YEŞIM NAZLAR: Buenos días, buenas tardes y buenas noches a todos. Bienvenidos al quinto seminario web de los cinco seminarios web obligatorios para ATLAS III. Hoy vamos a abordar el tema de la ciberseguridad. Nuestro presentador el día de hoy es Patrick Jones, quien es director sénior de participación de partes interesadas globales. No vamos a pasar asistencia para este seminario web. No obstante, sí vamos a considerar la asistencia presente durante los primeros 10 minutos de esta llamada. Luego de esto, la participación no será considerada como válida como requisito para las métricas de participación. Si solamente se encuentran conectados al puente telefónico, por favor, únanse a la sala de Zoom tan pronto como sea posible para poder cumplir con el requisito de la asistencia.

Contamos con interpretación en francés y en español para este seminario web. Quiero recordarles a todos los participantes que mencionen sus nombres al momento de tomar la palabra para que los intérpretes los puedan identificar en los canales lingüísticos correspondientes y también para la transcripción. También recuerden hablar a una velocidad razonable para que los intérpretes puedan hacer una interpretación adecuada.

Todas las líneas estarán silenciadas durante la presentación y al momento de la sesión de preguntas y respuestas podrán tomar la palabra al final de la presentación. Este seminario web se está llevando a cabo en Zoom. Las características son similares al Adobe Connect para poder ver la lista de participantes y la sala de chat. Deben hacer clic en los iconos que aparecen en la parte inferior de la pantalla. Solo van a

poder ver la transcripción del chat una vez que se unan a la llamada, no con antelación a la misma. Para levantar la mano deben hacer clic en el icono que indica levantar la mano. Ahora voy a darle la palabra a Joanna Kulesza, quien es copresidenta del subgrupo para ATLAS III. Joanna, adelante, por favor.

JOANNA KULESZA: Gracias a todos. Gracias, Yeşim. Gracias por la presentación. Gracias a todos los participantes conectados. En nuestro quinto seminario web obligatorio mi especial agradecimiento a Patrick por estar aquí presente el día de hoy. Nos va a hacer una introducción al tema de la ciberseguridad y ya tuvimos la primera edición de este seminario web hace 14 horas con David Huberman. Patrick está focalizado en ciberseguridad. Le agradecemos a Patrick por su tiempo y por participar debido a su experiencia en la participación de partes globales. Habiendo dicho esto, Patrick, le cedo la palabra para que comience con la presentación. Adelante, por favor. Patrick, si está hablando no lo escuchamos.

PATRICK JONES: Hola, hola. Sí. Estoy conectado ahora sí. Perdón pero se me desconectó Internet hace unos momentos. ¿Me escuchan? ¿Están listos para comenzar?

JOANNA KULESZA: Sí, sí. Ya estamos listos. Hemos comenzado la grabación del seminario y ya lo he presentado. Estamos listos para dar comienzo.

PATRICK JONES: Muchas gracias por darme la oportunidad de presentar este tema en este seminario web. Ayer seguramente escucharon a David Huberman, quien es parte del equipo de la oficina del CTO. Mi nombre es Patrick Jones. Pertenezco al equipo de participación de partes globales. Trabajo en la ICANN desde hace 13 años y trabajo en el equipo de seguridad y en realidad trabajé también antes en este equipo unos seis años. Les doy esta información teniendo en cuenta mi experiencia dentro de la ICANN. Espero que les resulte útil como un complemento necesario en relación a las herramientas que están disponibles en ICANN Learn. Recientemente hemos agregado un curso sobre cuestiones básicas de ciberseguridad y eso incluye el uso indebido del DNS. Esto les va a servir para poder tener un mejor entendimiento de cuestiones que tienen que ver con Internet. Sin más vamos a pasar a la siguiente diapositiva.

Vamos a comenzar entonces hablando de los elementos esenciales que existen en toda red. Hay cosas que están dentro de una red de una empresa o de una red universitaria o una red gubernamental. Los elementos más comunes dentro de estas redes son los servidores de correo, donde se brinda correo electrónico, funciones de calendario y también donde se guarda la información de los contactos. Luego hay servidores que son servidores de base de datos. Aquí se almacenan datos de empleados, de clientes u otro tipo de información que almacenan las empresas o los gobiernos. Luego tenemos información financiera. Esto se almacena en los servidores de archivo. Esa es información de una empresa, de un gobierno o también procedimientos y procesos organizacionales. Básicamente estos son los elementos para cualquier tipo de red en una organización.

Debido a que todas estas organizaciones cuentan con estos elementos, estos son objetivos de los atacantes. Estas funciones llevan a cabo una serie de servicios que tienen que ver con la gestión de identidad, lo cual incluye nombres de usuarios, las cuestiones biométricas y otras formas de autenticación. Esto también podría incluir la gestión criptográfica de las llaves.

Luego tenemos el almacenamiento. Es lo que se hace con la retención de los datos. También pueden existir políticas creadas en pos de la protección de las redes y la información. Hay sistemas implementados como por ejemplo el material de software o hardware. También puede haber una revisión de software o patching. También existen infraestructuras como por ejemplo las direcciones de IP o el sistema de DNS que permiten la conexión a las redes tanto internas como externas. Todas estas cuestiones a menudo se encuentran bajo amenaza de ataque. Los atacantes tienen como objetivo extraer datos del sistema. Siguiente diapositiva.

Cuando hablamos de los tipos de ciberdelitos, los elementos más comunes que encontramos incluyen los siguientes. Phishing o suplantación de identidad, que es la práctica fraudulenta de enviar correos electrónicos presumiendo que esto proviene de empresas u organizaciones que tienen cierta reputación para poder engañar al receptor y hacer que revele información personal. Esto puede ser contraseñas, información de tarjeta de crédito, credenciales que permiten a los delincuentes acceder a la información como el correo electrónico o algún sistema. Esto resulta muy común.

Otro tipo de ciberdelito es el malware. En este caso se trata de un software que ha sido creado específicamente para dañar o corromper o ganar acceso no autorizado a un sistema informático. Esto incluye, entre otras cosas, ransomware, que es un malware que infecta una máquina. Uno se conecta a la computadora, por ejemplo, y le da acceso a la computadora o a la máquina. El delincuente, por ejemplo, dice: "Debe pagarme una cantidad de dinero como una especie de rescate para poder tener acceso a determinado sistema". Obviamente, esto nunca sucede.

Otro ejemplo muy común son los botnets o las redes robots. En este caso se trata de un sistema de computadoras infectadas que tienen control sobre un grupo. Estos botnets o redes robots son controladas por nombres de dominio que brindan este tipo de sistema de control. Luego les voy a contar un poco más al respecto. Siguiente diapositiva.

Dentro del contexto de la ICANN ustedes probablemente han escuchado hablar del término uso indebido del DNS. Vamos a hablar de esto en breve. La mayor parte de las organizaciones, ya sean gubernamentales, comerciales o individuos, utilizan el sistema de nombres de dominio para resolver sus nombres de dominio de manera amigable dentro de las direcciones del protocolo de Internet. Es decir, las direcciones IP son números y es muy difícil que los seres humanos recuerden esos números. Estos números se asocian a un nombre y por lo tanto resulta más sencillo poder realizar búsquedas dentro del nombre de dominio. Esto también se conecta a consultas en diferentes computadoras.

Los delincuentes lo que intentan hacer es romper el DNS para sus propios beneficios. Esto lo hacen interrumpiendo transacciones

comerciales, servicios gubernamentales, sitios gubernamentales o también pueden afectar las redes sociales. Vemos a menudo que hay organizaciones que son objetivo de estos ataques. También se puede explotar el DNS y se puede engañar a los usuarios. Esto a menudo se hace mediante el registro de nombres de dominio maliciosos o quizá al hacer un secuestro de la resolución de nombres o de los servicios de registros o mediante la corrupción de los datos del DNS.

Ahora les voy a contar sobre los ataques cibernéticos y cómo sería un ataque. El objetivo es atacar a las vulnerabilidades del sistema de enrutamiento de Internet. También a los sistemas de correo electrónico. Típicamente hay un intento de alterar la parte de la resolución dentro del DNS. En la siguiente diapositiva tenemos un ejemplo de un incidente que sucedió realmente en abril de 2018. Vamos a pasar a la siguiente diapositiva.

Bien. Este es un ejemplo real de un nombre de dominio denominado MyEtherWallet. Este nombre de dominio fue utilizado para albergar criptomonedas. Este era un dominio que fue atacado y los atacantes utilizaron la infraestructura o el sistema de nombres de dominio para redirigir a los usuarios a un sitio falso que parecía ser MyEtherWallet.com. Lo que los usuarios hacían era colocar sus credenciales de ingreso en el sitio web falso en lugar de hacerlo en el sitio real y, por supuesto, daban la información sobre sus criptomonedas. Esto les permitió a los atacantes robar unos 21 millones de dólares en criptomoneda. Este es uno de los tantos ejemplos donde el secuestro o el desvío de información pueden dar forma a un ataque.

Otro tipo de ataque tiene que ver con los ataques cibernéticos que están motivados por cuestiones políticas. En noviembre del año pasado, en algunos casos todavía siguen vigentes, hubo un ataque de muy alto nivel y fue un ataque muy coordinado que se conoce como DNSpionage y Sea Turtle. Este es un ejemplo donde hay un preposicionamiento de los delitos cibernéticos a nivel militar, cuyo objetivo es hacer ataques cibernéticos. En diferentes oportunidades se han identificado 40 organizaciones en 13 países. En realidad había más de estas cantidades pero cuando sucedió el ataque en primer lugar esto se dio primariamente en África del Norte y en Oriente Medio.

Las organizaciones de seguridad, las aerolíneas, también los ministerios de asuntos exteriores o las compañías energéticas son los objetivos primordiales. También hubo ataques en otras partes de Europa a los proveedores de hosting, incluso de los Estados Unidos. Lo que pudieron hacer los atacantes fue infiltrarse en el DNS y en el correo electrónico y en las autoridades de certificados y perpetrar el ataque. Siguiente diapositiva.

El rol de la ICANN es limitado. Una de las cuestiones que nosotros podemos hacer es brindar una plataforma para compartir las experiencias y generar concienciación. El comité asesor brindó unos talleres y guías prácticas para las distintas partes interesadas que estaban presentes sobre las cosas que se pueden hacer para proteger las redes de seguridad. Es bastante común para todo aquel que tiene un nombre de dominio. Voy a hablar sobre esto un poco más adelante.

Los ataques que están ocurriendo cubren incluso a gobiernos, empresas, organismos de aplicación de la ley y usuarios de Internet en general.

Esto está ocurriendo a nivel diario. Hay un equipo de ICANN que está trabajando con registros y registradores y otras partes interesadas de la comunidad de Internet para poder compartir conocimiento e información y generar conciencia sobre lo que se puede hacer. También para brindar una plataforma para compartir información cuando este tipo de ataques ocurran. Siguiente diapositiva.

Vamos a entrar ahora a qué es lo que va a ocurrir antes de que ocurra un incidente. Vamos a dar un poco de contexto. Según nuestros estatutos hay un gran énfasis en asegurar que el sistema unívoco de identificadores de Internet es seguro y estable. También se incluyen algunos compromisos que incluyen la preservación y mejora de la administración del sistema de nombres de dominio y la estabilidad, confiabilidad, seguridad, interoperabilidad global, resiliencia y apertura del DNS y de Internet. Hacemos esto dando una forma en la cual las partes contratadas, los registros y los registradores pueden compartir información cuando existan vulnerabilidades y cuando existan ataques que van ocurriendo. También brindamos una plataforma conveniente en nuestras reuniones a través de listas de correo para aquellos que están participando en la comprensión de los problemas de seguridad y la información, y también trabajamos con otros socios en el ecosistema de Internet que incluyen los registros regionales de Internet donde las organizaciones y otros están incluidos, y trabajan colaborativamente compartiendo conocimiento e información.

Vamos a ver ahora que en ICANN hay algunas palabras que se usan muy seguido. Empezamos con seguridad, estabilidad y flexibilidad. ¿Qué queremos decir en este sentido? La seguridad es la capacidad de proteger el uso indebido de los identificadores únicos de Internet.

Cuando hablamos de estabilidad nos referimos a asegurar que el sistema opera tal como se espera y que los usuarios de esos identificadores únicos tienen confianza en que el sistema opera como se espera. En cuanto a la sensibilidad o la resiliencia, hemos de referirnos a la capacidad de que los sistemas únicos puedan soportar ataques maliciosos y otros eventos sin interrumpir o cesar el servicio. Siguiente diapositiva.

Tenemos algunos compromisos también para la seguridad, estabilidad y flexibilidad del sistema de identificadores únicos. Lo hacemos a través de alentar a todas las partes interesadas en el ecosistema de Internet a que participen en un desarrollo activo de las políticas. También a través del trabajo técnico. Veo aquí un comentario en el chat de Zoom. Creo que el equipo de At-Large les va a dar un link a estos archivos una vez que esta sesión finalice. Espero haber respondido la pregunta. Será un link a las diapositivas.

Otros compromisos incluyen que trabajamos en colaboración con partes regionales en cuanto a lo que se refiere a entrenamientos en seguridad o generación de capacidad. Esto también es solicitado por las organizaciones locales. Muchas veces hacemos capacitaciones sobre las extensiones de la seguridad del DNS y otro sobre el uso indebido del DNS, para reconocer el uso indebido del DNS. Esto depende de qué es lo que solicita la organización regional para ese entrenamiento o capacitación.

Dentro de los distintos grupos de partes interesadas de ICANN y de comités asesores hay algunas comunidades que desarrollan políticas y procedimientos vinculados con la mejora de la seguridad, estabilidad y

flexibilidad. Uno de esos grupos está dentro de nuestro comité asesor gubernamental. Se llama grupo de trabajo de seguridad pública. Existe desde hace unos 6-7 años. Tuvo un esfuerzo inicial de reunir la experiencia de las organizaciones de seguridad pública y organismos de aplicación de la ley. Este grupo de seguridad pública ha estado brindando feedback y también comentarios públicos. Se focalizan también en las políticas y procedimientos de la ICANN que se vinculan con el abuso del DNS. También brindan una forma de compartir información con el comité asesor.

Con respecto a otros comités asesores están por ejemplo el comité asesor de seguridad y estabilidad. Este comité asesor está dentro de la comunidad de la ICANN y trabaja para realizar por ejemplo análisis de riesgos o evaluación de amenazas del sistema de identificadores únicos. También brindan charlas en las sesiones públicas de la ICANN. Algunos de los temas recientes que han estado abordando tienen que ver con temas relacionados con los nombres de dominio internacionalizados. También han hecho observaciones con respecto al ciberataque de DNSpionage.

En la reunión de Marrakech este comité va a tener una sesión sobre uso indebido del DNS. Finalmente tenemos el comité asesor del sistema de servidores raíz que, por supuesto, se encarga de cuestiones que tienen que ver con el sistema de nombres de dominio y en este caso la función es asesorar a la junta directiva al respecto y a la comunidad sobre cuestiones que tienen que ver con la operación. En próximas reuniones habrá una posibilidad de participar en los comentarios públicos con respecto al modelo de gobernanza para este comité asesor. Habrá en

este sentido más oportunidades para que la comunidad participe. Siguiente diapositiva, por favor.

Hablemos de la relación entre los registros y registradores o las partes contratadas. Estos son importantes para promover la seguridad, la estabilidad y la resiliencia. El acuerdo de acreditación de registros impone la obligación de investigar un uso indebido o cuestiones que tengan que ver con el uso indebido de los nombres que gestionan y recientemente el acuerdo de registro incluye una cláusula que prohíbe a los titulares de nombres de dominio registrados distribuir malware u operar de forma abusiva, botnets, hacer phishing, piratería o infringir derechos de marca o derechos de propiedad intelectual o alguna otra práctica fraudulenta. Siguiente diapositiva, por favor.

Aquí vemos un diagrama de las partes contratadas dentro del ecosistema de la ICANN y cómo interactúan. Existe una relación entre la ICANN y las partes que está cubierta por el acuerdo de registros. Tenemos los registradores que también tienen un acuerdo y existen también acuerdos entre los registros y lo que estos ofrecen a los usuarios. A veces los registradores utilizan revendedores pero estos revendedores no tienen un contrato con la ICANN. Muchas veces vemos preguntas por parte de la comunidad que tienen que ver con temas que suceden a nivel de los revendedores pero estos no tienen relación con la ICANN. Los registradores y los revendedores tienen una relación con el registratario y esto se da a través del acuerdo de registratarios.

Todos los acuerdos de registro están disponibles en el sitio web de la ICANN. Hay una página dentro del sitio web de la ICANN donde se puede ver el acuerdo de acreditación de registro. Si uno está utilizando un

registrador también puede conocer cuáles son las expectativas o cuáles son las obligaciones al acceder a esta información y también puede comunicarse con el departamento de cumplimiento contractual de la ICANN.

ICANN tiene una subsidiaria que se llama identificadores públicos técnicos y que es responsable de la operación de los aspectos de los sistemas de Internet. Hablamos de IPv4, IPv6 o de sistemas autónomos para los registros regionales de Internet. También mantienen la zona raíz para el sistema de dominio y administran la zona ARPA. También se mantiene el ancla de confianza para las extensiones de seguridad en el dominio y se coordinan más de 3.000 registros para otros protocolos que ocurren en el IETF. Esto nos lleva entonces a un poco más de contexto hacia qué son las extensiones de seguridad de dominio del DNS en la próxima diapositiva.

Cuando la comunidad técnica de Internet y los investigadores desarrollaron el sistema de nombres de dominio la seguridad no estaba en el top de las prioridades. Era al principio de los años 90, fines de los 80 donde había algunas vulnerabilidades que se descubrieron y como respuesta a eso la comunidad técnica y los investigadores generaron un nuevo protocolo para las extensiones de seguridad de dominio. De esta manera se agregó un nivel de seguridad y protección a los datos del DNS. Hay algunos operadores de código de país que utilizan DNSSEC. En el año 2010 ICANN firmó la zona raíz junto con estos protocolos.

Esto ayudó a brindar un nivel de seguridad a los usuarios de que los datos son válidos y son ciertos. También da una cadena de confianza desde el primer nivel del sistema de nombres de dominio hacia el nivel

de los registradores. Así se firman extensiones como .COM. También hay bancos, aerolíneas y otras organizaciones que implementan DNSSEC y esto permite a los operadores de DNS que se validen todos los datos que pasan y que estos datos son precisos. De ese modo, el usuario no puede ser redirigido maliciosamente hacia un sitio y va hacia el dominio que tiene intención de encontrar.

Las extensiones de DNS utilizan la infraestructura de clave pública. Seguramente escucharon hablar de la firma de la llave, la KSK. Es la llave más alta en criptografía. La KSK se basa en unos pares de llaves públicas. Es decir, es el punto de inicio para la validación que los resolutores van a tener que utilizar y la parte privada contiene la zona de firma de la llave. ICANN a través de la PTI mantiene la ZSK, la clave de la firma de la zona, para que luego los individuales tengan la KSK para la parte pública. Así se genera la cadena de confianza que brinda un mayor nivel de seguridad para el sistema de nombres de dominio. Siguiente diapositiva.

Como mencioné, la PTI emite, gestiona, cambia y distribuye las claves de DNS. Firman la llave para las extensiones de DNS y luego siguen buenas prácticas desarrolladas por la fuerza de trabajo de ingeniería de Internet y la comunidad pública. Nosotros varias veces al año hacemos ceremonias de llave. Cualquiera lo puede seguir remotamente cuando hacemos las actualizaciones a la KSK y a la infraestructura del DNS. Si les interesa, esto se publica con bastante anticipación a la ceremonia en el sitio web de la ICANN. Es una forma fascinante, diría, de ver cómo los identificadores clave de Internet son asegurados. Siguiente diapositiva.

Nuestra oficina del CTO con su equipo y los distintos equipos de participación se ocupan de esfuerzos para trabajar con nuestros socios

privados en cuestiones vinculadas con los identificadores de Internet y la ciberseguridad. Lo hacemos a través de las sesiones de la ICANN o webinars como este donde participamos en talleres técnicos y en capacitaciones y también a través de distintos tipos de generación de capacidad. Por ejemplo, hace dos semanas muchos de nosotros estábamos participando en sesiones en el simposio del DNS en Bangkok, Tailandia junto con otros talleres que iban ocurriendo allí. Hubo capacitaciones que fueron brindadas por THNIC como parte del operador de red de Tailandia. La razón por la que lo hacemos en distintas partes del mundo es que ICANN y sus socios participan en eventos de generación de capacidad para ayudar a compartir las experiencias y el conocimiento con otros que están en torno a la comunidad técnica. Siguiente diapositiva.

Cuando sucede un incidente de un ataque cibernético, vamos a hablar de lo que hacen las distintas organizaciones. La ICANN es miembro de los equipos de respuesta ante incidentes. Hay un equipo de respuesta a nivel nacional. Son plataformas donde se comparte información cuando sucede un ataque. A menudo se comparte esta información con otros operadores de redes, con agencias de seguridad o con agencias de cumplimiento de la ley como INTERPOL, EUROPOL y otros organismos globales. Esto también puede incluir una respuesta coordinada de los registros y registradores de dominios de alto nivel. Estos son los principales actores que pueden estar involucrados en la mitigación de un ataque cibernético a través de una respuesta coordinada. Siguiente diapositiva.

Cuando sucede un ataque, es muy difícil identificar la fuente de ese ataque pero es importante que aquellos que responden traten de

identificar las direcciones de IP que se están utilizando, si hay nombres de dominio que están involucrados en este ataque, hay que identificar quién es el registratario, dónde está el registro o el registrador ubicado y cuáles son las organizaciones que también están detrás de esto. También verificar las bases de datos para intentar identificar la fuente de ese ataque. La atribución requiere fuentes de datos. Esto también podría incluir información de contacto de la registración asociada por ejemplo con las direcciones de IP o también los números autónomos. Siguiente diapositiva.

Como mencioné anteriormente, ICANN tiene un equipo dentro de la oficina del CTO que trabaja con otras organizaciones y con otras comunidades para tener una respuesta coordinada ante un ataque cibernético. Este equipo tiene un entendimiento o comprensión profunda de lo que sucede, cuáles son las respuestas durante un ataque. También el equipo participa junto con las agencias de cumplimiento de la ley, los registros y registradores. Lo que hacen es compartir experiencias después de que suceden los ataques durante unas reuniones de la ICANN y nosotros en nuestro sitio web brindamos un proceso de divulgación coordinado que permite a los investigadores y registros en materia de seguridad encontrar información.

Hubo un caso donde un usuario descubrió una vulnerabilidad en la funcionalidad de Adobe Connect. Nosotros tuvimos que abordarla y por eso estamos trabajando hoy con Zoom. Esto se dio y pudo ser posible porque hubo una respuesta rápida de este miembro de la comunidad, quien hizo una investigación para poder llegar a la fuente y después derivarnos la responsabilidad. Esa es la forma en la que trabajamos cuando hablamos de coordinación. Nosotros pasamos información.

Cuando llegó esta información sobre el Adobe, nosotros compartimos esta información y pudimos hacer los ajustes necesarios a las redes correspondientes. Siguiente diapositiva, por favor.

Aquí vamos a hablar del rol de la ICANN luego de un incidente de seguridad o de un ciberataque. Lo que hacemos comúnmente es compartir nuestras experiencias como por ejemplo en eventos tales como el simposio del DNS o con las comunidades técnicas o con los operadores de redes. En la comunidad técnica, los investigadores y otros pueden tomar esta información y también coordinarla o definir nuevas políticas, quizá hacer cambios a los contratos o a sus contratos o quizá también identificar protocolos que deban ser mejorados o que deban ser modificados. Lo que también se puede hacer al compartir esta información con los operadores de redes es compartir esta información con los operadores de redes o con las agencias de cumplimiento de la ley. Siguiente diapositiva.

Nos vamos acercando ahora al final. Luego les voy a dar la palabra para que efectúen preguntas. El punto de partida es que el DNS no es solamente una función técnica que es administrada por los administradores de sistemas sino que es una infraestructura crítica necesaria para la comunicación diaria que implica correos electrónicos, búsquedas en la red y también aplicaciones en los teléfonos móviles. Esto puede ser una plataforma de despegue para que otros dispositivos de Internet se conecten. Es crítico que quienes crean políticas o toman decisiones estén atentos a esta infraestructura del DNS. Si uno ve que la estructura del DNS está comprometida, entonces todos los sistemas y redes están en riesgo.

En la siguiente diapositiva vamos a ver algunas recomendaciones efectuadas por la ICANN. Esto data de febrero de este año. La ICANN publicó una serie de recomendaciones para la comunidad de Internet en general y esto incluye, por ejemplo, mejores prácticas para la autorización de las redes, la autenticación de los sistemas, para efectuar encriptación. También patching o revisión de software y determinar si existe una seguridad adecuada de los correos electrónicos. Toda esta información se puede encontrar en el enlace que ven más abajo. Esto fue publicado el 15 de febrero. Una de las recomendaciones más importantes es tener implementadas DNSSEC para minimizar el impacto de los ataques.

En la siguiente diapositiva vemos que la seguridad y la flexibilidad de Internet son importantes para la comunidad. Nosotros también definimos el ciberdelito e incluimos distribución de malware, intentos de phishing o suplantación de identidad, la operación de botnets, piratería para socavar prácticas comerciales. Hay mucho esfuerzo que está haciendo la comunicación actualmente para contribuir e incrementar la estabilidad, la seguridad y la resiliencia del sistema y de Internet y de los identificadores únicos. Espero que haya preguntas. Yo voy a tratar de responderlas adecuadamente. Si no, los voy a dirigir al lugar donde pueden encontrar esas respuestas.

Veo que en el chat de Zoom hay algunas preguntas ya planteadas. Hay una pregunta que dice si un ataque puede apagar Internet o redes en general. Los ataques al DNS es un tipo de ataque. No quiero entrar en detalles con respecto a los diferentes ataques que existen porque quiero tratar de que este contenido se dé a nivel general pero obviamente puedo responder las preguntas más en detalle.

JOANNA KULESZA: Tenemos una pregunta de Joan Katambi. Le voy a dar la palabra para que haga una pregunta. Adelante, Joan. ¿Nos escucha? Joan, ¿nos escucha? Tiene la palabra. Adelante, por favor. Parece que no. Me pregunto si hay alguna otra pregunta por parte de los participantes. Pueden levantar la mano y hacer la pregunta si así lo desean. Voy a comenzar con las preguntas. Dave nos dio algunos puntos pero me pregunto, Patrick, cuál es su perspectiva con respecto a lo que pueden hacer los usuarios finales para incrementar su conciencia o resiliencia en materia de ataques cibernéticos. Creo que esta es una pregunta que nos puede resultar útil a la comunidad. Me pregunto si usted tiene algún punto de vista para compartir con nosotros.

PATRICK JONES: No escuché la presentación de David ayer. Quizá mi respuesta sea un tanto distinta a la de él. Como usuario final, lo que se puede hacer es que si uno tiene un nombre de dominio, por ejemplo. Uno tiene que ir a un registrador y preguntarle si tiene las extensiones de seguridad, las DNSSEC implementadas y ver si esto es así de los servicios que ustedes obtienen de los registradores. También pueden implementar seguridad de correo electrónico. Pueden no reutilizar contraseñas en diferentes sitios. También pueden, por ejemplo, estar al tanto de quién tiene acceso a sus nombres de dominio críticos o a los servicios críticos. Es decir, quién tiene acceso al correo electrónico en la corporación o en la agencia en la que ustedes están trabajando por la cual son responsables. Hay bases de datos que son clave.

Si uno es un usuario común y no tiene un nombre de dominio pero, por ejemplo, hace transacciones bancarias en línea tiene que ser cuidadoso cuando utiliza las contraseñas. Si uno utiliza, por ejemplo, el correo electrónico, se pueden utilizar diferentes niveles de autenticación. Los portales bancarios lo ofrecen. Me voy a detener aquí. Creo que esto les va a resultar útil. Espero que sí.

JOANNA KULESZA: Tenemos otras preguntas en el chat. Espero que las puedan ver. Si no, con gusto las puedo plantear.

PATRICK JONES: Satish tiene una pregunta que tiene que ver con la evolución del DNS en el futuro y cuál va a ser el rol en los próximos años. Hay aplicaciones que se pueden descargar, por ejemplo, en los dispositivos o en las computadoras que operan en el background y que también acceden a nombres o direcciones IP o protocolos de Internet y que nos permiten conectar a otras máquinas. El DNS aun así sigue siendo una tecnología clave. Cada vez se utiliza con más frecuencia. Cada vez hay más dispositivos que se conectan. Desde la perspectiva de la ICANN no vemos una disminución de la importancia del DNS. Quizá haya nuevas formas de utilización del DNS en las cuales se pueda explotar el DNS. Es una estructura básica común.

También hay que incrementar el conocimiento de las tecnologías mediante sesiones técnicas, sesiones de trabajo con el OCTO. También hay otras sesiones que tienen que ver con sesiones técnicas entre la junta directiva, los expertos técnicos que a menudo debaten temas que

tienen que ver con los cambios a la tecnología del DNS. Estas son las sesiones que se deben seguir.

La siguiente pregunta tiene que ver con la gobernanza que parece ser necesaria para la ciberseguridad. Lo que intentamos hacer desde el equipo de GSE es tener una participación activa en el trabajo de política en materia técnica. Esto es algo de interés, los temas de seguridad. En nuestras reuniones hay varias formas de participar. Una de ellas tiene que ver con asistir al día técnico y a las reuniones o participar remotamente. También participar como voluntarios. Hay una política de ciberseguridad y es importante que se pueda participar en estos esfuerzos dentro de la ICANN o en las distintas organizaciones técnicas para poder saber cuáles son los temas clave que se están debatiendo actualmente.

JOANNA KULESZA: Patrick, tenemos una pregunta más de Michael sobre el apoyo financiero para asegurar las infraestructuras de los países. Creo que John también quiere tomar una pregunta. La pregunta de Michael también está en el chat.

PATRICK JONES: Vamos a volver un poquito para atrás entonces. Los esfuerzos sobre el desarrollo muchas veces se discuten en otros foros.

JOANNA KULESZA: Patrick, no podemos escucharlo.

YEŞIM NAZLAR: Patrick, si está hablando, no podemos oírlo.

JOANNA KULESZA: Creo que Patrick se desconectó por un momento. Lo vamos a volver a llamar y vamos a conectarnos con él nuevamente. Les pedimos un poco de paciencia. El orden de los oradores es una pregunta que tenemos de Michael, que la va a responder Patrick en cuanto se conecte. Tengo dos manos levantadas. Una es de Joan, que parece que también se desconectó. Tengo también una mano levantada de Abdelmonem Galila a quien le voy a dar la palabra a continuación en cuanto volvamos a conectarnos con nuestro orador. Luego tenemos otras dos preguntas que aparecieron en el chat y que espero también que puedan ser respondidas en los próximos siete minutos que tenemos disponibles en esta llamada. En cuanto a las cuestiones técnicas, voy a tratar de nos extendamos un poquito más del tiempo asignado. De nuevo, esto se debe a cuestiones técnicas. Esperamos que se puedan resolver en los próximos minutos. Por favor, tengan en cuenta que la diapositiva va a estar publicada en el sitio web de la ICANN.

YEŞIM NAZLAR: Sigo esperando que se conecte Patrick. No puedo tener una respuesta de él.

JOANNA KULESZA: Gracias, Yeşim. Si hay algún comentario de los participantes también pueden aprovechar para compartirla en este momento con el grupo.

YEŞIM NAZLAR: Voy a intentar con un número que pude encontrar en nuestra lista. Él acaba de compartir un número también. Les pido que tengan paciencia por un minuto o más mientras volvemos a conectarnos con él en el puente telefónico.

JOANNA KULESZA: Gracias, Abdelmonem, por este feedback. Debo decir que estamos muy contentos de tener una alta participación y queremos seguir evolucionando en ese proceso. También en las reuniones presenciales en Marrakech o en Montreal. Veo la mano de Joan para arriba y para abajo. Joan, si quiere compartir algún comentario lo puede hacer.

PATRICK JONES: Incluso en los lugares desarrollados tenemos problemas de conectividad de Internet. Es muy frustrante. Les agradezco por haber tenido paciencia.

JOANNA KULESZA: Tenemos a Joan, que quiere hacer una pregunta. Diría que tomemos primero la pregunta de Joan y luego tengo una lista de otras preguntas que también han sido escritas en el chat. Quisiera saber si tenemos permiso para continuar algunos minutos más, Patrick, si a usted le parece bien.

PATRICK JONES: Ahora que estoy solo conectado por teléfono, espero que esta comunicación continúe. Adelante.

JOANNA KULESZA: Le voy a dar la palabra a Joan y voy a ver si podemos continuar con la interpretación.

JOAN KATAMBI: Soy Joan Katambi, de Uganda. Espero que me escuchen bien. Mi pregunta para usted, Patrick, y quiero agradecerle por la presentación, es la siguiente. ICANN tiene una política de ciberseguridad que está disponible. Número dos, ¿ICANN tiene una estrategia de ciberseguridad que esté disponible y que puede ser vista por el público? Estas son mis dos preguntas. Gracias.

PATRICK JONES: Tenemos una estrategia de ciberseguridad que es parte de nuestra estrategia general de seguridad. Nuestros elementos estratégicos están allí. Recientemente nosotros publicamos un plan estratégico del año fiscal 2021-2025 donde se incluyen objetivos estratégicos vinculados con el DNS y la seguridad de los identificadores únicos. Si ustedes miran un poco más en nuestra historia hemos tenido un marco de seguridad, estabilidad y flexibilidad y ese documento está en el sitio web de la ICANN a pesar de que este trabajo está siendo actualizado como parte de nuestro equipo de revisión que está analizando estos asuntos. Es el mejor documento para ver ahora porque no se focaliza únicamente en la seguridad sino en el plan estratégico general de la ICANN que contiene elementos de seguridad. Si me puede repetir la primera pregunta, por favor.

JOAN KATAMBI: ¿ICANN tiene una política de ciberseguridad incluida? En Uganda, por ejemplo, tenemos una política de ciberseguridad pero la estrategia está esperando que se apruebe.

PATRICK JONES: Para las redes que nosotros operamos tenemos políticas internas vinculadas a cómo utilizamos nuestras redes y nuestros sistemas pero ese documento no se ha publicado. Nosotros tenemos una declaración de práctica para la implementación de extensiones de seguridad de dominio. Por lo tanto, yo no creo que tengamos una política de ciberseguridad como documento público sino que lo que tenemos son prácticas internas que vamos siguiendo.

JOANNA KULESZA: Gracias, Patrick. Le voy a leer tres preguntas si les parece bien. También les quiero confirmar que nuestros intérpretes han aceptado amablemente continuar un poco más. Tenemos unos ocho minutos más. Voy a leer las preguntas. Voy a darle la palabra a Patrick para que las responda y luego voy a abrir la lista de oradores para ver si hay más preguntas.

La primera es de Vrikson Acosta. Quiere saber de qué manera se deben tratar las cuestiones técnicas del DNS. Esa es la pregunta una. La segunda es de Ibtissam Kaifouf que quiere saber cuáles son las cuestiones de seguridad del DNS que plantean las tecnologías del 5G y otra de Abdelmonem Galila quien quiere saber en el contexto de los nuevos protocolos vinculados al DNS como DOH o DOT cuál es el rol de la ICANN en este sentido. Es decir, cuáles son los protocolos que aplican

DNS. Espero que las preguntas sean claras. Si no lo son, vamos a pedir más claridad. Le damos entonces nuevamente la palabra. Si necesita alguna aclaración, díganoslo, por favor.

PATRICK JONES: Respecto de las cuestiones éticas de DNS, debemos decir que ICANN no se involucra en cuestiones vinculadas al contenido en el DNS. Nuestro trabajo se focaliza en la política y en las cuestiones técnicas vinculadas al funcionamiento del sistema. Es decir, si hay cuestiones vinculadas a cómo se utilizan los identificadores para entregar contenido, esas discusiones no ocurren en ICANN org. Podemos establecer una plataforma conveniente para las partes interesadas a las que les interese. Tenemos una unidad constitutiva de negocios que participa en nuestro contexto. También una de propiedad intelectual que participa en el trabajo de política. Desde el punto de vista del trabajo de la ICANN, las cuestiones vinculadas al contenido, que creo que a eso se refiere la persona que hace la pregunta cuando habla de las cuestiones éticas, no están incluidas en este contexto. Espero haber respondido la pregunta.

Las tecnologías 5G tienen que ver con el foro del DNS para el Medio Oriente y otros operadores de telecomunicaciones que hablan sobre el 5G. Puede haber cuestiones de evolución de la tecnología en nuestras reuniones. Tenemos una agenda para las próximas reuniones en Marrakech, en Montreal. Espero que empecemos a escuchar un poco más sobre otras organizaciones. Uno de nuestros socios es el GSMA, que es una organización paraguas para los operadores de telecomunicaciones que se focalizan en el 5G, en la implementación del

5G. Vienen a nuestras reuniones y seguramente los vamos a escuchar un poco más.

En cuanto a la última pregunta, DNS sobre HTTP, DOH y DOT son temas de muy alto interés de los gobiernos, de los proveedores de servicios de Internet y otros. Hubo paneles sobre la evolución de la tecnología del DNS en Bangkok. Vamos a escuchar un poco más sobre la facilitación de la discusión que va a tener ICANN para la mejora de este protocolo en la reunión en Marruecos y también probablemente en otras ustedes van a escuchar un poco más sobre el trabajo de la ICANN.

JOANNA KULESZA: Muchas gracias, Patrick. Tenemos un okey de Abdelmonem. Supongo que esa fue una respuesta satisfactoria. Tenemos cuatro minutos más. Quisiera saber si hay preguntas o comentarios. Siéntanse en libertad de levantar la mano. No he visto ninguna pregunta más en el chat. Si hay algo más que pasé por alto y que ustedes quieran plantear, ahora es el momento de hacerlo. Parece que nuestros participantes están satisfechos con toda la información que se ha compartido. Vamos a avanzar hacia el cierre. Les agradezco mucho por haberse tomado el tiempo y por haber aceptado las dificultades técnicas. Les agradecemos a todos por haberse conectado, por haber participado en este seminario web. Muchas gracias. Le agradecemos también al personal, sin el cual no hubiéramos podido hacer este seminario. También a nuestros intérpretes, que han dado esta interpretación para que haya un nivel más internacional. Les agradecemos. Este seminario web va a estar disponible en la wiki de At-Large. De nuevo, gracias a Glenn por reeditar estas diapositivas que están disponibles gratuitamente online.

Si tienen más pregunta o comentarios pueden conectarse conmigo, con Alfredo, con el personal. Los vamos a guiar incluso más. También esperamos verlos en relación con At-Large. Que tengan un buen día. Hasta luego. Esta llamada finaliza aquí. Este seminario web termina ahora. Que tengan un buen día. Hasta luego.

[FIN DE LA TRANSCRIPCIÓN]