indebido del DNS. Estas sesiones generalmente son abiertas. Se llevaron a cabo dos y esto incluye también a miembros de la comunidad académica, los equipos CERT, agencias de cumplimiento de la ley, administradores de ccTLD, entre otros. También brindamos estas capacitaciones en forma de seminarios web.

Generalmente nosotros llevamos a cabo capacitación en materia de DNSSEC en las regiones. Esto es para concientizar sobre los temas de seguridad pero también lo llevamos a un nivel que pueda comprenderse, que lo puedan comprender los reguladores y quienes toman decisiones. A veces tenemos

diferentes programas de capacitación como capacitar a los capacitadores, donde se brinda información. ICANN no puede llegar a todas partes. Este tipo de capacitación es útil para entrenar a aquellas personas que después van a diseminar la información. La idea es llevar el mensaje a otras partes y crear confianza en relación al sistema de nombres de dominio. La idea también es apoyar la implementación local por parte de los administradores de TLD y también que se adhieran a las buenas prácticas.

Hubo un taller que se llevó a cabo hace dos días. Hubo unos 1.300 TLD que firmaron las DNSSEC. Un 50% de los ccTLD están firmando las DNSSEC. Es difícil trazar una línea entre la capacitación que se brinda y lo que finalmente se hace en práctica con los operadores de TLD pero, recientemente, una serie de TLD están activando las DNSSEC en los últimos tres meses. Vemos lo siguiente. Después de haber hecho el taller vemos que la gente sí termina implementando las DNSSEC. Aquí vemos algunos ejemplos. Hubo un ccTLD, un administrador de ccTLD que asistió al taller y una vez que volvió a su organización, implementó o activó las DNSSEC y después formó parte de una delegación en Pakistán donde también contribuyó a la implementación de las DNSSEC. Se entrena a las personas.

En la siguiente diapositiva vemos que dentro del año fiscal 2019 llegamos a una serie de lugares. Para que ustedes sepan hicimos

una serie de capacitaciones a nivel de la comunidad local para que pudieran tener una mejor comprensión del ecosistema de Internet y los usos indebidos. También abordamos cuestiones que tienen que ver con los nombres de dominio genéricos, los nombres de dominio internacionalizados, la aceptación universal y estamos trabajando también en temas actuales como los nombres de dominio con emoji y algunas otras cuestiones que tienen que ver con los ataques al DNS. Esto incluye algunas capacitaciones que hemos hecho en las organizaciones de TLD regionales, también en reuniones de los RIR, etc.

Es difícil demostrar el impacto que tienen estas capacitaciones pero, con el tiempo, podemos ver que es una forma de hacer difusión externa directa. Si nos retrotraemos 10 años, teníamos poca colaboración de la comunidad. Había algunos botnets como por ejemplo Avalanche que afectaron. Hay registros que actualmente utilizan solicitudes de seguridad de registro expeditivas. La ICANN tiene un proceso de divulgación de vulnerabilidades que está coordinado. Hubo un miembro, de hecho, de la comunidad de la ICANN que identificó una vulnerabilidad en el sistema de Adobe Connect. Básicamente, este es un claro ejemplo de una persona que puede identificar una vulnerabilidad y presentar un informe y de este modo la ICANN o alguna parte de la organización puede trabajar directamente con la organización afectada para poder

determinar cuál es el problema. Por lo tanto, esto implica también una colaboración y una coordinación con las agencias de cumplimiento de la ley y grupos de seguridad pública.

Después de que hay un incidente, los representantes de la ICANN y también los miembros de la comunidad lo que hacen es presentarse en diferentes eventos como por ejemplo el simposio que se llevó a cabo en Tailandia. También hay otro grupo en el cual participa la ICANN que se denomina Centro de Investigación y Análisis de Operaciones de DNS. También participa de los grupos de operadores de redes. La idea es que las organizaciones utilicen esta información que se brinda para hacer actualizaciones de política en sus contratos o quizá redireccionar los protocolos.

En la siguiente diapositiva vemos lo siguiente. Tenemos que tener en cuenta que el DNS ya no es solamente una función técnica sino que constituye una parte clave de la infraestructura de las organizaciones. Es importante también que presten atención a todos sus sistemas, infraestructura de DNS, datos y redes porque pueden ser atacados. La última diapositiva contiene algunas recomendaciones que publicó la ICANN en febrero de este año. Ahora sí les doy la palabra.

JOANNA KULESZA: Muchas gracias, Patrick. Su presentación ha sido muy útil. Se combinan los temas técnicos y también de la comunidad. Vamos a usar esta presentación para la creación de capacidades. Voy a pedir que alguien sea voluntario para poder realizar comentarios al documento que está publicado para comentarios públicos. También quiero felicitar al equipo de GSE porque ha sido maravilloso al brindar esta información. Patrick pertenece a este equipo. Si ustedes requieren esta información en su región, estoy segura de que la van a poder brindar. También quiero agradecerles. Sé que la junta está trabajando mucho al respecto. Si tienen algún comentario, con gusto se lo puedo dar. Quizá tenga algún comentario para relacionarlo con lo que está haciendo la junta directiva. Adelante, León.

LEÓN SÁNCHEZ: Gracias, Joanna. Voy a ser breve en mi comentario para dar lugar a las preguntas que quizá tenga la audiencia. Sí. Tiene razón. Esta es una de las prioridades de la junta directiva. La misión de la ICANN, por supuesto, consiste en garantizar una Internet que funcione, que sea estable y segura. Esto también está contenido dentro de nuestro plan estratégico a cinco años. Constituye uno de nuestros cinco objetivos estratégicos que se van a incluir también en el plan operativo que va a ser diseñado por el personal a fin de poder implementarlo. Sí, tenemos este principio de seguridad que consiste en garantizar el

funcionamiento estable y seguro de Internet. Esta es una de las prioridades más importantes de la junta directiva en relación a la misión de la ICANN.

JOANNA KULESZA: Entiendo que Patrick también lo apoya en esta tarea. Muchas gracias. Tengo una breve lista. Hadia y Holly, creo que es en ese orden. No sé si es correcto. También me pregunto si hay alguna otra pregunta de la participación remota. Judith también. ¿Me salté a alguien? Eduardo. ¿Quién más? Holly, Hadia y Javier. Me pregunto si hay alguien en la sala que no sea miembro de ALAC o líder de At-Large que quiera tomar la palabra o quiera hacer alguna pregunta. Si es así, piensen la pregunta que quieran hacer. Vamos a colocar un cronómetro de dos minutos. Le voy a dar primero la palabra a Hadia y luego vamos a seguir.

HADIA ELMINIAWI: Gracias. En primer lugar quiero felicitarlo por los esfuerzos que están haciendo y por los talleres tan buenos que ofrecen. Mi pregunta tiene que ver con lo siguiente. Considerando que tenemos acuerdos internacionales como por ejemplo la convención de Budapest en materia de ciberdelito, ¿la ICANN tiene algún tipo de obligación de trabajar con estas organizaciones para combatir el ciberdelito? No después de que

ocurra un incidente sino más bien colaborar o trabajar con estas entidades que combaten el ciberdelito.

PATRICK JONES: Sé que sí se colabora cuando se pide colaboración. Trabajamos muy de cerca con diferentes instituciones y gobiernos cuando suceden este tipo de ataques. Está contenido en nuestros estatutos, como mencioné, pero también nuestras partes contratadas están sujetas a diferentes jurisdicciones. Se nos pide que colaboremos. No somos signatarios de ningún tratado ni ninguna legislación pero sí colaboramos. Espero que eso responda a su pregunta.

HADIA ELMINIAWI: Imagino que también colaboran en cuanto a los datos o a la información.

JOANNA KULESZA: Sé que hay más preguntas. Vamos a dejar aquí esa pregunta. Holly, adelante, por favor.

HOLLY RAICHE: En realidad quiero hacer un comentario específicamente porque se debate mucho sobre esta cuestión del acceso a los datos. Lo que escucho es que esto no solamente incluye a las agencias de

cumplimiento de la ley. A mí me gustaría saber quién más accede a esos datos. Seguramente lo podamos hablar en otro momento.

En la presentación que se hizo en la última reunión de la ICANN se plantearon dos amenazas. La primera es que existen algunas vulnerabilidades del sistema de seguridad y algunas cuestiones que fueron implementadas por las corporaciones. Parece que hay mucha seguridad porque hay ciertos paquetes que no cumplen con las medidas de seguridad. Otro presentador en Kobe señaló que se está utilizando el DoH o DoT. Hay varios resolutores, no los recuerdo bien, que lo utilizan. Si se comienza a contratar este tipo de resolutores, en realidad lo que se está creando es un grupo objetivo.

PATRICK JONES: No sé si lo dije antes pero seguramente van a escuchar que el SSAC tiene un grupo que se encarga de abordar cuestiones que tienen que ver con DoH o DoT. Seguramente ellos van a brindar más información sobre cuáles son estas tecnologías pero depende después de cada uno de los grupos, de las comunidades seguir abordando la materia. Desde el punto de vista de la comunidad se brindará información fáctica que les puede servir para guiarlos en este sentido.

JOANNA KULESZA: Gracias. Tengo a Judith y a Javier. No sé si es correcto este orden. Primero las damas.

JUDITH HELLERSTEIN: Gracias por esta presentación tan informativa. Tengo dos preguntas. En este esfuerzo de que se implementen las DNSSEC y que lo hagan varios grupos, quizá la ICANN esté colaborando y pueda trabajar en algunas campañas de creación de conciencia sobre la implementación de las DNSSEC y quizá podamos tener versiones no tan caras aunque sigan siendo seguras, versiones del DNSSEC que no sean tan caras y seguras, para que esto pueda ser aplicado por organizaciones más pequeñas.

En segundo lugar, quizá tener una campaña de concientización para proteger el sistema y, por qué no, trabajar con los directores ejecutivos y quienes implementan políticas para que no envíen enlaces en sus correos electrónicos, por ejemplo.

PATRICK JONES: Como mencionó León, y yo lo mencioné en la presentación, la seguridad es una parte fundamental del plan estratégico y se van a realizar actividades para crear conciencia sobre la implementación de las DNSSEC. Por eso les digo que estén atentos a este espacio que se va a crear.

JUDITH HELLERSTEIN: León, quizá pueda comentar algo. Nosotros tuvimos un programa sobre el DNS y la encriptación donde se trabajó y se habló de implementarla sin que esto sea tan costoso.

LEÓN SÁNCHEZ: ¿Se refiere a la implementación del DNSSEC? Esto es parte del plan estratégico y de seguridad. Yo no soy la persona técnica calificada para hablar al respecto pero seguramente mis colegas en el equipo puedan hablar al respecto. Por supuesto, habrá un coordinador de enlace que va a estar trabajando con el personal para determinar la mejor manera de tener una implementación más amplia de las DNSSEC de manera costoefectiva.

PATRICK JONES: También hay otro esfuerzo que no está relacionad con la ICANN que se llama CRYPTTECH. Es un esfuerzo por crear un hardware para implementar esto, que no sea tan costoso. Esto puede ser bastante costoso pero este sería uno de los esfuerzos que se están llevando a cabo para que el proceso sea más costoefectivo.

JOANNA KULESZA: Gracias. Eduardo.

EDUARDO DÍAZ: Esta es una pregunta que tengo por curiosidad. ¿La ICANN sufrió algún otro tipo de ataque, más allá de lo que conocemos del Adobe?

PATRICK JONES: Bueno, no voy a hablar en representación del equipo de ingeniería pero sí sé que saben de algunas otras cuestiones que sucedieron en el pasado.

JOANNA KULESZA: Estas son otras cuestiones que podemos hablar entre nosotros después pero gracias por mencionarlo. Javier, adelante, por favor.

JAVIER RUA JOVET: Gracias, Patrick. Es una gran presentación. Tengo una pregunta. ¿Podría contarnos un poco o hablar sobre cómo una organización gubernamental internacional o un gobierno puede pedirle a la ICANN ayuda? Le tiene que mandar una carta a Göran o cómo sería. Cuáles serían los pasos para contactarnos, para abordar algo que esté dentro de nuestro mandato.

PATRICK JONES: Yo mencioné que la ICANN es parte de un equipo de respuesta a emergencias de seguridad. También hay otros miembros que

son parte de otros equipos. Es allí donde surgen las solicitudes o donde se presentan los pedidos. Hay parte del personal que pertenece a la oficina del director de tecnologías. Allí se comparte información con las diferentes organizaciones, agencias de cumplimiento de la ley y gobiernos. Básicamente, ese sería el canal de comunicación. Quizá Göran pueda recibir alguna carta pero esto va a ser publicado en la página de correspondencia y en realidad las solicitudes se hacen a nivel de la oficina del CTO.

JOANNA KULESZA: ¿Tenemos alguna otra pregunta? Tengo una pregunta en general. Quisiera que la podamos resumir. No sé si habrá más preguntas luego. Usted mencionó que el DNS ya no es más una cuestión técnica. Yo lo entiendo también así. La cuestión de seguridad va más allá de la perspectiva técnica. Lo hemos escuchado en la ICANN durante mucho tiempo. Hay otros temas que tienen que ver con la sociedad. Tenemos miembros del GAC aquí en la sala que también están interesados en el contenido. Hay un debate de ciberseguridad que parece ir mucho más allá de la valla técnica que mencionaba oportunamente la ICANN. Mi pregunta es específicamente dónde trazamos esta línea. Dónde termina la responsabilidad de la ICANN y dónde comienza la responsabilidad en materia de contenido. Cómo podemos delinear esa barrera.

PATRICK JONES: Por eso yo mencioné las relaciones contractuales. Esto es clave. Algunas cuestiones no están directamente relacionadas con el trabajo y rol de la ICANN pero sí tienen un impacto significativo sobre algún registro o registrador en particular y, por lo tanto, es necesario identificar dónde sucede esto. A veces esto se debate dentro de la GNSO. El GAC también puede tener cierto interés al respecto pero allí es donde deben llevarse a cabo los debates. Lo importante a entender es que este tipo de ataques están sucediendo. Cada vez son más significativos. Todo el mundo confía en sus teléfonos para conectarse y resulta un problema. La pregunta es: ¿Se hacen actualizaciones de las máquinas? Hay que hacerlo, hay que asegurarse de que las contraseñas se actualicen. Uno tiene que comenzar con la protección propia. Esos son los temas que se debaten.

JOANNA KULESZA: Tenemos pautas muy prácticas para los usuarios. No voy a entrar en detalle en este debate. Todavía tenemos algunos minutos disponibles. Hadia, ¿quiere agregar algo?

HADIA ELMINIAWI: No, no. No quiero agregar nada más.

JOANNA KULESZA: Perdón. Había un comentario. Disculpen. Evin, adelante.

EVIN ERDOĞDU: Evin Erdoğdu, del personal. Hablo en nombre de Remmy Nweke que tiene una pregunta. “Hola. Quisiera saber si la ICANN tiene un plan de apoyo específico para que las ALS promuevan el DNS para las mujeres en África”.

PATRICK JONES: Nuestro equipo de participación en África ha trabajado para tener una estrategia regional y creo que la seguridad es uno de esos pilares. Los invito a que dialoguen con los miembros del equipo de participación en África, Pierre Dandjinou, Yaovi Atohoun y Bob, que está en nuestra oficina de Nairobi. Yo empezaría por ahí para solicitar información acerca de la comunidad local. Gracias.

JOANNA KULESZA: En mi experiencia personal, el equipo de GSE siempre es muy accesible. Tiene muy buena disposición. Si ustedes pueden compartir esa información con su comunidad local, es muy interesante y nos interesa recibir sus comentarios para luego pasárselos a León también. Veo que un miembro de la audiencia del público quiere hacer una pregunta. Le pido que se aproxime

a la mesa y utilice cualquier micrófono que esté disponible. Muchas gracias.

CRAIG JONES: Hola. Soy Craig Jones, de INTERPOL. Soy el nuevo director de ciberdelito en mi organización y me interesa mucho la prevención. Siempre dedicamos muchos recursos a este tema de la prevención porque queremos prevenir los ciberataques. Con todo gusto entablaré una conversación con ustedes. Gracias.

PATRICK JONES: Muchas gracias. Seguramente usted habló con John Crain y con Carlos Álvarez y también con nuestro representante de la región de Asia-Pacífico, que hizo una presentación para INTERPOL en un evento en Corea. Ya sabe con quién puede dialogar.

JOANNA KULESZA: Bueno, veo que alguien más quiere hacer alguna pregunta. También un miembro del público. Allí tiene un micrófono disponible, señor. Adelante.

MATOGORO JABERA: Hola. Soy Matogoro Jabera. Agradezco su presentación, que fue muy buena. Quiero mencionarles que también represento a mi entidad ante el equipo de revisión de seguridad y estabilidad de

la ICANN. Agradezco su presentación. Tomo nota de sus comentarios. Vamos a tener todo esto en cuenta. Gracias.

JOANNA KULESZA: Muchas gracias. ¿Alguna otra pregunta? Bien. Si no hay más preguntas voy a concluir esta sesión. Voy a comenzar agradeciéndole a Patrick por su presentación, por toda esta información. También le voy a agradecer a León por su tiempo, por estar aquí con nosotros. Quiero agradecerles a todos por su presencia. Si tienen preguntas y son un poco tímidos, nos pueden escribir por correo electrónico al personal, a mí. Necesitamos redactores de nuestro comentario acerca de la seguridad de los servidores raíz. Muchas gracias a nuestro personal técnico. Muchas gracias a nuestros maravillosos intérpretes. Muchas gracias a todos. Que tengan una muy buena tarde. Gracias.

[FIN DE LA TRANSCRIPCIÓN]