TORONTO – Panel de Expertos sobre la Seguridad de ICANN (Foro sobre Abuso del DNS)
Lunes, 15 de octubre del 2012 – 13:30 a 14:45
ICANN - Toronto, Canadá

BRAD WHITE: Vamos a comenzar. Queremos que esta sesión sea un poco diferente de las otras sesiones que han -- de las cuales han participado en la ICANN. Queremos que sea una sesión tranquila, flexible, interactiva, es decir desestructurada, con mucha participación. Eso es lo que queremos lograr aquí hoy. Tenemos un panel excelente, un panel inigualable.

Tenemos a Jeff Brueggeman, Vicepresidente de políticas publicas de AT&T, el coordino y desarrollo las posturas de políticas de AT&T para Internet y tecnología. El lidera las iniciativas de política estratégica de la empresa AT&T como por ejemplo computación en la nube (cloud computing) y seguridad en Internet.

Sigue el Doctor Stephen Crocker, Presidente de la Junta Directiva de la ICANN y co-fundador de Shinkuro Corporation que se encarga de mejoras de seguridad en Internet, también del DNSSC. Stephen es un pionero de la Internet quien colaboró con la creación de los protocolos del Arpanet, que son los cimientos de la Internet como la conocemos hoy.

Junto a él tenemos a Jeff Moss, nuestro Vicepresidente y principal ejecutivo de seguridad. En 1992 fundó la comunidad más importante a nivel mundial en este tema. Luego comenzó Black Hat y ha liderado conferencias en temas de seguridad. El fue designado como miembro del departamento de seguridad interna de los Estados Unidos. ¿Es así esto, Jeff? Tiene una biografía muy extensa, tuve que resumirla para poder presentarlo.

Luego tenemos a Debbie Monahan, quien se encarga del CCTLD. NZ de Nueva Zelanda y la supervisión del espacio de estos nombres de dominio. Se encarga de la autorización de políticas para la autorización de los registradores que supervisan a los registratarios.

Luego tenemos al famoso Dan Kaminsky, quien es un famoso investigador en el área de seguridad. Ha asesorado compañías como Cisco y Microsoft, que forman parte de la lista de empresas de Fortune 500 o las 500 empresas líderes en la revista Fortune. Él lidero lo que paso a ser la solución más importante para un problema de Internet en todos los tiempos.

Y luego tenemos al Doctor Paul Twomey, anteriormente Director Ejecutivo de la ICANN. Es Director de Argo Pacific, una consultora de nivel internacional que ayuda a gestionar tecnologías de Internet para uso comercial. El fue nuestro Director Ejecutivo desde el 2003 al 2009. También lidera el Consejo de la Agenda global del Fondo Económico.

Así que como les dije tenemos a un distinguidísimo panel y queremos que esta sesión sea lo más desestructurada posible. Yo voy a formular las primeras preguntas, pero cuando ustedes estén preparados, por favor acérquense al micrófono y formulen las preguntas. También tenemos a Margie a cargo de los participantes remotos.

Stephen, exactamente ¿cual es el rol de la ICANN respecto de la seguridad?

STEPHEN CROCKER: Me encantan estas preguntas tan breves y concisas. Me estoy tomando una pausa porque estoy tratando de buscar una definición y no solamente decir que se trata de A, B o C. El rol de la ICANN en la seguridad deriva de su misión de

coordinar los identificadores únicos de Internet que son códigos que incluyen, pero no se limitan, al sistema de nombres de dominio y sobre todo al nivel superior de DNS. Esto comprende también las direcciones y los números del sistema autónomo. También la publicación de los protocolos y parámetros de la IETF. Y también participamos en el mercado junto con los gTLD registros y registradores, de estos gTLD para ver que se realice esta operación de gTLD de manera precisa.

La seguridad abarca muchas cosas. La seguridad en Internet según mi experiencia, no es un termino lo suficientemente preciso porque incluye desde la suplantación de identidad (phishing), a la extorsión, espionaje y otra variedad de malas acciones. Por ejemplo, los correos electrónicos no deseados para infringir o invadir la privacidad de las otras personas. Ese es un tema de seguridad y nuestra misión es muy acotada al respecto. Nosotros nos preocupamos mucho por la estabilidad de las operaciones del servidor raíz, y nos preocupamos mucho más porque queremos ver que la información en la zona raíz tenga calidad y exactitud, y esa es un área muy, muy acotada.

Nos importa mucho también la operación en general del sistema de nombres de dominio por eso respaldamos mucho la DNSSC. Y desde el punto de vista del consumidor nos ocupamos mucho de las operaciones, de los registros y registradores para que haya una cantidad acotada de abuses y fraudes en este campo. Pero Mark te puede decir más al respecto.

BRAD WHITE: Jeff, usted ha dicho cuando comenzó esta sesión, estábamos conversando y usted me menciono que quizás haya una desconexión entre el rol y la misión de la ICANN y el rol de la seguridad del DNS.

JEFF MOSS: En el ICANN siempre respaldamos mucho a la comunidad en todas nuestras acciones. Como dijo el S-S-R-R-T, nosotros tenemos un punto de vista sobre el rol de la ICANN en cuanto a la S-S-R y estamos listos para publicar el informe con toda la retroalimentación de la comunidad. La ICANN tiene un punto de vista de lo que es su rol a nivel interno, y los miembros de la comunidad tienen otros puntos de vista al respecto.

Entonces, cuando se dice que la ICANN coordina globalmente el sistema del DNS, hay que ver que significa la palabra coordinar. Porque si hay un país que no tiene servidores raíz y hay una interrupción en su servicio, usted quizás quiera recurrir a la ICANN al respecto porque son los coordinadores globales. Si uno habla con los operadores de la zona raíz, este problema no termina en la ICANN sino que termina en los operadores de la raíz.

Con lo cual, cuanto mayor claridad, mejor será esto, no solo para la ICANN sino para la comunidad para poder entender cuales son las expectativas. Y creo que una mejor y mayor atención de los gobiernos permitirá que nosotros podamos clarificar esto y evitar ambigüedades no solo para el GAC, sino para todo el mundo.

BRAD WHITE: Usted y yo hablábamos acerca de los fra -- hablamos de algo que sucedió en febrero de este año, y usted dijo que cuando se publicó esa amenaza muchas personas dijeron, bueno, tenemos que llamar a Internet.

JEFF MOSS: Sí hay un gobierno que -- hubo un gobierno que levanto el teléfono y dijo, por favor quiero hablar con Internet. Entonces para ellos, en su mente, ICANN era Internet. Así que -- porque nosotros somos conocidos como los coordinadores globales entonces ellos pensaron que nos tenían que llamar a nosotros. Yo hable con uno de los operadores en la raíz y me dijo "que interesante". La verdad, no los envidio para nada porque ustedes han plasmado por escrito que son los coordinadores y yo no.

Entonces lo único que tengo que hacer es lo mejor que puedo para mantener mi servicio operativo. Pero, si no lo logro, voy a intentar lo mejor que pueda. Si ustedes no lo logran, eso esta escrito en sus documentos, no en los míos. Así que yo me puse a pensar y dije "que situación interesante".

BRAD WHITE: Paul, desde que usted fue Director Ejecutivo, ¿ha visto usted preocupaciones de seguridad respecto de la ICANN y preocupaciones -- cambios, en las expectativas al respecto?

PAUL TWOMEY: Primero quiero retomar lo que dijo Jeff. Creo que desde que existe la ICANN la interacción con los operadores del servidor raíz ha sido una relación de cooperación y participación. Creo que los operadores de la zona raíz han entendido al menos cual era la intención del gobierno de los Estados Unidos en los comienzos. Entonces ellos han realizado una buena coordinación y celebro este nuevo mandato y celebro el acercamiento de los operadores de la zona raíz a la ICANN.

Primero por las razones mencionadas por Jeff, pero la realidad es que esta parte de la infraestructura debe ser una suerte de termino abarcativo en el cual todas las partes interesadas puedan participar incluso si hay una crisis. Y creo que todas las partes interesadas tienen que ver que significa la flexibilidad en dicho espacio.

Entonces hay una pregunta para comentario público que tiene que ver con una transición en la ICANN para que los operadores de la zona raíz participen en esto. Yo creo que definitivamente ellos deben participar.

JEFF MOSS: Nosotros hablamos muchas veces de lo que sucede en caso de una emergencia.

BRAD WHITE: Usted aparentemente tiene la percepción de que esto va a suceder.

JEFF MOSS: Creo que esto ya ha sucedido dos veces anteriormente, no hubo un procedimiento. Creo que una instancia fue la adquisición de otra compañía. Entonces en el futuro, uno se puede imaginar otra situación y que pasa si uno por ejemplo decide retirarse o jubilarse, ¿qué hace? Recurre a la ICANN, al eBay, ¿qué sucede con todo esto, entonces? Seria bueno tener cierta claridad y poder predecir esto.

BRAD WHITE: Debbie, desde su punto de vista, ¿cuál es el rol de la ICANN en seguridad?

DEBBIE MONAHAN: Bueno, la ICANN no tiene un rol operativo con respecto a los ccTLD. Entonces, lo que nosotros procuraríamos es que haya una coordinación y al respecto la ICANN puede involucrar a todas las partes interesadas y brindar ciertos documentos orientativos que los ccTLD puedan utilizar. Porque en definitiva, ellos son responsables por los ccTLD en los países.

Con respecto a los servidores raíz, nosotros tenemos un acuerdo con la ICANN que incluye que la ICANN nos garantice la seguridad y estabilidad en tal respecto. No tengo un documento al cual recurrir, pero creo que uno de los roles de la ICANN es tener procesos documentados de cómo se administran los ccTLD. Y nosotros también tenemos que compartir parte de nuestro material porque operamos en el mismo espacio y queremos que las partes interesadas claves participen.

Entonces, no tienen un rol operativo en la administración de punto nz, pero creo que nosotros utilizamos la base de datos de la IANA y nosotros al respecto hemos implementado soluciones. Entonces creo que concienciarnos, alertarnos, creo que eso esta bien pero nosotros nos administramos nosotros mismos.

BRAD WHITE: Dan, quiero escuchar su perspectiva respecto de la amenaza que usted ve en este momento para el DNS.

DAN KAMINSKY: Hay muchas personas que quieren complicar al DNS últimamente, no solamente los hackers. Me preocupan mucho los ataques de denegación de servicio contra la estructura del DNS. Los hemos solucionado durante décadas, y ahora, los que están en el otro bando también están teniendo problemas y esto es una -- esta

escalando este problema y es una suerte de carrera armamentista. Yo veo que están creciendo los ataques de denegación de servicio de modo exponencial. Pero también veo que hay un compromiso o una solución de compromiso de los registradores y los registros.

Estoy comenzando a ver que hay mucha fuerza que se esta aplicando en una escala tal con la cual no estamos conformes, pero se desea en gran medida la independencia en el DNS. Y quizás otras personas puedan recibir información si así lo quieren, pero este es nuestro espacio. Y funciona hasta tanto uno tenga actores que tienen un poder sorprendente para actuar en ese espacio y llegado ese punto uno tiene que hacer que retrocedan estos actores. Y es allí donde interviene el rol de la ICANN. Necesitamos organización, coordinación.

La respuesta a la amenazas de anónimos, como le dije ayer, implica una amenaza al DNS. Y quizás eso es lo más valioso que hizo anónimos en toda su vida. Fue como una vacuna, no hubo ninguna amenaza en si, pero sí creo una respuesta de inmunidad porque hubo una amenaza que no lo era de verdad o efectivamente, pero el DNS respondió. Así que sí veo amenazas significativas, pero también hay voluntad de responder a esas amenazas por parte de un grupo coordinado. Así que esta es mi opinión al respecto.

BRAD WHITE: Bien, hablemos acerca de la coordinación. Cuando yo empecé a trabajar para la ICANN teníamos una amenaza de Conficker. Realmente se pensó en como combatir esa amenaza. ¿Ese es un modelo de defensa?

DAN KAMINSKY: Creo que no hay ningún otro modelo, nosotros tenemos que trabajar juntos. La envergadura de las amenazas actuales está en un orden de magnitudes mucho mayor que el que veíamos originalmente. Debemos trabajar juntos para solucionar estas cosas como conficker y los ataques que estamos recibiendo. No hay ninguna organización, registro o registratoria de manera individual que pueda abordar esto de manera individual. Y esas coordinaciones deben fijarse antes del ataque.

JEFF MOSS: Entonces, ¿qué va a hacer usted cuando sucedan estos ataques? ¿Estas cooperaciones van a funcionar cuando haya otros ataques? ¿Qué pasa con esta situación?

Cuando surgió la amenaza de anónimos uno decía, bueno ¿cuál es el flujo mayor que se haya visto? Teníamos en aquel entonces 132 Gigabytes, entonces los ataques de 212 Gigabytes tuvieron lugar la semana pasada contra Wall Street. Entonces, en menos de un año tuvimos este incremento y a mi no me gusta esto y no se como nos defendemos en contra de esto salvo que tengamos mucho, mucho, mucho ancho de banda, porque si esto sigue aumentando vamos a estar en problemas.

Y algunos operadores de TLD tienen a todos sus servidores en un solo país, e incluso en un solo sitio para que cuando se suma todo ese trafico en su país o en su locación, ubicación, ya es demasiado tarde. Hay que localizar todo esto lo más lejos de casa que sea posible. Así que me gustaría ver una estrategia unificada de coordinación para limitar estos flujos de 200-300 Gigas.

ERNIE DANIELS: Nos preocupan un poco los ataques al DNS, pero hay algunos factores adicionales que empiezan a jugar allí y uno de ellos conocido o usado en el pasado es que al principio el servicio de DNS se ofreció debido a una falla que apareció y entonces la solución a eso fue poner un patch al TCP/IP y esa estrategia ha sido mucho más difícil con el enfoque de abajo hacia arriba porque es muy difícil identificar a todas las maquinas de los clientes que tienen un patch, o un parche, y enfrentar eso y saber eso puede tomar cierto tiempo.

Creo que hay otro factor del cual yo no estoy muy consciente hasta que punto de vista se abordo y que va más allá de una falla en el sistema que uno pueda llegar a reparar, tiene más bien que ver con el diseño del protocolo. A medida que se va utilizando el protocolo, uno puede ir teniendo una reflexión de una gran magnitud más allá del aporte. Y se que no estoy muy seguro cuales son los otros protocolos que puedan tener esta falla subyacente, ya sea que es conocida o que todavía no se descubrió.

Mi pregunta es qué es lo que va a suceder en la industria y como se van a buscar estrategias para enfrentar el servicio de denegación que no sea simplemente emparchar cosas, sino más bien enfrentarse con las cuestiones de diseño y los protocolos.

DAN KAMINSKY: El DNSC no es particularmente seguro en su implementación. Ha habido algunos reclamos, pero lo que hemos visto en el campo es que cuando la amplificación ocurre, no siempre involucra al DNS, es decir no es estrictamente DNS. A fin de cuentas, nosotros -- nuestra reparación a las denegaciones de servicio tienen que ver con que tengamos más ancho de banda. Quizás nosotros tenemos dinero y ellos no, quizás hay una fuerza bruta en este problema.

En el punto en el que llegamos a flujos de 212 Gigabytes, la fuerza bruta no tiene una escala suficiente y este es el tipo de cosas que yo estoy viendo que va a suceder en la próxima década. Nosotros tenemos muchas soluciones con las cuales estamos cómodos, pero no todas ellas funcionan en una orden de magnitud de cuatro, cinco, seis veces mayor a la que habíamos diseñado.

Entonces la pregunta es, vemos que los protocolos se rediseñan, que las redes se rediseñan, si eso lo vemos, lo vamos a ver que sucede a nivel técnico pero también sucede a nivel de la política. La gente tiene que estar de acuerdo en que tenemos que analizar las cuestiones interesantes que suceden como, qué hacemos con el trafico espumeado, o cuáles son los protocolos requeridos para validar lo que se comunica con un par, hasta que punto están bien comunicados con un par, como esta en un bond.net y el ataque efectivamente controla a varios millones de maquinas.

Una de las cosas más interesantes que suceden es que hasta hoy todavía no sabemos que estaban tratando de hacer. Sabemos que lo dividieron en unas cuantas cosas. Sabemos que se mantuvieron agarrados a eso lo más fuerte que pudieron. Pero, ¿qué estaban haciendo? Todavía no lo sabemos.

STEPHEN CROCKER: Estoy de acuerdo con todo lo que ha dicho Dan en el sentido de que ha reflexionado sobre hay cuestiones que no depende del DNSC en si solo. Lo que subyace todo esto es el mecanismo de -- que tiene que ver con la reflexión de estos ataques y las direcciones falsas. Hay paquetes que se envían hacia la red y hay un resolutor del DNS con una dirección de retorno ficticio. De hecho, una dirección de retorno es el objetivo que nosotros tratamos de atacar sin importar quien sea el que la envía.

La mitigación de esto, la reducción de esto es chequear las direcciones fuente a medida que van entrando para que el ISP pueda utilizar algún usuario o alguna maquina que esta utilizando un paquete que no se sabe muy bien de donde viene y que lo vemos descrito como un documento donde hay unas mejores practicas, el numero 38. Y hay una gran atención, no tanto como la que quisiéramos, pero hay una atención en tratar de implementar esto en todos los ISP. Creo que una de las cosas que va a llamar más bien la atención, va a ser una evaluación de donde estamos en ese proceso y hasta que punto es efectivo o no lo es.

JEFF MOSS: Ciertamente no tengo nada que decir sobre lo técnico, pero quiero decir que esto también esta creando cuestiones políticas, de las cuales todos tenemos que ser conscientes. Y en el peor de los casos, un deseo del gobierno de que Internet funcione mejor y que los problemas se solucionen esta allí. Queremos asegurarnos de que ICANN tenga en cuenta su rol. Nos preocupa que los gobiernos y en particular la caber-seguridad se conviertan en un problema en nuestro radar. Y no entender que es lo que sucede hoy y buscar más un rol de gobierno en esto, es lo que nosotros estamos viendo que esta sucediendo en término de las asociaciones publico-privadas.

Estamos luchando con todas las cuestiones técnicas y hasta cierta medida también esta es una oportunidad para mostrar la falta de control centralizado, y no la falla, sino más bien los beneficios de la forma en la que esta diseñada Internet. Y creo que ICANN tiene un rol crítico, fundamental, en ayudar no solamente como coordinador formal sino como un órgano importante que trae la experiencia técnica a todos los operadores que están en la infraestructura de modo que pueda ser útil.

PAUL TWOMEY: Hay una frase muy antigua…y una de las cosas que a mi más me preocupa esta semana es que el Secretario de Defensa de Estados Unidos hace tres días habló sobre unas alertas bastante claras de los países que tienen una infraestructura critica. Yo creo que es bastante urgente, francamente, que la comunidad de ICANN en términos generales, pueda definir ampliamente y trabajar en el modelo de múltiples partes interesadas en torno a cuestiones como el servidor de raíz, los operadores. Y el hecho de que el servidor de raíz no tenga ningún cambio potencial. Todas las cuestiones que puedan aparecer con el DNS. Los comportamientos de los registradores y el cumplimiento que puede llagar a tener.

Y hay que tener muy en claro cuales son los roles que tienen que aparecer aquí porque ICANN esta muy preocupado porque podemos encontrarnos en una situación en la que van a aparecer conflictos offline, que van a ayudar a que ocurran conflictos online.

Y nosotros estamos muy preocupados también por el contenido. El ciberespionaje y el ciberconflicto generan que sea muy importante tener una infraestructura de red. Y lo que a mi me preocupa es que el modelo de ICANN y el modelo de la comunidad es de múltiples partes interesadas y de transparencia. Por eso tiene que prestarse mucha atención a este asunto para prevenir una crisis, porque no queda muy claro cuando va a suceder una crisis.

BRAD WHITE: Me preocupa lo siguiente, usted dijo que el conflicto convencional puede aparecer a partir de un conflicto online, son específicos del DNS. Y por eso yo creo que es importante entender esto y veo que hay países que tienen uno solo

uplag y si esto no funciona, el país no funciona y queda desconectado. Por eso yo creo que es muy importado entender y distinguir entre lo que se relaciona con el DNS y lo que no se relaciona con el DS y que tiene más bien que ver con la infraestructura en si. La infraestructura esta en el cableado, digamos.

Cuando hablamos de estos ataques, estamos hablando de que no podemos garantizar que todas las calles en África sea fácil manejar ahí igual que como una autopista en Estados Unidos. Y por supuesto, va a haber casos en los que uno no pueda llegar a ese lugar en África a través de Internet. Y obviamente debemos de entender qué es el DNS, qué no es DNS y qué es lo que tiene relación con el GAC. Es un paquete de Switch. Cuando hablamos de un ataque de DDOS nadie sabe muy bien de que estamos hablando.

Y si estamos hablando por ejemplo del día de Navidad y todo el mundo llama por teléfono a su familia, solamente el 10 por ciento se conecta, entonces ahí es un ataque de DDOS. Pero el 90 por ciento no puede conectarse porque eso esta dentro del protocolo. El protocolo establece que es una conexión punto a punto y el protocolo garantiza esa dirección punto a punto. No tenemos una red de packet Switching de Internet, sino que esto subyace al protocolo de manera que si hay un packet switch y hay mucha gente conectándose, no va a funcionar.

Tenemos que hacer que la gente entienda esto y no debemos decirles y explicarles todos los problemas, cada uno de los problemas, sino que tenemos que enfrentarlos y distinguirlos. Y creo que es muy importante esto, para ser transparentes en la medida de lo posible, ver qué es lo que no es posible y ver qué es lo que sí y lo que no esta relacionado con el DNS.

DAN KAMINSKY: Estamos hablando de una reunión donde había 200 ingenieros. Y ahí yo les pregunto, ¿cuántos de ustedes escriben software que depende del DNS? Se levantaron dos manos de las 200. Y yo dije, en ese simposio dije, a ver, les voy a volver a hacer esta pregunta, ¿cuántos de ustedes tienen un software que ustedes consideran que va a tener una string de texto y va a recibir una dirección IP para que se establezca una conexión de red? Y después se levantaron allí 198 manos. Todo es un problema de DNS. Esta fundación, estos fundamentos tan increíbles en los que nosotros construimos estos protocolos en los que podemos tener una organización, la única razón por la cual estos protocolos lo pueden hacer es que el DNS les da esa capacidad.

Lo que nosotros estamos viendo de hecho, es que hay una gran cantidad de hackers, y no solo hackers sino que son personas que ven que si pueden manipular el DNS, pueden manipular todos estos protocolos más grandes y esto puede ser por ciberguerra, puede ser por activismo, puede deberse a algún adolescente que se esta divirtiendo y quiere hacer algún fraude. Hay una gran cantidad de razones que tienen que ver con meterse con Internet. Y resulta entonces que el DNS es un muy buen punto al cual atacar.

Imagínense ustedes una gran cantidad de países en el que el uplink cae, ¿eso significa que cada uno de los países, en el país no va a funcionar? Bueno, puede ser una -- algo que esta hosteado fuera del país, algo que esta alojado de alguna otra forma, pero a veces ninguna de estas cuestiones importa porque no se puede encontrar ninguna de las direcciones.

Tenemos este punto de inflexión, o punto objetivo, que es tan importante para muchos de los atacantes donde dicen, “bueno, a ver, no importa como funcione todo ahí, si llegamos hasta acá, vamos a poder romper todo lo que se construyó antes”. Vemos mucha gente que tiene varios intereses en cambiar la red.

Hay cuatro estándares: seguridad, soberanía, privacidad, piratería, hay distintas fuerzas que están tratando de cambiar las cosas. Pero hay una fuerza que es la que realmente unifica a todas las personas que están en esta sala que es la confiabilidad. Nosotros hemos construido algo fantástico y tiene que seguir funcionando. Y es fundamental, es muy remarcable ver como mucha gente en esta sala no esta considerando el asunto de la confiabilidad.

RICK WESTON: Les agradezco a todos por tomarse el tiempo y hablar de la seguridad. Creo que la conversación que yo he tenido muchas en el mundo de la ciberseguridad ha tenido que ver con la ciberguerra y la dualidad de la capacidad online de conectar ciertas cosas. Me parece a mi que ICANN esta en una posición singular para ayudar a coordinar muchos de los aspectos que aparecen en Internet y hacer que se mantenga estable. Hacer que se mantenga en marcha, en funcionamiento.

Si pudiésemos separar la conversación de la seguridad y transformarla en ayuda, creo que hay mucha -- una actitud mucho mayor para que el Internet sea un lugar seguro, saludable, para que haya sistemas en un lugar más saludable. Lo vemos por ejemplo vas -- hay muchos otras formas más amigables de mantener una discusión sobre como funciona Internet de un modo más positivo que beneficie a la comunidad global sin importar el estado soberano que tenga un país.

Por eso, lo que yo quisiera ver que haga ICANN, es crear un esfuerzo que empuje a la seguridad y la salud, digamos así, de Internet y la Organización Mundial de la Salud hace una gran colaboración para ayudar a la comunidad porque ellos tienen relaciones. Eso es lo que hace ICANN, creo que ahí es donde

esta su valor como una comunidad global. Y tendríamos que salir un poco de la conversación de la guerra, creo que eso seria algo saludable.

Muchas gracias.

SIMON MCCALLA: Hola soy Simon McCalla, de Nominet del Reino Unido.

Nosotros hablamos de DDOS, hablamos -- nosotros los expertos en el DNS decimos que siempre tenemos que solucionar este problema de DDOS. Trabajamos con los ISP en el Reino Unido para ver como podemos llegar al cliente y solucionarle los problemas respectivos. Pero cunando vemos que hay cuestiones de privacidad, vemos que hay que educar o ayudar al cliente.

Tengo una pregunta para Jeff, ¿cómo podemos ayudar a los clientes a que mejoren la salud de su propio DNS sin invadirles su privacidad por completo?

JEFF MOSS: En general este es un gran tema no solo por cuestiones del consumidor, sino también por cuestiones de compartir información y ver como mejorar esta información, o compartir esta información entre el sector privado y el gobierno. Creo que esto lo hacemos con protecciones estructurales para asegurarnos de que antes de ver un tema individual en su computadora, o en su servidor, tenemos que ver temas de privacidad. Pero, según tengo entendido, nosotros estamos tratando temas de flujo de datos que se pueden compartir sin invadir la privacidad personal.

Y también creo que lo que puede ser un balance entre como abordar estas amenazas para que Internet siga siendo abierta, también puede ser algo a

considerar. Y la única respuesta que tengo es que, tiene que haber una solución transparente para que no haya sorpresas respecto de lo que hacen los ISP.

BRAD WHITE: Quiero hacerle una pregunta más, Jeff. Dado el esfuerzo corporativo cuando surgió la amenaza de conficker, hubo personas de relaciones públicas que participaron al respecto. ¿Ustedes hablan de la transparencia? Obviamente eso es importante. ¿Cómo equilibran los beneficios y la transparencia con una amenaza?

JEFF MOSS: Una de mis preocupaciones es que nosotros los técnicos, ignoramos el problema de política. Entonces, por ejemplo, supongamos que falla un servidor de nombre, técnicamente se lo puede solucionar, pero ¿cuáles son las otras consecuencias de índole política?, si eso impulsa a cierto grupo a decir que no estamos haciendo una buena tarea.

Probablemente tenemos que dar un paso más y tomar esto con mayor seriedad. Es decir que hay una situación o hay situaciones en las cuales uno dice “esto es un problema técnico, no necesitamos a gente de relaciones públicas”, pero en ultima instancia son de mucha utilidad.

PATRICK JONES: Nosotros estamos tratando de educar a los consumidores y es interesante hacer una analogía con el tema de la salud para que nuestras maquinas sean no solo seguras sino también saludables. Parte del gobierno de los Estados Unidos, los ISP, las empresas buscadoras de Internet también participan y no podemos resolver esto nosotros mismos.

En muchos lugares llegamos a los consumidores y quizás no tuvieron la misma información y creo que gran parte de su frustración es porque ellos quieren que le demos dos o tres cosas para hacer, o dos indicaciones y eso no es tan fácil. No siempre les queda claro, o esta tan claro, qué es lo que tienen que hacer.

PAUL TWOMEY: Creo que el precio a nivel político es la transparencia en los procesos. Entonces, si tomamos el ejemplo de conficker, en parte abordar esta crisis va a tener que ver con la privacidad y con la falta de transparencia, y eso es importante en estos aspectos. Pero es importante que la gente sepa que los procesos se van a seguir y que eso fue transparente de antemano. Y que hay mecanismos de interacción y seguramente van a querer ver que haya un nivel de relaciones públicas y comunicación apropiado.

También tenemos que ver quien esta participando y cómo. Esta no es solo una cuestión de conficker, sino de todo el rumbo que esta tomando la ICANN en cuanto al DNS y a la seguridad del DNS. Porque este problema de nivel o capa ocho, layer eight en ingles, va a seguir empeorando. Y con todo el respeto que se merecen los ingenieros, no lo van a poder resolver ellos solos, porque van a ir en una espiral descendente. No va a ser una respuesta aceptable cuando surja una crisis. Entonces hay que distinguir la transparencia de los procesos. Y esto es distinto de la transparencia durante una crisis en si misma.

DEBBIE MONAHAN: Creo que tenemos la responsabilidad de encontrar soluciones independientemente de cuales sean las cuestiones. Por ejemplo con conficker, en punto nz bloqueamos la registración de los nombres que estaban en la lista. Pero luego fijamos un proceso mediante el cual los registros y los registradores

podían también participar del proceso. Así que este es un aspecto clave para abordar todas estas cuestiones. Aun así somos responsables de la administración del ccTLD de manera tal que sirva a los registratarios. Hay muchas soluciones innovadoras.

DAN KAMINSKY: creo que las relaciones públicas en temas de seguridad se tienen que focalizar en la acción. No alcanza con anunciar que algo no funciona, si lo hacemos estamos perdiendo una oportunidad. Cuando hay cierta acción que la gente debe tomar para que Internet sea más segura, allí hace falta la comunicación y las relaciones publicas. Hay que decirle a la gente, instale esto, haga tal cosa. Si uno solamente informa, no alcanza. Básicamente no hay que anunciar que existe tal problema, no hay que decir solamente "existe tal problema y estamos trabajando en ello". Creo que lo más importante es decir "existe este problema pero usted puede hacer tal o cual cosa. Si usted esta de acuerdo con esto entonces tiene que adoptar tal o cual acción". Hay que focalizarse en las acciones.

JEFF MOSS: Creo que tenemos que hacerlo también con los gobiernos, además de con los consumidores. Porque básicamente, no saben que hacer y quizás la comunidad técnica y los que operan la infraestructura, quizás nosotros no hemos hecho una buena labor de articulación. Tenemos que ver donde pueden ayudar los gobiernos, cual puede ser nuestro rol, para articular mejor esta relación. Creo que este riesgo esta incrementando el nivel de preocupación. Entonces debemos incluirlos en esta categoría y darles margen de acción.

RICK WESTON: Es importante hablar de -- aprender de otras industrias y estoy no estar de acuerdo plenamente con usted, Dan. Hay que ver todos los problemas de salud que tuvimos, o que evitamos en el mundo desde que aprendimos a lavarnos las manos. Pensemos en el sida por ejemplo, hablamos acerca de esto durante muchos años hasta que aprendimos como solucionar el problema.

Entonces tenemos que tomar estos ejemplos como formas de abordar una situación global, cuando tenemos un problema global. Estos problemas afectan a toda la población.

DAN KAMINSKY: Esa es una analogía interesante, la de la salud. Obviamente la salud es algo que todos procuramos, pero es un problema diferente. Nosotros hablamos de cosas técnicas y no tiene tanto que ver con las bacterias o los virus de las personas. En el tema de seguridad, la gente todo el tiempo se obsesiona con estos problemas. Así que estamos atacando un enemigo diferente.

BRAD WHITE: Señor, tome la palabra.

MIKEY O´CONNORS: Hola, soy Mikey O´Connors, soy uno de los Vicepresidentes del DSSA. Algunos de ustedes ya están familiarizados con este grupo. Me gusta mucho lo que se esta diciendo en esta sala. Me encanta todo lo que dijo Stephen al principio cunado dijo “no hablemos de lo que la ICANN no hace, sino de lo que sí hace”. Me gusta mucho también la postura de coordinación y transparencia presentada por Paul. Me encanta siempre todo lo que dice Dan.

Y quiero hablar acerca de un documento que se uso como base para esta reunión, que es un acuerdo revisado de la ICANN y la declaración correspondiente. No voy a entrar en mucho detalle. Yo soy miembro de la unidad constitutiva de ISP y no voy a repetir esto nuevamente, pero creo que tenemos que mejorar y ajustar esto, afilar esto. Creo que el rol y la incumbencia de la ICANN están plasmados en los estatutos. ¿Qué queremos decir cuando decimos asegurar, garantizar por ejemplo? Y no es algo que vamos a definir en una reunión como esta. Me gusta mucho el hecho de que tengamos esta conversación y se que las cuestiones tácticas y técnicas son muy importantes, pero también tenemos que empezar a ver como podemos trabajar juntos y ver que hace cada cosa en el ecosistema del DNS.

BRAD WHITE: Retomemos este concepto. Jeff, ¿quiere decir algo?

STEPHEN CROCKER: No, Jeff dijo que no va a contestar a esa pregunta. Creo que lo dicho por Marggie, y por Mikey, es correcto. Lo que dice en los estatutos está bien para la época en que los estatutos fueron redactados. Yo no participe de esa redacción, pero supongo que en aquel momento parecían razonables y si había preguntas o requerimientos de más detalles, se iban a abordar según cada caso.

Creo que ahora llego el momento de repasar y revisar todo esto para darle una mejor forma. Como dije, la ICANN no es el único operador de este espacio, hay gobiernos, miembros de la industria, lo que nosotros llamamos los registros regionales de Internet, la ITF, los operadores de raíz por supuesto.

ALEJANDRO PISANTY: Soy Alejandro Pisanty. Soy de la Universidad Nacional de Méjico, y soy del capitulo de la ISOC Méjico que se dedica a seguridad. ¿Me escuchan?

Al comienzo de este año Jeff Brueggeman, Simon McCalla y yo estuvimos en un panel junto con un gran equipo de múltiples partes interesadas y le dimos la revisión de seguridad, estabilidad y flexibilidad de la ICANN. Parte de esto ya ha sido implementado, para mi eso es algo muy bueno.

No veo que el debate de hoy este tan adelantado como nos gustaría. Por ejemplo, en lugar de hablar solamente de seguridad y ataques, tenemos que hablar de un panorama más integral de gestión de riesgos. La diferencia que haría esto seria significativa. Y no me estoy quejando de que no hayan hecho lo que redactamos con mi equipo. La ICANN esta en una situación asimétrica de conflicto. Una de ellas tiene que ver con lo siguiente, hay muchas personas que quieren que la ICANN no haga nada hasta tanto algo suceda, y son casi siempre las mismas personas la que dicen siempre lo mismo cuando se refieren a la ICANN.

Así que, si tienen un ataque de DOS masivo contra el DNS y el servidor, bueno o un DDOS, se supone que la ICANN no tiene que intervenir con los ccTLD, con los registros, con los ISP, con nadie, porque todos son independientes en el modelo de múltiples partes interesadas. Pero cuando está esta denegación de servicio que hace que caigan los servidores raíz, todo el mundo espera que suceda algo. Y todo el mundo va a preguntar, ¿dónde estaba la ICANN? ¿Por qué la ICANN no estaba preparada para esto? Espero recibir algún informe de progreso sobre esta temática y hacer que sea muy concreto y que sea una gestión de riesgo a todo nivel. También a nivel político.

Me gustaría ver la opinión del panel, es decir, ¿cuánto ha aumentado el riesgo? No me concentraría solo en los DDOS, sino también en los daños políticos para

la ICANN o sus aliados más visibles. Es decir, ¿cuánto ha aumentado este riesgo, en el último riesgo, con el anuncio del Departamento de Defensa de los Estados Unidos? Este anuncio, junto con el interés de algunos grupos que les gustaría ver mejorada esta infraestructura, ¿cómo tiene -- cómo causan un impacto?

PATRICK JONES: Me gusta su visión de la gestión de riesgos y entiendo hasta donde quiere llegar esto. Una de las preguntas que yo hice fue, ¿cuál fue la tasa de crecimiento de DDOS? Si no tenemos una capacidad, y volvamos al ejemplo del DOS, una de las formas que yo veo, es que tenemos la escala y no se exactamente, no conozco ninguna otra solución para que haya un mejor uso de banda. Si ese es el mundo en el que vamos a vivir, ¿qué significaría un crecimiento normal? IPv6 tiene queries de dispositivos móviles para cargar más rápido las páginas para Chrome o para lo que sea. Y ha habido una tasa de crecimiento de 30 por ciento de las queries de DNS. Eso no va en contra de la raíz, pero el software que esta en general, y veo que usted esta sacudiendo su cabeza y me podrá dar un mejor número, pero hay un crecimiento en el tráfico de queries y si no estamos en ese nivel, nos estamos quedando un poco atrás.

Estoy escuchando muchas discusiones sobre cual es el crecimiento proyectado, si es que tenemos que planificar una capacidad de crecimiento del 50 por ciento. Y pareciera ser que esos números que parecen estar en una escala mayor en cuanto al marco de gestión de riesgo, bueno parece que no hay que decirlo en voz alta porque no hay que decirles a los atacantes cual es la capacidad. Y es como el problema de la gallina y el huevo.

JEFF MOSS: En cuanto a lo que dijo Alejandro, hay estructura y procesos para enfrentarse con ese tema. Creo que la Junta ha tomado un paso en esa dirección y vamos a tomar los debates que haya necesario para incluirlo en la forma en la que opera ICANN.

TOM DALY: Somos un operador de DNS. Me gusta lo que tiene para decir el panel hasta ahora y se que se están focalizando los temas adecuados.

Quisiera ahora que pensemos en una de las ventajas que sí tenemos y que normalmente es ignorada, que es el efecto del cashing. Volviendo a la analogía de la salud del mundo, lo bueno de un gran DDOS, es que sabemos quien -- qué es lo que esta sucediendo y quien esta enfermo y podemos ir a curar a los que están enfermos.

A mi me gustaría que el panel comente sobre el nuevo vector que estamos viendo en los últimos seis meses, en cuanto a los intentos en los registros y los registradores en si, porque me parece que eso es un problema mucho más grande. Dada una población de personas, tenemos que saber quien esta enfermo y quien no, como en el caso del DDOS.

DAN KAMINSKY: Gracias. Mencione esto un rato antes, de hecho fue en una reunión con ICANN hace algún tiempo donde me dijeron “bueno, los registros y los registradores van a dividirse y esto va a ser un problema creciente”. Y déjenme que les diga, yo no fui muy popular cuando lo dije en esa reunión. Pero es cierto, todo se esta dividiendo y en registros y registradores, y ellos no son la excepción. No hay ninguna razón mágica por la cual su servicio Web no van a ser atacados. Y

estamos viendo consecuencias de Google punto ie que se quebró y algunos otros.

Usted toco el tema, el miedo más grande que yo tengo. Sí podemos ir adelante, y podemos decir en forma visible, yo voy a cambiar este record para que todo el mundo lo pueda ver y que todo el mundo pueda generar ese cambio . Pero al mismo tiempo, no lo hacemos. También se puede elegir o decir selectivamente si uno entra a un registro o a un registrador para que ellos tengan algunos registros. Es decir, que hagan que todo funcione bien. Hemos visto esto muchas veces en el resto de la seguridad, desde gusanos enormes que afectan el mundo, hasta ataques muy atacados que les llaman spear phising.

Creo que la transición -- no solamente estamos viendo una transición de una denegación de servicio no inteligente hacia el ingreso al registro de un registrador, sino que también estamos viendo un uso muy dedicado de esa capacidad.

PATRICK JONES: Este es un problema conocido y en el equipo de seguridad de ICANN le dedicamos mucho esfuerzo dentro del paraguas de nuestro equipo de capacidad para trabajar con registros y registradores y pedir ayuda. Y ayudarlos a generar políticas y procedimientos para enfrentar esto, así como tecnología, soluciones de tecnología.

Yo no estuve en esa reunión, pero yo no me hubiese enojado. Es un problema conocido y yo no se si hay una respuesta coherente de la industria.

PAUL TWOMEY: Creo que tenemos que pensar en esto con mucho cuidado. En cuanto a lo que dijo Alejandro de que ICANN hace esto o hace aquello, y cómo funcionan los actores individuales, parte de lo que decimos es qué es lo que hace ICANN. Yo y otros hemos construido a generar una institución y parte de eso ha sido que haya ejecutivos y fondos, etc. Pero no debemos olvidarnos que el corazón de esto, en los años 90 cuando hablábamos de la formación de esta comunidad, era que fuese que las partes interesadas se involucren, que participen.

Y creo que este es el limite con el que nos encontramos mucho más en relación con el nivel de las partes interesadas que hablan entre si y que generan una claridad de que es lo que quieren ver que suceda. Si esto preocupa, lo que hacen los registratarios, o no están haciendo y entonces quien esta compartiendo qué cosa en los operadores de servidores de raíz, si es que los gobiernos hablan directamente o no. Creo que hay alguien aquí de Portugal, no hay mucha gente del gobierno en este momento, lamentablemente.

Pero este tema en particular me preocupa a mi muchísimo. Tenemos que -- a ver, estoy pensando en los momentos de crisis que puedan llegar a ocurrir. Es decir que, si no nos ocupamos de la unidad constitutiva, la unidad constitutiva, y generamos un enfoque común en torno a la transparencia y a los procesos y lo que hacemos hoy es simplemente decir, “Patrick y su grupo se tienen que ir”, nos vamos a perder el punto.

Y la razón de la participación es necesaria porque tiene que haber un sentido común de que es un enfoque verdaderamente transparente porque cuando ocurre la crisis, como dijo Alejandro, y aparecen las desconexiones, tiene que haber una forma de decir este es el camino que todos hemos elegido. Porque si no, las alternativas es ir siempre al plan B. Cuando ocurre una crisis nos vamos al

plan B, y tiene que haberlo, siempre nos vamos -- va a haber algo que se rompa en ese proceso.

Alguien hablo en este discurso de los ciberataques que pueden ocurrir, y cual es el impacto que puede ocurrir en Estados Unidos, después de lo que paso el 11 de septiembre. Después del 11 de septiembre, la comunidad de Estados Unidos pago un trillón de dólares para que haya una guerra. Estos eventos pueden tener un cambio gigantesco realmente. Yo espero que continuemos con este dialogo y que las partes interesadas hablen en forma practica sobre cual es la visión en común y no solamente de que pensamos, cual pensamos que debería de ser la función.

DEBBIE MONAHAN: Yo dije antes que ICANN tiene un rol de coordinación y que los ccTLD tienen mucho que contribuir, y muchos de ellos han dedicado mucho dinero y esfuerzo a que los registros hagan otra cosa. Yo se también que hay una cantidad de ccTLD que establecen políticas de seguridad para tratar de proteger a lo que están protegiendo los registradores.

Nosotros en punto nz tenemos unas políticas de seguridad que deben ser definidas y los registradores están en la línea de frente porque entre el registrador y el registratario hay algunas cuestiones de vulnerabilidad.

Por eso tenemos que poner esto en la línea del frente más rápido, y se que tenemos que poder tomar prestado cosas de otros, como nosotros hicimos con la comunidad de ICANN y con toda la gama de partes interesadas. Porque no hay una sola respuesta, sino que tenemos que -- no tenemos que elegir lo que hace punto ez, o punto com, o punto uk, sino que tenemos que encontrar la solución optima para punto nz. ICANN tiene el rol de coordinar la información.

BRAD WHITE: Paul, usted tiene algún problema con la interacción entre los funcionarios del gobierno porque los gobiernos tienden a ser reactivos y no preactivos. ¿Cómo hacemos para que haya mayor compromiso, para que este sobre la mesa?

PAUL TWOMEY: Hay un dialogo entre los gobiernos sobre todo el tema de la ciberseguridad y la ciberguerra, de hecho esto ha llegado a ciertos servicios y hay quienes han tratado de que no se tire al bebe por el autobús, porque hay que tener cuidado de estas cosas. Y esa voz tiene que ocurrir. Pero no podemos confiar en una generación, una sola generación de personas que tienen experiencia en el sistema, sino que más bien tiene que haber -- a ver, yo creo que la comunidad y el GAC tienen que ser parte de esto.

Las partes interesadas tienen que ser una voz diciendo, estamos haciendo esto o aquello. Tiene que haber un mensaje, tiene que haber una voz en cada país que hable sobre la información que se va mostrando. Tiene que haber una capacidad de plataforma de esta comunidad.

CATH GOULDING: Hola, soy Cath Goulding de Nominet. Soy muy nueva en este entorno, pero no soy nueva en las amenazas cibernéticas, por eso les pido disculpas si mi pregunta es un poco básica.

Yo veo muchos registros nacionales donde hay una amenaza terrorista o un volcán en Islandia que no permite que los aviones aterricen en el Reino Unido. Entonces tiene que haber una amenaza que es bastante abarcativa y también una estrategia de ciberseguridad para hacer que esto no se retroalimente.

Para mi ICANN y la raíz del DNS es una amenaza internacional y no hay un registro internacional, por eso para mi este es un gran lugar. Mi pregunta es ¿existe un registro de riesgo para la raíz DNS? Y si no, ¿A dónde tienen que ir los gobiernos para que existan registros nacionales de raíz?

BRAD WHITE: Stephen, ¿esta huyendo de las preguntas?, ¿se esta escapando de las preguntas?

STEVE CROCKER: Queremos desear a Stephen un feliz cumpleaños. El Doctor Crocker cumplió diecisiete años hoy.

PATRICK JONES: En la raíz hay ejercicios y hay juegos en cuanto a los planes de contingencia. Se dice mucho en la -- respecto de la raíz. Recuerden que no hablamos de los operadores de raíz, sino estos son simplemente verisying NTIA y el grupo de ICANN. Los operadores de raíz individuales hacen lo que hacen. O sea que si vieron uno, vieron uno.

JEFF MOSS: Desde la perspectiva de alguien que rompe ciertas cosas, la raíz es demasiado grande. La raíz -- cuando yo pienso en alguien que va a atacar al DNS, no pienso en la raíz, por varias razones. Uno es que están muy bien alojadas, no hay muchas, y por el cashing y porque no todas las solicitudes pasan por ahí, yo prefiero entrar al verisying y no entrar a la raíz.

Hay varias cosas que se pueden decir. Pero seriamente, cuando a mi me preocupa que va a atacar a alguien para poder impactar en el DNS, la raíz es un objetivo bastante sexy, bastante interesante, pero no es el objetivo primario. El objetivo primario siempre va a ser los nombres de servidores para organizaciones a las cuales yo quiero impactar, o los registradores o registros que están literalmente enviando otros sistemas a estas maquinas en particular. Ahí es donde hay menos atención y más exposición.

Pensemos por ejemplo en los servicios a los que expone los servicios de raíz, ellos exponen el DNS y eso es todo en general. Hoy hay una gran cantidad de servidores que alojan mucho más que DNS y hay registradores y registros que tienen semi-fiascos por los cuales preocuparse. Eso es el -- eso es lo que a mi me -- lo que yo creo que hay que tener en cuenta.

AMY MUSHAHWAR: Soy Amy Mushahwar y represento a la Asociación Nacional de Publicistas.

Hemos llegado a tener una política de seguridad pero nuestro grupo representa a una amplia gama de marcas nacionales estadounidenses e internacionales. Y queremos que conste en los registros que a nuestras marcas les preocupa mucho la seguridad. Sin embargo no tanto a nivel de infraestructura o de entender cuando va a haber un ataque de denegación de servicio causado por un hacker.

Sino que más bien nos preocupa el retorno sobre la inversión y que uno pueda utilizar al DNS en si mismo y poner en practica las pocas protecciones que tenemos para proteger a las marcas comerciales y a los nombres de spoof. Entonces queremos que el equipo de seguridad trabaje con el IPC y desarrolle mayores protecciones de derechos para los nuevos gTLD.

Porque por supuesto que siempre nos preocupa el ataque de un hacker, pero nos preocupa también la inversión. Tenemos que preocuparnos por ello también.

BRAD WHITE: Me dicen que nos estamos quedando sin tiempo. Pero lo interesante es ver que todas las personas aquí hablaron de la importancia de la continuidad de estos debates y de la participación de las partes interesadas. Así que quizás estos panelistas puedan estar en la próxima reunión. A ver.

PATRICK JONES: Levanten la mano a quienes les pareció interesante esta sesión. ¿Cuantos quieren o desean continuar con esto en otras reuniones? Entonces voy a esperar que si levantan tantos la mano, formulen preguntes en las próximas reuniones que tengamos. También les recuerdo que estaremos aquí durante toda la semana, durante toda la conferencia. Si nos quieren hablar en privado por supuesto se pueden dirigir a nosotros.

BRAD WHITE: Ustedes han sido maravillosos, señores panelistas. Muchísimas gracias.