

SAN JUAN – ALAC y líderes regionales: sesión de trabajo, parte 11

Martes, 13 de marzo de 2018 – 15:15 a 16:45 AST

ICANN61 | San Juan, Puerto Rico

HOLLY RAICHE: Hoy podemos minimizar los riesgos y al menos tendremos la ventaja de que ICANN esté a la vanguardia y que se apoye a los usuarios lo más posible con la mayor cantidad de información posible. Esas son las únicas condiciones que yo aceptaría avanzar.

ALAN GREENBERG: Vamos a hacer una encuesta para ver cuántas personas cambiaron su opinión. Dos cosas. Internet deja de funcionar muchas veces. Si tienes una infraestructura de Internet, deja de funcionar. Incluso un ISP de tamaño moderado, hay personas técnicas que lo arreglan. La perspectiva es que Internet es muy poco confiable. Los problemas ocurren todo el tiempo. Si uno está operando un ISP seguramente va a tener personas que lo van a poder hacer. No me preocupa ese nivel. Tiene la palabra Eduardo.

EDUARDO DÍAZ: Gracias, Presidente. Esta cuestión de la implementación es como una especie de problema porque la misión de ICANN es que el

Nota: El contenido de este documento es producto resultante de la transcripción de un archivo de audio a un archivo de texto. Si bien la transcripción es fiel al audio en su mayor proporción, en algunos casos puede hallarse incompleta o inexacta por falta de fidelidad del audio, como también puede haber sido corregida gramaticalmente para mejorar la calidad y comprensión del texto. Esta transcripción es proporcionada como material adicional al archivo, pero no debe ser considerada como registro autoritativo.

DNS esté seguro y estable. Una vez que se implementa este rollover todo debería continuar. No entiendo todo el proceso pero una vez que uno lo cambia, hay que cambiarlo al mismo tiempo en todas las zonas horarias del mundo. Por eso les digo que si eso ocurre, eso detendrá Internet para algunas cosas. Yo entiendo que eso también va a ocurrir el 11 de octubre. Está muy cerca del 11 de septiembre. Eso es lo que yo sentí cuando alguien me habló del 11 de octubre. Lo último es que hace mucho tiempo yo aprendí que si funciona, no hay que repararlo.

ALAN GREENBERG:

Funciona pero con un potencial de dejar de funcionar. Recuerden, si la clave está comprometida y hay algo que empieza a ocurrir, a lo mejor podemos llegar a pensar que va a haber un problema en la raíz y vamos a tener que implementar la clave. Es algo desconocido y es una práctica criptográfica mala no hacerlo.

EDUARDO DÍAZ:

Hay muchos que intentaron encontrar la fórmula de la Coca Cola.

ALAN GREENBERG:

No hay tanto en riesgo en el caso de Coca Cola. Solo hay miles de millones de dólares en juego. Sébastien.

SÉBASTIEN BACHOLLET: Para mí, la pregunta es si estamos en la misma situación que en el año 2000 con el riesgo de que ocurrieran muchas cosas y no pasó nada. Todo eso, ¿para qué nos sirvió? El segundo punto, si comprendí bien tiene que haber por lo menos DNSSEC. Tenemos algunas habilidades técnicas en ese nivel. Pasaron a DNSSEC, que no es tan sencillo. Mi ISP no tiene DNSSEC. No se ha hecho todavía y es una compañía bastante grande. Estamos a punto de hacer una montaña de una cosa que no es tan complicada. Son personas que ya pasaron a DNSSEC y por lo tanto tienen la competencia técnica para asegurar esta cuestión de la clave pública que hay que traspasar. Gracias.

ALAN GREENBERG: Ricardo.

RICARDO HOLMQUIST: Voy a hablar en español. Lo que yo no veo es un plan estratégico o una campaña de mercadeo. Hoy apenas estaba oyendo decir: “Vamos a hablar con los RIR acerca de las direcciones que nos están respondiendo que no están resolviendo correctamente”. Eso lo tenían que haber hecho hace un año. Ya hablamos con los bancos. Para mí, los principales implementadores de DNSSEC son los bancos, son los que transfieren dinero, son la gente que

lleva dinero, más allá que un ISP. Ya hablamos con las asociaciones de bancos mundiales, regionales, nacionales. Yo no veo que haya un plan desde el punto de vista de ICANN de hablar con los mayores involucrados de esto y muchos de ellos no saben que esto está ocurriendo.

A lo mejor el 11 de octubre sigue siendo una fecha válida pero una fecha válida, como decía Holly, con cosas claras en el medio, entre aquí y el 11 de octubre, que yo no las estoy viendo. Yo no estoy viendo que hayan venido aquí y nos hayan pedido nuestra ayuda para hablar con nuestras ALS locales para hablar con los diferentes ISP. Qué van a hacer los usuarios, cómo podemos ayudar nosotros. Al final del día, vamos a ser los afectados. No me quiero imaginar algún país que tenga tres o cuatro bancos que no funciona el DNSSEC y que no puedan transferir dinero ese día. Eso puede causar una crisis financiera en muchos de nuestros países pequeños. Eso puede ocurrir. No es solamente que no vayas a entrar en Internet.

ALAN GREENBERG:

Tijani.

TIJANI BEN JEMAA: Gracias. Primero, si usted hace un comentario después de cada comentador, va a impactar en la decisión de las personas. Por favor, comente igual a todos.

ALAN GREENBERG: Paré y me puse en la fila.

TIJANI BEN JEMAA: Muy bien. Es una muy buena decisión. Vuelvo entonces al tema. La gente que considera que está segura si no hacemos la implementación porque la implementación puede hacer que se para Internet, yo les digo que tienen más riesgos si no cambian la clave. Ustedes saben cómo es. Si alguien puede hackear la clave del DNSSEC no va a haber más clave. El peligro está allí. Si nosotros queremos tener algo adecuado, tenemos que hacer las cosas de un modo adecuado y el personal técnico nos ha dicho que lo tenemos que hacer. Yo entiendo que hay un problema de los resolutores. Este es el problema de los resolutores pero también hay resoluciones.

Primero ICANN hace una campaña de difusión para que todos los ISP y los operadores sepan que esta implementación puede afectar los resolutores que no están actualizados. Solo es una actualización de software. Sé que no todos lo hicieron y quizá no lo hagan pero la solución, e ICANN debe decirlo, es que si uno no

está seguro de lo que tiene, simplemente tiene que apagarlo, tiene que apagar el DNSSEC y la Internet va a continuar funcionando.

Una vez que la clave esté implementada, se puede volver a encender y si hay un problema se puede apagar otra vez y resolver el problema. En este caso, no tenemos un problema grave. No es una catástrofe pero si mantenemos la misma clave desde el principio, no sé cuánto pasó, creo que son cinco años, ¿no? Se planeó que se cambiara con anterioridad.

ALAN GREENBERG: Abdeldjalil.

ABDELDJALIL BACHAR BONG: Muchas gracias. Mi pregunta es la siguiente. Nosotros hablamos de la clave KSK pero realmente tenemos que ver cuál va a ser el impacto para los usuarios que se conectan. ¿Cómo podemos explicarlo? ¿Cómo podemos ver la cartografía de todo esto? Si nosotros no cambiamos la clave, si entiendo bien las explicaciones técnicas, esto va a desconectar Internet. ¿Hay muchas personas que no tienen conexión a Internet ahora? ¿Puede ser esto visto como censura? ¿Dónde se encuentra la clave y cómo la vamos a cambiar?

ALAN GREENBERG: Javier, creo.

JAVIER RUA JOVET: Estaba escuchando a todos y desde el lado técnico hay expertos y creo que hay un consenso de que los riesgos podrían no ser catastróficos. El problema aquí es más bien político. Fíjense en lo que dice Ricardo y lo que dice Sébastien. Son premisas similares que caen en distintos lugares del tema. Tuvimos el Y2K. Parecía que el mundo se iba a acabar. El mundo hizo un enorme esfuerzo de información. El mundo no se terminó y todo está bien. El mundo de hecho no se va a terminar con el cambio de la KSK pero hay cosas que sí pueden ir mal. Si uno vuelve a mirar, ve que ICANN hizo entre poco y nada para advertir. Estados Unidos está un poco loco ahora.

Algo que sí podemos predecir es la imprevisibilidad de algunas personas que están en el gobierno. Si vamos a proteger la estabilidad de Internet, debemos proteger la existencia de la ICANN, la cual puede dejar de existir con un pequeño error. Esta no es una cuestión técnica. Es una cuestión política sobre... La palabra óptica no me gusta pero más bien diría la reputación de la ICANN y la capacidad de crear crisis para beneficio de algunos. Nosotros no podemos estar en esa situación. Creo que se requiere de precaución, la mayor precaución posible.

ALAN GREENBERG: Hadia.

HADIA ELMINIAWI: El único riesgo que veo es que no lo hemos hecho anteriormente así que hay que avanzar y hacerlo. Respondiendo a lo que dijo Ricardo cuando mencionó que hay un momento en que una deja de funcionar y comienza a funcionar la otra, tendría que haber un periodo de superposición en el cual ambas claves estén en funcionamiento para que la clave del 2010 se pueda utilizar mientras la clave de 2017 presente, hasta que el sistema entienda que la clave del 2017. Habría un periodo de superposición. También habría un periodo en el cual una clave dejaría de ser utilizada y la otra comenzaría a ser utilizada cuando el sistema lo entienda, aprenda esto. Así habría un sistema de superposición. Se va a usar una pero la otra estaría presente hasta que el sistema entienda, aprenda a utilizar la clave de 2017.

ALAN GREENBERG: No funciona así pero vamos a hablar de eso después.

JOHN LAPRISE: Yo tengo unos breves comentarios. Uno es que cuando hablamos con la comunidad técnica hoy, lo que dicen es que si se rompe, se tiene que resolver. Yo entiendo esto de la comunidad técnica

porque hablan de tecnología pero nosotros representamos a los usuarios y ese es nuestro principal objetivo y preocupación en primer lugar.

Con respecto a los riesgos, hablamos mucho de los posibles riesgos, de quién podría estar afectado y por qué pero el riesgo también es un riesgo interno porque son datos que no entienden, no entienden por qué va a suceder, qué es lo que sucede. Simplemente van a ver lo mismo que nosotros, que no están cumpliendo con algo pero no exactamente con qué y nadie va a saber con qué en seis meses.

Con respecto al plan de comunicación, los puntos que surgieron en la comunidad técnica fueron que no saben cuáles son los resolutores. Cómo van a hacer un plan de comunicación para llegar a estas personas y a las personas que operan estos resolutores. Esos serían mis puntos principales y los quería mencionar. Como ALAC, nosotros representamos los intereses de los usuarios finales en primer lugar y eso es lo que nos tiene que ocupar. Gracias.

ALAN GREENBERG:

Todavía tenemos unas siete personas en la lista de oradores y si queremos debatir algo sobre las métricas voy a dar por finalizada la lista de oradores ahora. ¿Es importante?

CHERYL LANGDON-ORR: Es importante que sigamos con este debate.

ALAN GREENBERG: Si les parece importante vamos a seguir con la lista de oradores. Adelante, Olivier.

OLIVIER CRÉPIN-LEBLOND: Muchas gracias, Alan. Creo que uno de los problemas que enfrentamos es la cantidad de cosas desconocidas que no conocemos y que tenemos por delante. Cuando esto se descomponga, muchas personas van a estar fuera o desconectadas de Internet porque los resolutores no van a funcionar pero el hecho es que la Internet está tan diversificada que hay muchas maneras en las cuales la gente accede a la red y hay muchas topologías. Algunas pueden depender de un resolutor simple, algunas dependen de múltiples resolutores.

Quizá haya algún retraso de milisegundos en la resolución. El problema es que no lo sabemos. Las consecuencias también son desconocidas y todo es desconocido porque no se puede probar, no se puede testear qué sucedería si algo funciona mal en la red. No se puede probar. Me parece que la solución es buscar soluciones. Teniendo en cuenta todo esto y de todas maneras, Internet tiene que seguir avanzando. Esto es parte de la

tecnología y no podemos mantenernos siempre con motores de vapor solo porque la gasolina puede explotar y matar a gente.

Hay algo cierto y es que no hay un análisis certero de todo esto hasta cierto punto y todo parecen ser rumores y la junta le pide al SSAC que analice las cuestiones o que brinde asesoramiento o que haga un informe sobre el tema, lo cual va a llevar tiempo y todo va a depender de la velocidad con la que pueda actuar el SSAC. No sé si esto va a responder nuestras preguntas pero con respecto a lo que nosotros tendríamos que hacer, mi punto de vista personal es que creo que tendríamos que pensar en planes B y C. Tenemos un rol que cumplir en la comunicación. Esto, por supuesto, no está en línea con lo que escuché del GAC y la respuesta del GAC anteriormente pero al igual que lo que dijo Ricardo, hay un representante también en ese momento que dijo que hay gente que no conoce el tema y que tiene que aprender todavía cosas sobre la ICANN. Hay que admitirlo. Quizá tengamos que tomar el liderazgo en esto.

ALAN GREENBERG:

Gracias. Soy el próximo que va a tomar la palabra. Yo simplemente quería decir que había un hecho técnico que no era correcto. Pero me contuve. Los detalles son desconocidos pero la gente que ha estado trabajando en esto tiene buenas ideas.

Sabemos que el DNSSEC no ha sido ampliamente aceptado. Los que no lo han aceptado sí van a recibir el impacto.

También tenemos algunos números que son bastante buenos. No son 100% exactos pero son buenos. Cuando David me dijo que probablemente el 4% de las personas estén impactadas, no sabemos cuáles son las cifras concretas pero seguramente no será un 50%. Probablemente será un 20%. Las cifras no son tan desconocidas tampoco.

En cuanto a lo que se dijo sobre la superposición, la cosa funciona así. Los resolutores permiten insertar el anclaje de confianza ahora. Sin entrar en detalles técnicos, el resolutor tiene un anclaje de confianza viejo y uno nuevo. El resolutor solamente va a funcionar con el anclaje viejo hasta que se cambie. Una vez que se cambie en los servidores raíz, se cambia. Uno tiene todo el tiempo necesario para instalar el segundo anclaje de confianza. Ahora son dos años pero llega un punto, el momento de la verdad, cuando se cambia en la raíz, cuando se instala una nueva versión de la raíz que está firmada con la clave nueva solamente la nueva funciona. No hay posibilidad de superposición en la vida de este sistema. Es el momento de la verdad.

En cuanto a la cuestión del Chad, si el Chad no tiene buena conectividad, los ISP hacen lo mejor que pueden para brindar

conectividad y quizá tenga que instalar el DNSSEC. Si no lo han instalado y, como dije anteriormente, la Internet se descompone todo el tiempo, si no instalan DNSSEC probablemente puedan tener a alguien que los ayude a instalarlo. Esto no es una garantía al 100% pero al menos es una mejora.

Pasando ahora a activar el DNSSEC. Si alguien desactiva el DNSSEC, también se va a mantener seguro. No es una regla segura pero es lo mejor que se puede hacer, al menos desde el punto de vista psicológico para protegerse. Hemos visto hasta el momento, probablemente debido al traspaso de esta KSK, que la gente a veces desactiva el DNSSEC. Probablemente no sea lo que uno recomiende pero la gente lo hace.

Con respecto al Y2K, si todo el mundo hubiese dicho: “Esto no es un problema” los sistemas bancarios, las aerolíneas, las universidades, las industrias tendrían códigos que no funcionarían. Es decir, nada funcionaría. No hemos visto un problema mayor porque mucha gente en todo el mundo dedica tres, cuatro o cinco años escribiendo códigos. Que no pase nada no quiere decir que esto vaya a ser así. Realmente es impresionante cuántos sistemas recientes funcionan correctamente. Los sistemas construidos a mediados de los 90 fueron vulnerables en muchos casos.

Ricardo mencionó hablar con la gente. El tema de los bancos es un punto bueno porque los bancos centrales se comunican con las asociaciones bancarias y probablemente sea un buen punto para inyectar esto dentro de los países. Quizá tengan servidores de DNS. Es una buena opción para que tengan el DNSSEC activo. La ICANN sí está hablando mucho del tema con los ISP y con las personas encargadas y se está encargando de ser escuchada, pero no todo el mundo escucha.

Creo que las ALS, siempre y cuando se hable de un país pequeño y uno pueda tener contacto con los decisores, siempre y cuando se sepa quién administra los ISP, las computadoras de los bancos centrales, si los conocen hablen con esas personas. Me parece que aquí tenemos un rol por delante y es comunicar lo más que podamos. El siguiente orador es Seun.

SEUN OJEDEJI:

No estoy seguro de las cuestiones técnicas. Probablemente me tengan que corregir. En realidad el tema tiene que ver con el intercambio de los resolutores. No sé qué puntos técnicos se corrigieron. Nosotros no somos la comunidad técnica. Somos usuarios finales. Yo en alguna oportunidad participé de la comunidad técnica y la comunidad ha dado su aprobación para esto. No somos nosotros los que vamos a arreglar el problema. Si hay que hacerlo, hay que hacer un traspaso el 11 y se pospone,

son cuestiones técnicas. Nosotros no somos la comunidad que las va a solucionar. Es la comunidad técnica la que se va a encargar de resolver los problemas. Me parece que tenemos que abordarlo desde esa perspectiva. Es decir, este problema es un problema técnico. Es algo que tiene que continuar, especialmente si los técnicos están de acuerdo con avanzar. Lo escuchamos claramente.

No tengo un problema con esta cuestión de seguir dando vueltas en torno a la conciencia y lo que deberíamos hacer. No es nuestra responsabilidad porque no tenemos una solución para resolverlo. El IPv6 hace mucho que ya está. Hace mucho tiempo. La gente todavía no lo ha implementado completamente. Lo van a hacer cuando las cosas dejen de funcionar. Ahí surgirá el problema pero no es nuestra labor. No debemos apoyar esto porque ciertos usuarios o ISP no estén haciendo su trabajo. Esto lo que hace es negar el progreso a aquellos que sí lo hacen. Si nosotros no permitimos que se lleve a cabo el traspaso vamos a ir en contra porque no vamos a permitir el avance y recompensaremos a quienes no han hecho su trabajo.

ALAN GREENBERG:

Alberto tiene la palabra.

ALBERTO SOTO:

Gracias. Lamentablemente tengo que diferir de la última opinión porque estamos representando a los usuarios finales y tenemos que tener en cuenta a la totalidad de los elementos de las medidas que se toman en un sistema multi-stakeholder para saber si afectan o no a los usuarios finales. En particular, Ricardo creo que dijo que faltó un plan de mercadeo. Yo no estoy tan seguro si ese plan de mercadeo faltó o no pero sí tengo la total y absoluta certeza de que hablé con nuestro RIR, con el representante de nuestro RIR, creo que ya lo he mencionado aquí, para ofrecer que LACRALO con toda sus 20 y pico de países y todas nuestras ALS llegaríamos porque tengo el conocimiento necesario. A las cámaras de los ISP, a las universidades, a cualquiera, como dije, que tenga un data center, para hacer relevamientos, hablar... Porque ellos pidieron una cierta ayuda con el pasaje de IPv4 a IPv6 porque dentro de LAC hay todavía un retraso importante. Nosotros íbamos a hacer relevamiento con darles el conocimiento necesario pero yo agregué KSK hace casi un año. Se dijo: “Sí, sí, sí, sí” y nunca tuve la respuesta. No sé si ese mercadeo que tenía que haberse hecho antes a todos, se hizo o no. Si se reaccionó de la misma forma que nosotros teníamos la seguridad de llegar a 20 y pico de países y no se hizo nada, no sé si realmente se hizo correctamente esa difusión. Además, hay que tener en cuenta, Alan dijo que muchas veces se cayó Internet. Es cierto pero si se cae esta vez y la caída es grande, la culpa la tiene ICANN.

ALAN GREENBERG: Bartlett.

BARTLETT MORGAN: Lo que quiero decir es breve. El miedo es un consejero muy, muy, pero que muy malo. Si uno tiene que tomar una decisión y si lo que impide la decisión es el miedo, no se pueden tomar las medidas adecuadas. Escucho los ejemplos que se están mencionando y cuando se dice que no tenemos que avanzar. La propuesta puede ser buena pero quizá utilizar bancas, por ejemplo, no sea una buena idea porque quizá se dé información errónea. Probablemente haya mucha gente a la cual la ICANN no llegue.

John mencionó una lista de cuestiones de la transición de la IANA pero cuando leímos la lista de todas las cuestiones que están enumeradas como cuestiones de alto riesgo, se dijo que la probabilidad era cercana a cero. También quisiera avalar las observaciones de Sébastien. No quiero extenderme mucho. No estamos aquí para hablar eternamente del tema.

También hay otro punto a mencionar. Esta es una cuestión política. Tiene que ver con la reputación de la ICANN, etc. Sí, está bien. A favor de esto, nosotros representamos a los usuarios finales. Desde mi punto de vista, son cuestiones distintas. El

resultado que la ICANN enfrente no estará relacionado con nuestro rol para dar apoyo a los usuarios finales. No los quiero confundir más.

Desde mi punto de vista, el tema no es si avanzamos o no sino cómo la ICANN va a seguir adelante. Se han planteado muchas cuestiones con respecto a la campaña de difusión, el mercadeo, la comunidad. No creo que nuestro comité tenga el suficiente conocimiento sobre la KSK como para tener un debate informado sobre este tema. Podemos empezar por ahí. No quiero tomar más tiempo.

ALAN GREENBERG: Tijani.

TIJANI BEN JEMAA: Gracias. Yo escucho lo que usted dice y puedo decirle que los que más saben que la transición no debería colapsar son los estadounidenses. ¿Sabe por qué? Porque ellos saben que al menos hay dos raíces que están listas para operar. El mayor miedo es la fragmentación. No piensen por un momento que los estadounidenses van a aceptar la fragmentación. Ellos no van a pedir volver a traer a ICANN a la NTIA. Este es el primer punto.

John y Alberto, esto lo digo porque yo pienso en los usuarios finales. Quiero preservar la seguridad de los usuarios finales y

por eso pido que se haga la implementación. Si no implementamos, no vamos a saber cuándo puede haber un problema grande. Si queremos que el sistema sea seguro, si tenemos DNSSEC por supuesto, hay que hacer esta implementación.

El último punto. Yo no creo que nosotros tengamos que decir en base a presunciones de que si el DNSSEC se apaga nunca se va a poder volver a encender, o algo así. Quizá no hay ningún técnico para hacer esta operación y todas estas son presunciones. Nosotros no podemos construir una decisión en base a presunciones. Gracias.

HOLLY RAICHE:

Estoy aquí escuchando algo que me da bastante miedo. Como dije antes, va a haber pocos que tienen DNSSEC. Nosotros estamos hablando de algo muy básico. Para ellos, la ignorancia es lo mejor hasta que se les venga el cielo encima. David Conrad vino el año pasado a la reunión de la Asociación de Telecomunicaciones de las Islas del Pacífico, donde están todos los operadores de telecomunicaciones de la región y les dio una muy buena charla.

Yo pensaba: “¿Cómo va enfocar esta charla?” Muchos de los operadores no son de habla inglesa y el inglés no es su primer idioma pero él habló a un nivel que realmente cualquier persona

podría haber entendido. Estos son técnicos de todos modos. Deberían haber entendido lo que él decía. Hace no tanto tiempo, yo en persona les pregunté si habían recibido algún feedback de personas que habían implementado DNSSEC. Cuando verificamos, no había nadie. ¿Qué hacemos?

ALAN GREENBERG: Kaili.

KAILI KAN: Gracias. Soy la única persona que no tiene una posición. Mi razonamiento es el siguiente. Supongamos que alguien en mi familia se agarra una enfermedad y tiene que ir al hospital. El médico dice que necesita una operación. Hay beneficios y hay riesgos. ¿Cuál es mi opinión? Yo no tengo una opinión. Yo no soy médico. Usted es el médico. Usted es el profesional y usted es el que tiene que sopesar los beneficios versus los riesgos. Es usted el que decide. Todo lo que yo quiero es que mi familia esté bien por eso yo no tomo una posición, porque no soy yo el que tiene que juzgar esto. De todos modos, yo no estoy convencido de que pueda adoptar una posición para tener un juicio sobre este tema. Esta es entonces la posición que yo tomo. Gracias.

ALAN GREENBERG:

John y yo vamos a partir en breve. Voy a hacer algunos comentarios y luego quiero hacer una encuesta aquí en la sala. En términos de programas de marketing, creo que ICANN está haciendo mucho pero si ustedes creen que tienen alguna idea de a quién hay que contactar más allá de hacerlo a través de las ALS propias, porque nosotros no tenemos que pedirles que lo hagan, hablen porque si creen que tienen una buena idea, quizá la tengan.

Yo hablé de los bancos porque Ricardo dijo que si los bancos fracasan, tenemos un problema. Los bancos a lo mejor ya están despiertos y prestan atención pero en caso de que no hayan resuelto el DNSSEC, este es otro camino de la comunicación.

Alguien hizo un comentario, no recuerdo si fue Tijani del lado de “Avancemos”, sobre las presunciones. De lo que estamos hablando está basado en presunciones de los dos lados. En última instancia, vamos a tener que tomar la decisión de avanzar o no avanzar en base a información no clara y no completa. Antes de irme, yo sé, John, que está en la lista de oradores. Le voy a dar la palabra. La sesión tiene unos 20 minutos para finalizar. ¿Hay alguien aquí que haya cambiado de opinión en base a la encuesta inicial? Holly, ¿cambió de opinión? Un comentario muy breve, por favor, porque tengo que salir.

HOLLY RAICHE: Yo votaría que sí pero me gustaría tener una seguridad en cuanto a las campañas, que van a ser amplias y que van a tener que garantizar que la interpretación de ICANN es para un advertencia proactiva. En esa condición, yo entiendo que es algo bueno pero también quiero que la ICANN haga todo lo posible. Usted mencionó el Y2K. No hubo ningún desastre por lo que hicieron. Si nosotros podemos pasar esa línea, votaría que sí.

ALAN GREENBERG: Usted puede cambiar. ¿Tijani cambia? Vamos entonces a dejarlo. Tijani quiere estar en la lista de oradores. Hay 15 minutos antes del receso, un poco más si quieren tomar parte del receso. John y yo vamos a estar fuera. Hay otra reunión fuera. No podemos ir más allá del receso. John, hable rápidamente.

JOHN LAPRISE: Quiero que entiendan mi posición con un matiz. Estoy diciendo no a la implementación en la fecha actual. Lo que quisiera es que, del lado técnico, que se analicen mejor los datos, porque en este momento la comunidad técnica no está entendiendo lo que ven en los flujos de datos. Quiero entender un poco mejor. Me gustaría que hubiese una mejor campaña de comunicación antes de la implementación. Gracias.

MAUREEN HILYARD: Vamos a continuar con la lista de oradores, los que quieran hacerlo. Le doy la palabra a Daniel.

DANIEL NANGHAKA: Soy Daniel para los registros. Yo no entiendo mucho sobre todo esto pero pareciera que hay miedo por lo que le va a pasar a Internet. Les guste o no, en un cierto punto, van a hacer la implementación. El usuario final necesita Internet, lo cual es un factor constante pero qué pasa en caso de que cuando ocurra la implementación haya quejas. Considerando que otros factores sean constantes, mi opinión es que la comunidad técnica ya entiende los riesgos del futuro. Tenemos que mitigar los riesgos. Hacer la implementación. Para aquellos que no actualizaron el sistema, deberían hacerlo porque tienen que cuidar a su clientela. Gracias.

MAUREEN HILYARD: Sébastien.

SÉBASTIEN BACHOLLET: Gracias. Hay partes del mundo donde hay más de un proveedor para conectarse a Internet. Uno utiliza uno para el teléfono, otro para la laptop. Hay otros países donde hay dos o tres compañías. No es que sean muchas y no podemos contactarlas para asegurarnos de que los usuarios finales tengan acceso. Hay

formas de mitigar la situación. No se olviden que ustedes tienen en ese caso un solo dispositivo para conectar a Internet en muchos lugares del mundo.

MAUREEN HILYARD: Javier.

JAVIER RUA JOVET: Gracias, Presidenta. En cuanto a si esto es del interés de los usuarios finales, yo entiendo que somos una región desatendida. Puerto Rico es uno de los primeros que adoptaron el DNSSEC. El .PR creo que fue el tercero en el mundo y hay otros que lo han seguido. Les importa a los usuarios finales que están cerca de mí. Gracias, Tijani, por responderme directamente con su opinión. [Alan] habló de presunciones. Creo que lo que usted me dijo es que estamos asumiendo un mundo donde la geopolítica está siendo llevada adelante por adultos y la geopolítica se lleva adelante con intereses nacionales. Trump está loco y sorprende incluso a sus allegados más cercanos. Imagínense esto en un mundo de adultos. No sé nada sobre los aspectos técnicos de esto pero sí sé lo que los políticos de derechas de los Estados Unidos quieren hacer con ICANN. Trump va a hacer lo que a él se le ocurra esa mañana. Olvídense de las presunciones. Gracias.

MAUREEN HILYARD: Gracias, Javier. Narine.

NARINE KHACHATRYAN: Gracias. Mi percepción es que el proceso de la implementación de DNSSEC se puede detener en cualquier momento. Esto es así. ¿Es posible parar el proceso si sucede algo inesperado?

MAUREEN HILYARD: Gracias. Holly, ¿quiere decir algo más? Usted está en la lista de oradores.

HOLLY RAICHE: Creo que todo se ha dicho. Si retomo lo que dijo Javier, yo dejé en claro que es muy importante que haya campañas de publicidad muy amplias. Se está hablando sobre los riesgos. Entiendo el riesgo de no avanzar. Creo que cualquier comentario que hagamos tiene que reflejar nuestras reservas. Debemos decir que estamos desilusionados si apagamos el DNSSEC por una cuestión de seguridad pero también indicar que nuestras inquietudes tienen que ver con los usuarios. Gracias.

MAUREEN HILYARD: Tijani.

TIJANI BEN JEMAA:

Gracias. Escuché muchas veces a la gente decir que nosotros no sabemos las razones de los resolutores por las cuales habría problemas. ¿A quién vamos a acudir? Este no es un problema para nada. Estos no son usuarios finales. Estamos hablando de los proveedores y los proveedores tienen contratos. Esos contratos van hasta la ICANN. Hay un revendedor, no sé, y luego un registrador, un registro, etc. Al final está la ICANN. ICANN tiene todos los registros de cada uno de estos operadores y es fácil contactarse con ellos. No estamos hablando de personas, de usuarios finales. Sí hay que saber adónde hay que dirigirse. Si hay una campaña, esta es una campaña para cada uno de los operadores. Esta es la única manera en que la campaña se puede hacer.

Segundo. Alan dice que todo está basado en una presunción. Yo diría lo siguiente. Le voy a decir cuál es la presunción. Yo digo que si nosotros no hacemos la implementación de la clave, vamos a tener un gran problema porque nosotros tenemos ya cinco años con la misma clave y hackear los servidores es algo que un hacker puede hacer. Cuando tenemos un servidor hackeado, estamos en un gran problema. Esto no es una presunción.

Tercero, yo dije: “Hagan la implementación”. ¿Cómo lo hacemos si no tenemos visibilidad y tenemos mucho miedo? Hay que ir con seguridad, preguntarles a todos los que tienen DNSSEC,

pedirles que lo apaguen, hacer la implementación, luego pedirles que vuelvan a encenderlo y si hay un problema, el que tiene el problema lo vuelve a apagar, arregla el problema y lo vuelve a encender. ¿Cuál es la presunción? No hay presunción. Gracias.

MAUREEN HILYARD: Gracias, Tijani. Nos quedan algunos minutos. Le voy a dar la palabra a Alberto, luego a Olivier y luego a Satish. Un minuto cada uno.

ALBERTO SOTO: Yo he estado trabajando más de 30 años en sistemas de los cuales más de 20 he estado a cargo de la total responsabilidad en el área de IT con las implicancias por supuesto en seguridad. Escuché tres veces hablar de miedo y no tener miedo no es ser valiente, es vencerlo. En lo que respecta a mi tarea, nunca tuve miedo. Siempre tuve la responsabilidad de hacer lo que se tiene que hacer en seguridad. Un análisis de riesgo. No es temor un análisis de riesgo. Yo hago el análisis de riesgo con una determinada información y la información que me dieron no es suficiente. No es suficiente.

Si a mí el área técnica de ICANN me da qué es lo que hizo, cómo llegó y por qué es la presunción de que no van a ser muchos los

usuarios finales que van a sufrir y que va a haber un determinado plan B, C o D de que va a haber una buena regulación, ningún problema. Yo voto por el sí. Pero hasta este momento, con esa presunción y con los cuidados que tengo que tener, lamentablemente no. Gracias.

MAUREEN HILYARD: Gracias, Alberto.

OLIVIER CRÉPIN-LEBLOND: Quería responder a Narine Khachatryan en cuanto a parar la implementación. Si la implementamos y luego decimos que no, que no funciona. Sé que Cheryl respondió pero estaba fuera de micrófono. La respuesta es que no. una vez que uno empezó la implementación no se puede volver para atrás porque algunos sistemas van a seguir avanzando y otros podrían volver hacia atrás. Sería un desorden no continuar.

MAUREEN HILYARD: Satish, está en la lista.

SATISH BABU: Tengo un par de observaciones. Una es que yo apoyo la implementación pero hay problemas tecnológicos y políticas. Los tecnológicos aparentemente no son tan serios pero lo

político... Tijani mencionó dos países, no conozco el segundo, con un problema de raíz. En caso de que esto salga de las manos, yo tengo un resolutor en mi laptop y muchos puntos de acceso no utilizan DNSSEC. Debemos tener una estimación de algún estudio donde se diga cuál es el porcentaje de Internet que está bajo amenaza y cuál es el número que escuchamos, si es que es realista.

Seun dice que es imposible hacerlo pero quizá la ICANN tenga algunos medios. Quizá pueda generar alguna caja donde la pueda testear. Yo tengo más miedo de lo que menciona Javier en los temas políticos. Por un lado tenemos a Trump y por otro lado tenemos a otros países. Esta es la situación que en realidad me asusta más, más que los problemas técnicos.

MAUREEN HILYARD:

Gracias a todos. Tenemos casi 90 minutos de una excelente discusión. Yo aprendí tanto sobre este tema a pesar de que no fui a la última sesión. Quisiera que Cheryl haga un resumen. Una de las cosas que quisiera decir es que nos vayamos de aquí con un resumen y encontrar quizá algún redactor. Quisiera tener algo que podamos presentar. Hay tantas buenas ideas que hay una necesidad de tener más información, más comunicación, entre este momento y octubre. Les voy a dejar que lo hagan.

CHERYL LANGDON-ORR: Gracias, Maureen. Esta es una de esas ocasiones extrañas en la cual se me dificulta recordar si alguna vez hubo un debate tan interesante como el que tuvimos hoy. Felicidades. Desde mi punto de vista como observadora, creo que han tenido un debate muy fructífero. Si no entendí mal, esta conversación no finaliza aquí. Todavía hay puntos a considerar y, como acaba de decir Maureen, quizá podríamos tener a una o dos personas que consoliden las ideas que hemos escuchado hoy y que las compilen en la página wiki para que la gente que está apasionada sobre este tema lo pueda seguir comentando y veamos si podemos llevar esto que hemos debatido hoy a un documento.

Seguramente haya cosas que requieran aclaración. Un par de veces pensé que una de las cosas que se deberían mejorar son los potenciales efectos políticos. También escuchamos ideas que decían: “Traigan a la gente que tiene los resolutores”. ¿Por qué no prepararnos y estar listos para avanzar y hacer un ejercicio agresivo para minimizar el efecto sobre la ICANN? Creo que aquí hay una diferencia a veces de punto de vista pero les voy a proponer a todos, obviamente sé que a Alan también les gusta el tema, pero hay argumentos a favor y en contra así que le podemos por ejemplo pedir a Javier que tome la posta para una de las ideas y a Maureen para que tome la posta para otras. También Hadia. Podríamos hacer un ejercicio breve de redacción

para volcar todas las ideas y que después las podamos también volcar en la wiki.

SÉBASTIEN BACHOLLET: Hay tres nombres en el Skype que están diciendo que quieren ser voluntarios para redactar o hacer este ejercicio. Pueden ser Bastiaan, Seun y Aida. Esa sería mi sugerencia.

CHERYL LANGDON-ORR: Por supuesto, esto no tiene que ver con redactar el documento sino que más bien tiene que ver con hacer un resumen de las ideas. Si se decide que haremos comentarios, también necesitaremos redactores para estos comentarios. Vamos a darle tiempo, Maureen, a que se contacte con el resto de las personas. Seguramente durante esta reunión vayan a tener que hacer tiempo para poder reuniré y hacer esta redacción. Ahora, como hacemos habitualmente, hay una reunión en esta sala. Creo que tendríamos que despejar los espacios lo más rápido posible. Nuevamente, les vuelvo a agradecer a todos por una sesión que ha sido tan productiva.

MAUREEN HILYARD: Muchas gracias a todos. Voy a necesitar que se queden Hadia, Seun...

MAUREEN HILYARD: Seun, Bastiaan, Hadia, por favor.

[FIN DE LA TRANSCRIPCIÓN]