CLAUDIA RUIZ: Buenos días, buenas tardes y buenas noches a todos. Bienvenidos al quinto y último seminario web de los cinco seminarios web para ATLAS III. Hoy vamos a abordar el tema de las cuestiones de ciberseguridad. Nuestro presentador el día de hoy es David Huberman, especialista de participación técnica sénior. No vamos a tomar asistencia. Sin embargo, consideramos la asistencia durante los primeros 10 minutos de este seminario web. Después de transcurridos estos 10 minutos, la participación no será considerada como válida. Si están en el puente telefónico, por favor, únanse a la sala de Zoom tan rápido como sea posible dado que este es un requisito para la participación. Contamos con interpretación en español, francés e inglés.

Por favor, al momento de tomar la palabra mencionen sus nombres para que los intérpretes los puedan identificar en los canales lingüísticos correspondientes y también a los fines de la transcripción. Por favor, recuerden hablar a una velocidad razonable para poder realizar una interpretación adecuada. Todas las líneas estarán silenciadas durante la presentación y podrán tomar la palabra una vez que finalice la presentación. Como ustedes saben, este seminario web se está llevando a cabo en Zoom. Las características son similares a las de Adobe Connect pero para poder utilizar la lista de participantes y el chat les pido que por favor hagan clic en la parte inferior de la pantalla. Solamente van a poder ver la transcripción del chat una vez que se unan a la llamada, no con antelación a esto. Para levantar la mano, por favor, hagan clic en el icono de la mano. Ahora le voy a dar la palabra a Joanna Kulesza, quien es copresidenta del grupo de trabajo para ATLAS III. Adelante, Joanna.

JOANNA KULESZA: Muchas gracias, Claudia. Muchas gracias por participar en la primera edición del último seminario web de ATLAS III en el cual la participación es un requisito para poder asistir a ATLAS III. Sin más, con gusto quiero darle la palabra a David. Él es especialista técnico de participación sénior en ICANN. David, muchas gracias por participar. Vamos a escuchar su presentación. Entiendo que los participantes van a poder realizar preguntas durante la presentación en el chat así que, David, lo dejo a su criterio si usted quiere responder estas preguntas durante la presentación o bien al final de la misma. David, adelante, por favor.

DAVID HUBERMAN: Hola a todos. Voy a dar una presentación bastante breve el día de hoy. Luego vamos a tener suficiente tiempo para hacer preguntas después de que finalice la presentación. Durante la presentación no voy a abrir el chat porque quiero concentrarme en la presentación en sí. Bienvenidos. Hoy vamos a hablar de ciberseguridad y el ecosistema de la ICANN.

Mi nombre es David Huberman. Soy especialista de participación técnica sénior en la oficina del CTO de la ICANN. Estuve al frente de cuestiones de ciberseguridad durante aproximadamente unos 21 años. Este seminario web será un complemento a los cursos oficiales que ya existen en ICANN Learn. Esta presentación es nuestra presentación de los desafíos que enfrenta el ecosistema de la ICANN en materia de ciberseguridad. Además, esto se puede presentar de diferentes maneras y está bien.

Para comenzar, quiero que pensemos lo siguiente. Quiero que pensemos qué elementos encontramos comúnmente dentro de una red. Por ejemplo, en una red de una empresa o en una red de una universidad o incluso en una red gubernamental. Lo interesante que encontramos incluye, por ejemplo, servidores de correo. Los servidores de correo no son solamente para correo electrónico sino que sí tienen correo electrónico pero también tienen calendarios, todas las reuniones que nosotros agendamos, etc. También incluyen nuestros contactos. Es decir, información sobre nosotros e información sobre la gente que pertenece a nuestra red.

Otros elementos comunes son los servidores de bases de datos. Estos servidores de bases de datos contienen mucha información como por ejemplo datos de activos, datos de clientes. A veces incluso datos de los empleados. Otro elemento común en una red son los servidores de archivos. En este caso encontramos toda la información financiera, hojas de cálculo, documentos de diseño y también podemos encontrar información sobre los procesos y procedimientos de la organización.

Esto parece bastante simple pero es información muy útil e interesante que se puede encontrar dentro de las redes. Respaldar estos elementos es algo realmente interesante. Tenemos cuestiones como por ejemplo la gestión de identidad para poder acceder a nuestro correo electrónico, a los servidores de archivos o a las bases de datos. Tenemos que atravesar procesos que nos autorizan al acceso para poder ver los datos, procesos que son autenticadores. Es decir, nos piden una contraseña, un nombre de usuario para proceder con la autenticación, el token de seguridad que necesitamos además de esa contraseña.

Cuando uno administra este sistema también tiene que administrar la clave. El nombre de usuario y la contraseña son importantes pero también la llave criptográfica es importante. También algún otro token secundario que hace que nuestro sistema se mantenga seguro. También tenemos sistemas de ingeniería de sistemas. Tenemos hardware, tenemos software y este hardware y software requiere un patching que esté actualizado. Si ahondamos en estos sistemas encontramos la infraestructura de enrutamiento que tiene que ver con la conectividad interna y externa de nuestras redes. Es decir, fuera de nuestra compañía, fuera de nuestro gobierno o fuera de nuestra universidad. Con esta conectividad y en esta infraestructura se encuentran los elementos clave que son las direcciones de IP y el DNS o el sistema de nombres de dominio.

Finalmente tenemos el componente gubernamental. Es decir, en una política de seguridad quién puede acceder a estos datos y de qué manera se debe acceder a estos datos. También hay una política en materia de almacenamiento de datos, qué almacenamos, dónde lo almacenamos y también retención de datos. Es decir, durante cuánto tiempo se almacenan estos datos.

Al hablar de todo esto lo hacemos porque estos elementos son elementos que constantemente se encuentran bajo ataque por parte de personas que están tratando de encontrar las diferentes vulnerabilidades de todos estos elementos que ven en pantalla. Esto puede comprometer la actividad de estos sistemas.

¿De qué manera lo hacen comúnmente? Esto incluye el phishing o suplantación de identidad. Ahí coloqué una definición de diccionario que

es por cierto muy acertada. El phishing o la suplantación de identidad es la práctica fraudulenta de enviar correos electrónicos pretendiendo venir de una empresa con alta reputación para poder inducir a los individuos a revelar información personal como por ejemplo contraseñas o números de tarjetas de crédito.

Otro tipo de ataque tiene que ver con el malware. En este caso es un software que está específicamente diseñado para corromper, dañar o ganar un acceso autorizado a un sistema informático. Puede ser por ransomware, keystroke loggers, rootkits y los virus. Luego tenemos un tipo más complejo que son los botnets. Un botnet es una red de computadoras privadas que están infectadas con un software malicioso y que están controladas como un grupo. Un botnet puede ser miles o cientos de miles o millones de computadoras en todo el mundo que tienen un control en común y que se utilizan para llevar a cabo ataques.

Un ciberdelito muy importante y del cual hablamos con frecuencia aquí pero también en el ecosistema de la ICANN es lo que denominamos uso indebido del DNS. El DNS está en todas partes. El DNS se utiliza todo el tiempo para resolver nombres de usuarios amigables en relación a las direcciones de IP o de protocolo de Internet. Si se afecta el DNS, se pueden afectar las transacciones comerciales, servicios gubernamentales, redes sociales y muchas otras cuestiones también. Si se explota el DNS, entonces se puede defraudar o engañar a los usuarios. ¿De qué manera se puede hacer una explotación del DNS? A través del registro de nombres de dominio maliciosos, el secuestro de la resolución de nombres o servicios de registración y también se puede corromper los datos que están en el DNS.

No quiero hablar esto de manera [inaudible]. Quiero mostrarles cómo se ve un ataque en el mundo real. Para esto podemos mostrar dos ejemplos de ciberataques o ataques cibernéticos muy recientes. Estos incluyen apuntar a las vulnerabilidades del sistema de enrutamiento de Internet y también a las vulnerabilidades del sistema de correo electrónico. Estos ataques cibernéticos implican mucho uso indebido del DNS. En primer lugar, estos ataques de manera subrepticia alteran la resolución de nombres de modo tal que las víctimas ni siquiera se enteran.

El primer ataque se denominó MyEtherWallet.com. MyEtherWallet.com es un lugar donde la gente puede almacenar sus criptomonedas. Para eso se utilizó un secuestro de direcciones a través de enrutamiento y al hacer esto lo que se pudo hacer es engañar a los usuarios para incluir sus credenciales de registro en un sitio falso. Una vez que los atacantes pudieron ver esta información, terminaron robando aproximadamente 21 millones de dólares en criptomoneda de este sitio determinado.

El segundo ataque muy reciente tiene dos nombres. DNSpionage, que se llevó a cabo a finales de 2018, y un ataque que todavía está en curso que fue detectado por la comunidad técnica que se llama Sea Turtle. Estos ataques no tienen que ver con cuestiones monetarias. Muchos de los delitos cibernéticos están motivados por la obtención de dinero pero estos son ataques distintos porque tienen que ver con el preposicionamiento militar. Es decir, la idea es tomar información miliar para lanzar ataques cibernéticos. Este espionaje tiene unas 40 organizaciones en 13 países en África del Norte y Medio Oriente. Los objetivos son organizaciones de seguridad nacional, ministerios de

asuntos exteriores y compañías energéticas. Esto se hace mediante el infiltrado en el DNS. Se utilizan tokens de validación.

Este tipo de ataques de gran escala son poco frecuentes. Debido a la importancia que tienen o a la extensión o a la infiltración involucran cuestiones como por ejemplo gobiernos soberanos, empresas multinacionales, agencias de cumplimiento de la ley internacionales y también esto tiene una cobertura a nivel general. También hay otros ataques más pequeños o incidentes de ciberseguridad que suceden en todo el mundo todos los días. La comunidad de la ICANN, es decir, ustedes y los miembros de la organización de la ICANN, es decir, los miembros del personal, tienen un rol que cumplir en estas cuestiones o en incidentes de ciberseguridad.

Durante este seminario web vamos a describir la comunidad de la ICANN y el rol de la organización en materia de ciberseguridad en cuanto al ecosistema de la ICANN. Con esto nos vamos a familiarizar con algunos temas clave en materia de ciberseguridad.

Vamos a comenzar entonces con las cuestiones que suceden antes de que ocurra un ataque cibernético. Tenemos los estatutos de la ICANN. La misión de la ICANN pone un énfasis muy particular en la ciberseguridad. La misión de la ICANN es garantizar la operación de los operadores únicos de Internet que sea estable y segura. Esto da incluye varios compromisos. Uno de estos compromisos es preservar y mejorar la administración del DNS y la estabilidad operativa, la confiabilidad, la seguridad, la interoperabilidad global, la resiliencia y la apertura del DNS en Internet.

Tenemos estas palabras resaltadas que son: seguridad, estabilidad y flexibilidad o resiliencia. Estas palabras las van a escuchar en muchas oportunidades dentro del ecosistema de la ICANN. En los grupos de trabajo, en las listas de correo electrónico, en las reuniones, etc. Todo tiene que ver con la seguridad, la estabilidad y la flexibilidad de los identificadores únicos que coordina ICANN. A menudo los conocemos con el acrónimo de SSR. ¿Qué significan estos términos? Son bastante simples. Seguridad implica la capacidad de proteger y prevenir el uso indebido de los identificadores únicos de Internet. La estabilidad es la capacidad de garantizar que el sistema opere como se espera y que los usuarios tengan confianza en que los identificadores únicos operan como se espera. La resiliencia o flexibilidad es la capacidad de los sistemas de identificadores únicos de funcionar efectivamente sin eventos disruptivos y de manera continua.

Al cumplir con nuestros compromisos en materia de SSR, de los identificadores únicos, la ICANN se centra en tres áreas importantes. Una es el desarrollo de políticas, otra tiene que ver con las operaciones de los identificadores y todas las semanas y cada día nosotros participamos en esfuerzos de creación de capacidades para poder informar al público con respecto a las tecnologías y a las tendencias que existen en materia de ciberseguridad.

A través del ecosistema de la ICANN, donde hay tantas comunidades que trabajan para crear comunidades o políticas para mejorar la seguridad, la estabilidad y la flexibilidad o resiliencia, sabemos que hay muchas comunidades que están trabajando. Aquí enumeramos algunas. El GAC tiene un grupo de trabajo en materia de seguridad pública que se denomina PSWG. Este PSWG se encarga de trabajar sobre los aspectos

de políticas y procedimientos de la ICANN. Esto incluye desarrollar las capacidades de mitigación de los ciberdelitos y el uso indebido del DNS dentro de las comunidades de cumplimiento de la ley y de la ICANN.

Además de este grupo de trabajo hay otro grupo que es el SSAC, que es el Comité Asesor de Estabilidad y Seguridad. Este es un grupo que está compuesto por expertos de seguridad e ingenieros que han sido seleccionados para formar parte de un comité y que se encargan de hacer análisis de riesgos y evaluación de amenazas de los sistemas de identificadores únicos para evaluar también cuáles son las principales amenazas a la estabilidad y seguridad de Internet.

Otra comunidad que quiero mencionarles es una más pequeña. Es la de los operadores de servidores raíz. Ellos se reúnen en un comité asesor dentro de la ICANN que se llama RSSAC, que es el Comité Asesor del Sistema de Servidores Raíz. Este comité asesor asesora a la junta directiva y a la comunidad en materia de cuestiones que tienen que ver con la operación, administración, seguridad y la integridad del sistema de servidores raíz que está en la parte superior del árbol del DNS.

Otra parte distinta de desarrollo de política igualmente importante son los contratos. Los contratos entre la ICANN y los registros y registradores, que son herramientas muy importantes. Voy a adelantarme ahora una diapositiva pero después voy a volver. Tenemos muchos contratos en el ecosistema de la ICANN. De izquierda a derecha, abajo vemos que entre la ICANN y el registro de un nombre de dominio de nivel superior se celebra el contrato que se denomina acuerdo de registro. Entre el registro y los registradores, es decir, los registros de nombres para personas, está el acuerdo entre registro y registrador.

Arriba, entre la ICANN y el registrador está el acuerdo de acreditación, cómo se califica y cuáles son las responsabilidades que tiene que tener un registrador. También el registrador tiene contratos con revendedores y con el registratario.

Volviendo a la diapositiva anterior ahora quiero hablar de dos de los contratos más importantes y cuál es la relevancia para los expertos. El acuerdo que celebra la ICANN y el registrador, es decir, que le da la acreditación a un registrador, de hecho impone un deber contractual de investigar el uso indebido cuando el registrador tiene conocimiento de que existe el uso indebido.

El acuerdo entre el registro del TLD y la ICANN incluye una disposición que en el acuerdo entre el registro y el registrador requiere que los registradores incluyan en el acuerdo de registración una disposición que prohíba a los titulares de nombres registrados la distribución de malware, botnet que operen de manera abusiva, phishing, piratería, vulneración de marcas o derechos de autor, prácticas fraudulentas o engañosas, falsificaciones o cualquier otra participación en una actividad contraria a la ley aplicable, que son requisitos contractuales muy diferentes. Estos requieren investigar y prohibir el ciberdelito.

El segundo dominio donde la ICANN cumple sus compromisos es en las operaciones con identificadores. La ICANN tiene una subsidiaria, una afiliada que se llama Public Technical Identifiers, identificadores técnicos públicos. Verán la sigla PTI. La PTI es responsable de los aspectos operativos de coordinación del sistema de identificadores únicos de la Internet y lo hace a través de lo que se llama las funciones de la IANA. Estas funciones tienen tres pilares muy importantes. La primera son los

recursos de números, que tienen que ver con la asignación de las direcciones IPv4, las direcciones IPv6 y algo que se llama los números de sistemas autónomos, los números AS, a los RIR, que son los registros de Internet, que son los que manejan, los que entregan los números y las direcciones a las empresas en el mundo.

El segundo pilar importante que gestiona la PTI son las operaciones del DNS. En este campo hacen muchísimas cosas. Resalté tres. Es el mantenimiento de la zona raíz para los DNS forward. Luego administra la zona .ARPA para el DNS de reversa y algo que es muy técnico que es mantener el anclaje de confianza del DNSSEC. Aquí resalté DNSSEC porque vamos a hablar de DNSSEC para que tengan algún entendimiento básico de por qué hoy día es importante.

La tercera tarea que tiene la PTI es algo que se llama los registros de parámetros de protocolo. El grupo de trabajo de la Internet, el IETF, es un grupo que desarrolla y publica los protocolos básicos de la operación concreta de la Internet. Estos protocolos tienen parámetros. Un protocolo puede decir que el número 1 significa esto, el número 2 significa aquello y el número 3 significa una tercera cosa. Es muy importante definir los parámetros y publicarlos en algún lugar para que alguien los pueda leer. La PTI publica estos registros de parámetros. De hecho existen más de 3.000 que se encuentran en el sitio web de la PTI con todos los distintos parámetros de los protocolos.

Hablemos ahora brevemente de DNSSEC. DNSSEC es la sigla que representa extensiones de seguridad del sistema de nombres de dominio. El propósito del DNSSEC es ayudar a prevenir el uso indebido del DNS y lo hace a través de la introducción de criptografía. Esta

criptografía proporciona garantías a los usuarios del DNS de que los datos que ellos ven son válidos y son verdaderos. Los registratarios de los nombres de dominio, es decir, el dueño del nombre, el que lo corre, firma los datos del DNS. Es decir, dice: “Este es mi nombre de dominio y este es el que he publicado”. Los operadores del DNS validan esa información cuando los datos del DNS pasan a través de los resolutores.

DNSSEC utiliza claves. Esto se denomina infraestructura de clave pública, PKI. Aquí hay muchos términos pero, rápidamente, la clave de firma de la llave, la KSK, es la clave superior, la más importante en cualquier jerarquía criptográfica del DNSSEC. Es un par de clave pública y privada. La pública es la parte confiada. Es la parte en la cual confía toda la comunidad. La parte privada firma la clave privada en su zona. La idea es generar una cadena de confianza, que es una serie sucesiva de claves y firmas que pueden ser utilizadas por cualquiera para validar la autenticidad de cualquier dato firmado por DNSSEC. Al firmar estos datos, al validar estos datos, ayudamos a terminar con gran parte de las instancias de uso indebido posibles. Con todo esto viene el rol de la PTI en el DNSSEC.

La Internet ha encomendado a la PTI emitir, administrar, cambiar y distribuir todas las claves del DNS. Además son los que firman. Firman criptográficamente estos keysets. La PTI lo hace asegurándose de que las mejores prácticas en criptografía que han sido desarrolladas por el IETF, el grupo de trabajo de ingeniería de la Internet, se sigan.

El tercer pilar en el cumplimiento de nuestras obligaciones tiene que ver con la creación de capacidades. Los miembros de la comunidad, el personal de la ICANN, casi a diario participan de manera regular en

acciones de educación de las organizaciones en todo el mundo en temas relacionados con el sistema de identificadores únicos que la ICANN ayuda a coordinar y en ciberseguridad. Lo hacemos para que aumente el conocimiento y la concientización. Se hace de distintas formas, de distintas maneras e incluye webinars como el que estamos teniendo ahora. Cuando se va a las reuniones de la ICANN encontrarán que hay sesiones que en la agenda se llaman “How it works”, “Cómo funciona”. Son aquellas sesiones en las cuales se puede entrar en detalle en las distintas tecnologías para tener una buena comprensión de qué se trata y cómo funciona.

También se hacen talleres técnicos que pueden durar varios días, hasta una semana. Hay muchísima capacitación a los organismos de aplicación de la ley en todo el mundo para que ellos puedan entender estas tecnologías, entender las metodologías que utilizan los atacantes y para que puedan entender cómo podemos ayudar para terminar con el ciberdelito y muchos otros tipos de creación de capacidades.

Esto es lo que pasa a diario en el ecosistema de la ICANN. Esto lo hemos pensado, lo hemos visto desde una perspectiva anterior a un incidente. Veamos ahora qué hace la ICANN cuando ocurre un incidente. Cuando hay un ciberataque lo que queremos hacer es detenerlo. Esto requiere una respuesta grande y coordinada con la participación de varios actores. Estos actores son los operadores de las redes que son los proveedores de servicios o las redes de las empresas o de los organismos que usan los atacantes. Por supuesto, para detener un ciberataque se requiere una respuesta de las agencias de aplicación de la ley mundiales y luego surge esta cosa que se llama CIRTS, que son los equipos de respuesta ante incidentes nacionales, incidentes de

computación, que normalmente están organizados a nivel nacional, por eso son los CIRTS nacionales.

Otra cosa que tenemos que hacer para detener un ciberataque es involucrar a los registros. Los registros de nombres de dominio pero también los registros de las IP, los RIR. Necesitamos la ayuda de los RIR por sus atribuciones, para poder detener un ataque. Tenemos que saber quién está conduciendo el ataque, cuáles son las redes, cuáles son los recursos que se están utilizando en este ataque. Tenemos que saber quién es el registratario de las direcciones IP que están siendo utilizadas en el ataque. También tenemos que saber quién es el registratario de los nombres de dominio que se usan en el ataque. Para poder responder a estas preguntas necesitamos datos de la registración. Los datos de la registración son las fuentes de datos a partir de las cuales podemos hacer atribuciones. Estas fuentes de datos son los registros de registración, con las direcciones IP y los números AS. Estos están ubicados en los RIR, los registros regionales de Internet. Necesitamos los registros de registración también correspondientes a los nombres de dominio.

La organización de la ICANN también tiene un rol de coordinación. Hay un equipo dentro de la oficina del CTO. Cuando ustedes van a las reuniones de la ICANN, cuando están en las listas de mailing, verán que a la oficina de la CTO se la llama OCTO. Esta OCTO trabaja con todas estas organizaciones durante un ciberataque para coordinar las respuestas. Lo hacen porque estos son los profesionales que tienen una comprensión muy minuciosa de lo que es el ciberdelito desde ambas perspectivas, la perspectiva del atacante y del que da la respuesta.

El equipo de la ICANN tiene conexiones muy sólidas con los organismos de aplicación de la ley y algo que es muy importante también con la comunidad de seguridad operativa u OPSEC de Internet que son los operadores de red que están en la línea de fuego de los ciberataques. El equipo de la ICANN utiliza estos conocimientos minuciosos y estas sólidas conexiones con la comunidad para unir a todas las partes cuando queremos concluir o parar un ciberataque. Por separado, en nuestro rol de coordinación se incluye este procedimiento que hemos desarrollado que se llama proceso de divulgación coordinada que es un proceso que cualquiera, un investigador en seguridad, un registro, un registrador, cualquiera en la comunidad puede recurrir a este proceso para reportar vulnerabilidades y bugs. Los reporta a la ICANN para que la ICANN pueda trabajar con todas las partes pertinentes para resolver y emparchar lo que exista en el sistema para impedir futuros delitos.

Una vez que ya pasó todo es hora de ver por qué pasó. Son muchas las cosas que se hacen para saber qué es lo que estuvo mal. La gente analiza las vulnerabilidades que se descubrieron, los bugs que se hallaron. Hacen un poco de investigación, escriben papers e informes. De todo esto se habla en conferencias presenciales, a veces en conferencias virtuales para que todas podamos entender qué pasó y se identifiquen las vulnerabilidades que cada uno tendrá que reparar.

Son muchas conferencias distintas donde esos temas se discuten. Voy a marcarles tres muy importantes. Uno es el simposio de DNS anual que hace la ICANN, donde los expertos más importantes del mundo se reúnen una vez al año para hablar de la relevancia de la ciberseguridad en el DNS. Otra conferencia es la que se llama DNS OARC. Algo muy importante es ese concepto que se llama NOGS. Los grupos de

operadores de redes. Son nacionales, locales, regionales. Son grupos donde las comunidades se han reunido como operadores de red y quieren compartir información, compartir conocimientos y ayudarse recíprocamente para mejorar las redes.

Una vez que hemos hablado sobre el tema, ¿qué pasa? Una vez que hemos identificado los bugs y las vulnerabilidades es hora es hora de ajustar el ecosistema para endurecer, para hacer que la Internet sea más resiliente contra este tipo de ataques. Quizá sean necesarias muchas cosas distintas. A lo mejor es necesario actualizar políticas. Quizá haya que ir al PSWG y al RSSAC, a cualquiera de los grupos para que se elaboren políticas. Se traba en conjunto. Quizá haya que actualizar los contratos, los contratos que existen en el ecosistema, para manejar y mejor y que las personas respondan mejor ante los ciberataques. Quizá tengamos que salir a arreglar protocolos existentes o elaborar protocolos nuevos. Vamos al IETF para compartir nuestros hallazgos y trabajar conjuntos para reparar los protocolos que han quedado expuestos.

Lo más importante siempre es hacer creación de capacidades con la comunidad. Ir afuera, ir con los operadores de redes, con las agencias de seguridad de la ley, con la comunidad para discutir lo que pasó para que todos entiendan muy bien qué es lo que está pasando y qué tenemos que hacer. Hay algunos mensajes a destacar, esenciales, de todo lo que hemos hablado. El primer mensaje es que el DNS realmente importa. Esto puede sonar gracioso porque el DNS es una tecnología muy importante pero es importante pensar que el DNS no es solo una función técnica. Ya no lo es. Ya no es esa cosa que algunos administradores de sistema, algunos ingenieros detrás de bambalinas

cuyos nombres ni siquiera conocemos configuran para correr una red y que ni les prestamos atención. Es mucho más grande que eso.

El DNS hoy día es una infraestructura crítica que se usa en todas partes, email, web browsing, aplicaciones móviles, bancos, en todo. El DNS hoy día es la puerta de entrada a todos los sistemas internos. Los sistemas que hablamos al comienzo del webinar, email, las bases de datos, los servidores, los servidores de archivos, uno puede intentar protegerlos todo lo que quiera, no hay problema, pero si se deja el DNS abierto, si el DNS está comprometido todos los sistemas, todas las redes están en riesgo. Es crítico entonces. Los que hacen las políticas, los que hacen las políticas organizaciones tienen que prestar mejor atención a la infraestructura del DNS.

La ICANN tiene algunas recomendaciones muy firmes al respecto. Nosotros publicamos medidas de ciberseguridad para endurecer la infraestructura del DNS local contra los ataques. Hay varios pasos que no voy a detallar pero los pasos son autorización, autenticación, es decir, que sea mejor y más fuerte, el uso de encriptación, el patching, que el hardware y el software estén realmente actualizados. Es muy crítico endurecer la infraestructura, fortalecerla. Hay un paso muy importante que tiene que ver con la seguridad del email. Después de todo eso no les va a sorprender que les digo que una de las recomendaciones más importantes que hace la ICANN y que es muy, muy crítica es la implementación de DNSSEC. Los procedimientos de firma y validación con DNSSEC paran muchísimo del uso indebido de la infraestructura del DNS para proteger el sistema.

El último punto tiene que ver con el concepto general de la estabilidad, seguridad y resiliencia de Internet y la ICANN porque la ciberseguridad es un área en la que se centra la comunidad de la ICANN y la organización de la ICANN. La ICANN define el ciberdelito para incluir cuestiones como por ejemplo la distribución de malware, intento de suplantación de identidad o phishing, botnets que operan, piratería, prácticas comerciales engañosas o fraudulentas.

El tiempo y el esfuerzo que dedicamos en la ICANN tanto a los miembros de la comunidad como al personal, todo este tiempo contribuye y el trabajo que se realiza tiene como objetivo incrementar la estabilidad, la seguridad y resiliencia o flexibilidad de Internet y de sus sistemas de identificadores únicos. Ahora sí. Los invito a que hagan todas las preguntas que tengan en este momento.

JOANNA KULESZA: Voy a ver el chat. Tenemos tres preguntas al final del chat. Si no las puede ver, con gusto las puedo leer yo.

DAVID HUBERMAN: A ver, voy a ir desde abajo hacia arriba. El DNSSEC render AXFR. Así que el DNS es más rápido y es un recurso para Hungría. Esa es una decisión que deben tomar. Deben decidir si quieren aceptar o soportar AXFR o no. Fuera de esas razones es una recomendación importante que implementen el DNSSEC para que los registratarios dentro del TLD firmen sus nombres de dominio o sus datos del DNS o los datos de todo el mundo y que se pueda validar esa información. Aquí hay dos

cuestiones distintas. Creo que AXFR depende de una cuestión más individual.

La segunda pregunta tiene que ver con lo siguiente. ¿Por qué hay un incremento en amenazas de ciberseguridad a pesar de toda la seguridad que está implementada? Hay muchos motivos. El objetivo principal es obtener dinero. Alguien puede querer obtener dinero chantajeando a alguien. Hay gente informática, gente muy inteligente, ingenieros que son creativos y que han creado formas intrusivas para poder efectuar ataques cibernéticos. Eso lo hacen porque se pueden esconder detrás de una computadora sin dar sus caras o sin mencionar sus nombres. Este tipo de actividad les da cierto poder a las personas para hacer cosas que no harían cara a cara. Una de ellas es robar dinero. Hablamos de DNSpionage. Este fue un ciberataque. Aquí hay actores gubernamentales que están utilizando esto contra otros actores gubernamentales por cuestiones políticas. Ya podemos darnos cuenta de cuán apasionadas se pueden tornar algunas personas en materia de política.

Acaba de surgir otra pregunta de Vanda. ¿Con cuánta profundidad se debe implementar el DNSSEC? El DNSSEC se implementa en dos o tres áreas. En primer lugar está habilitado por un registro. Es decir, el registro es responsable del dominio de alto nivel. Cuando este dominio de alto nivel está firmado por el operador de registro, esto permite que todo el mundo que tiene un nombre de dominio en ese TLD pueda utilizar su propia validación. Esto está habilitado por el operador de registro. Una vez que esto se hace, cada registrador del nombre de dominio debería firmar los datos del DNS. El tercer punto es que todo el mundo, los que no tengan que ver con el TLD, todos los que quieran operar un resolutor

recursivo que obtengan datos del DNS de otras partes del mundo tiene que implementar DNSSEC. Cada vez que se firma el DNS o hay una respuesta del DNS que llega a un resolutor y que tiene que ser pasado a un usuario final tiene que validarse para saber cuál es el uso final que se le va a dar.

Otra pregunta es cuál es la responsabilidad de los registratarios en cuanto a un usuario que está comprometido o atacado o si ese proveedor de servicios de alguna manera penaliza a estos usuarios. En realidad es la persona que es el dueño del nombre de dominio, como por ejemplo, ejemplo.com. No sé cuánta responsabilidad tienen en este debate en sí si hay un usuario que es atacado o si hay un nombre de dominio comprometido. Este compromiso a menudo se da en un nivel incluso superior que no tiene que ver con el registrante. A veces se da a nivel del registrador. A veces se da a nivel del registro o en otros niveles. No siempre hay relación entre los registradores y los registros o los registradores y la ICANN. A veces se tornan más vulnerables para ser atacados. Todo lo que está por encima de los registratarios, en este caso no tienen gran responsabilidad en este debate.

La pregunta viene de Lutzy es si el DNSSEC puede ser responsable para los ataques de amplificación o reflexión distribuida y si hay alguna idea más allá de un BCP38. Los ataques de reflexión o de amplificación suceden debido a las vulnerabilidades que están dentro del sistema. El DNSSEC tiene que ver con la validación de los datos del DNS para garantizar que sean exactos. No sé si el DNSSEC tiene responsabilidad en esto pero para evitar los ataques de reflexión o de amplificación hay otras prácticas que se pueden implementar. Si hay alguna otra idea más allá de este BCP38, habría que pensarlo realmente. La buena higiene es

importante más allá de filtrar información o filtrar el tráfico que entra. También es importante solidificar o hacer sólidos los sistemas a nivel interno para evitar este tipo de ataques. Hay bastantes cuestiones a tener en cuenta. Es una buena pregunta.

Se pregunta si hay otros esquemas de seguridad que ofrezcan mejores políticas de seguridad más allá del DNSSEC. El DNSSEC es una herramienta en realidad que nos permite proteger los datos del DNS y muchos de ustedes como usuarios del DNS simplemente dicen: "La respuesta que obtengo es la que esperaba" pero hay otros esquemas de seguridad y otras políticas de seguridad que los operadores de DNS o los operadores en general tienen que aplicar. Hay firewalls, hay políticas para realizar el filtrado de información. A veces no son solamente esquemas sino que también hay mucha cuestión o herramientas de enrutamiento que están disponibles para los operadores para que puedan mejorar o brindar una mejor seguridad contra los ataques a los usuarios.

David Mackey dice: "Como miembro de NARALO estoy interesado en la perspectiva no técnica de los usuarios finales. ¿Qué cosas tendría que tener en cuenta los usuarios finales con respecto a la seguridad y si debería haber alguna seguridad para los usuarios finales?" Esta es una muy buena pregunta. En realidad, en el contexto en el que estamos debatiendo hoy los usuarios finales no tienen mucho control sobre estas cuestiones pero sí hay algunas cosas que podemos hacer para ayudar a protegerlos para que no sean parte del problema o víctimas. Uno de los mayores problemas dentro de Internet en el día de hoy son los botnets y los botnets se componen de computadoras que están comprometidas, por ejemplo, una computadora personal en una casa, el teléfono. Todos

estos dispositivos se pueden comprometer y ser utilizados como parte de un botnet y después pueden ser utilizados para atacar a ciertas instituciones. Creo que para un usuario final es importante que no se instale software o programas que no se conocen. Es importante entrenarse para no ser víctima de un ataque de phishing. El ataque de phishing o suplantación de identidad es uno de los principales tipos de ataques que sufren los usuarios finales. Se infectan con malware las computadoras. Es decir, hay diferentes prácticas que hacen que extraños puedan tomar control de nuestra computadora. Pueden ser sitios web falsos donde ingresamos nuestros usuarios y contraseñas.

Tiene que ver con ser inteligentes o hacer un uso inteligente de estas cuestiones de ciberseguridad y ser muy cuidadosos con respecto a lo que uno permite el acceso en un dispositivo. Esa sería la primera respuesta a su pregunta. Hay otras. También tiene que ver con demandar mayores medidas de ciberseguridad por parte de nuestros proveedores. Por ejemplo, que se pueda hacer un informe a los gobiernos o a las universidades o empresas para las que trabajamos. Cuando se ve algo, se detecta algo, es importante reportarlo o informarlo.

Bien. Aquí tenemos otra pregunta importante. Si la cadena de delegación puede soportar un ataque. Si lo diseñan bien, si son un operador de registro o registrador o un revendedor incluso y piensan de qué manera están construyendo sus sistemas, si lo hacen correctamente, si se comunican con las diferentes partes y si se mantienen actualizados entonces sí van a poder soportar el ataque pero no es sencillo y creo que esto también está implícito en la pregunta. No es algo sencillo porque los ciberdelincuentes son muy inteligentes, son

muy buenos en lo que hacen. Tienen que ser realmente muy, muy buenos.

Hay otra pregunta que tiene que ver con las técnicas de encriptado de mensajes y si esto ayuda a luchar contra el phishing o el malware. Probablemente. La encriptación es algo útil o interesante de utilizar pero creo que lo mejor es proteger de mejor manera nuestra privacidad. Quizá alguien puede obtener copia de los mensajes que hacemos pero si esto está encriptado entonces me parece que tiene que ver con brindar o proveer protección a la privacidad. ¿El encriptado ayuda a luchar contra el phishing o la suplantación de identidad y el malware? No lo sé. Es una buena pregunta.

Nos quedan algunos minutos de nuestro seminario web. No sé si hay alguna otra pregunta. Con gusto la voy a responder. Joanna hace una pregunta. "¿Estaría dispuesto a compartir sus puntos de vista en materia de atribución de ciberseguridad con el WHOIS o una vez que el WHOIS no esté?" Lo único que voy a hacer es dar mi opinión. Es mi opinión personal, no en representación de la organización de la ICANN. Voy a hablar como ingeniero. El WHOIS ha estado disponible durante mucho tiempo y ahora hay cosas que no están disponibles. No todo pero hay parte del WHOIS que no está disponible. Creo que la conclusión por sentido común es que esto de alguna manera reduce la capacidad de los que tienen que responder para determinar qué sucede.

Si uno comienza a investigar un ataque verá que hay diferentes tipos de información que no se han ocultado en el WHOIS como por ejemplo la dirección de IP. Están registradas en algunas organizaciones o ISP y esta información siempre está disponible en el WHOIS. Hay información

técnica que está en el sistema de números autónomos. Esta es información técnica. Hay números que no están escondidos sino que son brindados básicamente. Hay muy buenos ingenieros que pueden ver esta información básica de la atribución pero fuera del WHOIS hay que recurrir a estos operadores de redes y preguntarles. A ver, esta dirección de IP fue utilizada en esta ocasión para hacer algo. ¿Nos podría por favor ayudar a descubrir quién fue? Si es un gobierno, uno tiene que decir: "Aquí hay una orden judicial para cooperar". Probablemente todo esto enlentezca las cuestiones. Esto enlentece algunas cuestiones pero no tiene que ver directamente con el proceso de atribución. Hay que ir en otra dirección.

Vamos a tomar una última pregunta que acaba de traducir Claudia. "¿Puede la ICANN tener un centro de documentación para efectos de mantener informados a los miembros de diversas comunidades como por ejemplo técnicos, ingenieros, organizaciones, usuarios?" Sí. En el sitio web de la ICANN hay mucha información y entiendo que puede ser difícil encontrar esta información. Pero si ustedes van a icann.org/technology, que pueden incluso ingresar ahora, van a ver que hay muchos recursos publicados y también pueden obtener cierta documentación. También acceder a otros links muy útiles con esta documentación que los pueden ayudar. Sí, por supuesto, nosotros lo hacemos como miembros de la comunidad. Mis colegas y yo y también los miembros del personal de la ICANN siempre nos comunicamos con toda la comunidad, con NARALO, con los usuarios finales… Gracias, Claudia. Con los creadores de políticas que participan en los grupos de trabajo y también en los comités asesores, en teleconferencias, mediantes correos electrónicos, en reuniones presenciales y con

ingenieros. Una de las cosas que yo hago por ejemplo es ir a los diferentes grupos de operadores de registros, de ingenieros y hablar con ellos y ver qué está sucediendo. Eso sería todo de mi parte. Les agradezco nuevamente a todos.

JOANNA KULESZA: Gracias. Ha sido muy informativo esto. Les agradezco por el tiempo dedicado. Ha sido una presentación muy informativa. Quiero recordarles que esta presentación va a estar disponible una vez que finalice el seminario web. Va a estar disponible en la página wiki de At-Large. Para ustedes, para los que todavía quieren tener más información sobre ciberseguridad habrá otra edición del seminario web mañana. Esto es el 22 de mayo, miércoles, al mediodía. Patrick Jones será el encargado de presentar este tema nuevamente. Aproximadamente será dentro de 12 horas.

Muchas gracias, David. Gracias a todos los que han participado. Gracias por tomarse el tiempo. Gracias a nuestros maravillosos intérpretes y al personal que siempre nos ayuda. Por favor, siéntanse libres de contactarnos si hay más preguntas o cuestiones que quieran preguntar con respecto al seminario. Voy a detenerme aquí. Agradezco a todos. Gracias, David. Que disfruten el resto del día.

[FIN DE LA TRANSCRIPCIÓN]