
LONDRES – Resumen de parte del Grupo de Trabajo de Expertos (EWG) acerca del Informe Final sobre Servicios de Directorio de gTLD
Lunes, 23 de junio de 2014 – 15:15 a 16:15
ICANN – Londres, Inglaterra

JEAN-FRANCOIS BARIL: Bueno. Creo que podemos comenzar, Buenas tardes, a todos, sean bienvenidos a esta sesión pública del Grupo de Trabajo de Expertos. Soy Jean Francois Baril y soy el facilitador de este grupo.

Estoy muy feliz de estar aquí con ustedes y con mis colegas de este grupo para dar un panorama general de nuestro informe final sobre los servicios de directorio para gTLD, para la próxima generación.

Este informe fue publicado el 5 de junio. Durante la próxima hora aproximadamente vamos a tratar los siguientes temas, después de darles un pantallazo general acerca del EWG, le voy a dar la palabra a mis colegas en el panel para analizar las cuestiones más importantes de nuestro informe, luego veremos los pasos a seguir y finalmente hemos preparado dos sesiones de preguntas y respuestas.

La primera, tiene que ver con lo siguiente. A los efectos prácticos, porque creo que a las 06:30 todos van a estar ocupados, entonces, creo que a los efectos prácticos proponemos trabajar de las 04:30 a las 06:30 en esta sala, de manera tal de tener dos horas de diálogo fructífero y profundo acerca de la esencia del informe en sí mismo.

El día miércoles por la mañana, de 08:00 a 10:00 am tendremos una nueva sesión de debate y aclaración acerca de los elementos del informe y del proceso de nuestro grupo de trabajo.

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 archive, pero no debe ser considerada como registro autoritativo.

Entonces, retomando el origen de nuestro grupo de trabajo, bueno, este grupo fue creado a iniciativa de Fadi Chehade y de la Junta Directiva de la ICANN en febrero de 2013, para destrabar este punto de atascamiento respecto del WHOIS y todos los problemas que tienen que ver con la obtención y el mantenimiento de datos de registración de los gTLD.

Luego por supuesto, proponer una solución para la nueva generación de estos servicios que funcione mejor en pos o beneficio de la comunidad global de internet.

Entonces, esto debería ser la base o el fundamento para ayudar a la comunidad de la ICANN para que a través de los procesos de la GNSO genere una nueva política de servicios de directorio para gTLD.

Como ustedes saben, el modelo de múltiples partes interesadas basado en el consenso y de abajo hacia arriba es realmente algo que presenta un desafío y una dificultad para crear o generar una visión unificada o convergente, pero por otro lado, es muy satisfactorio ver que se llegan a conclusiones sólidas, cuando las personas están genuinamente contribuyendo de manera positiva en pos del beneficio de todos.

Entonces, es muy bueno tener estas discusiones o estos debates con la participación de todos como personas, como individuos, a título individual y no en representación de.

También tenemos que tener en cuenta la cortesía, la cooperación y el compromiso de todas las partes.

Entonces quiero resaltar esto último que acabo de decir, el compromiso de todas las partes.

Porque si no nunca hubiéramos llegado a una solución. Dicho esto también trabajamos muchísimo y tuvimos que comprometer mucho

esfuerzo, pero esto es quizás el precio a pagar si queremos una internet en la cual todos podamos confiar o tener mayor confianza.

Esta es una oportunidad muy buena para presentarles a estos voluntarios maravillosos, estos voluntarios trabajan denodadamente, prácticamente 24 horas al día los 7 días de la semana. Ellos son los artistas de esta obra, yo soy el experto, pero estas personas realmente han hecho un trabajo sorprendente.

La cantidad o la carga de trabajo es una cosa, pero a mí me complace mucho decir que hubo mucha calidad en este trabajo y una gran actitud que se traduce en todo, todo este largo camino que hemos recorrido juntos y en cómo se complementa sólidamente este equipo.

Nosotros contamos con Chris, Scott, Susan, Nora, Michelle, Mike, Stephanie, Rod, Carlton, Faisal y Fabricio, bueno, para mí realmente es un placer felicitar al personal de la ICANN por su eficiencia y efectividad, sobre todo a Denise, a Margie y a Lisa. Me gustaría que se pongan de pie para que todos las reconozcan y les agradezcan este trabajo excepcional que han realizado.

Y francamente sin ellas este informe no habría sido posible, porque es realmente complejo integrar todas estas cuestiones y el resultado de este debate tan activo y ellas realmente fueron muy creativas para poder ensamblar todo esto y conectar todos los aspectos en la forma correcta.

Con lo cual estoy muy agradecido, les estoy muy agradecido.

Cada uno de estos miembros fue seleccionado cuidadosamente, entre más de 70 expertos calificados en todo el ecosistema de internet y en todas sus geografías.

El factor de toma de decisiones se basó en un buen equilibrio entre la capacidad operativa y una experiencia concreta.

O sin ello este resultado no habría sido posible. En este caso, esto significa tener una actitud tendiente hacia el consenso, ver el panorama general y servir a la comunidad global de internet en lugar de promover el interés propio. Tener la capacidad de hablar con libertad y sinceridad y no estar mentalmente bloqueado debido a la postura de una unidad constitutiva en particular. Esto significa pensar por uno mismo y también pensar fuera de las soluciones de siempre y buscar la mejor solución para evitar el “status quo”.

Francamente, puedo sentirme orgulloso en informarles que hemos demostrado tener todas estas habilidades que acabo de mencionar. Y esto es probablemente la parte más importante de esta magia, si se quiere, que nos ha permitido llegar a los principios y a las recomendaciones de este informe que son más de 180.

Nosotros trabajamos en nuestro grupo, y hemos reflejado el enfoque que hemos adoptado en nuestro informe.

En primer lugar, bueno, les pido disculpas por estas 166 páginas que tiene el informe, pero, a pesar de que quisimos resumirlo y hacerlo más simple la extrema complejidad de esta situación que lleva tanto tiempo de atascamiento llevó a que tuviéramos que dedicarle tanto tiempo y tanto esfuerzo, mucho más de lo que yo hubiese previsto.

Quizás al principio fui un poco ingenuo, pero es esta la realidad, estas 166 páginas de recomendaciones son el resultado de unos intensos 15 meses de trabajo con horas de investigación en profundidad de procesar muchas páginas de comentarios públicos, respuestas a diferentes encuestas, investigaciones de todo tipo, 19 consultas públicas a la comunidad, 35 días de reuniones presenciales, y 42 llamadas o teleconferencias de este equipo. Y por supuesto muchísima interacción con expertos externos y miembros de la comunidad.

Aun así, nuestro mecanismo para llegar a consenso no fue perfecto y en realidad esperábamos que Stephanie Perrin escribiera un documento en disenso para ser publicado junto con el informe final de nuestro grupo. Y bueno, eso es algo normal porque no podemos estar de acuerdo en todo.

Desafortunadamente, no pudimos tener un debate antes de la publicación, pero estamos trabajando entre nosotros acerca de esto y seguramente podremos publicar esta postura de disenso en nuestro blog de nuestro grupo de trabajo.

Bueno, muy bien, todo este trabajo para qué. Para responder a una pregunta simple, ¿hay una alternativa al WHOIS actual para darle un mejor servicio a la comunidad global de internet?

Bueno. Cómo podemos contestar esta pregunta tan interesante con respecto a la dificultad de las cuestiones de privacidad, la calidad de datos, la exactitud de los datos, la protección de los datos, y lograr un equilibrio entre el acceso a los datos también o con el acceso a los datos también.

Este informe refleja muchísimo análisis por parte de muchos de los expertos dentro y fuera de la comunidad. Probablemente no sea ciento por ciento perfecto per, reitero, que es el resultado de muchos, muchos acuerdos entre muchas personas y no podemos decir “yo cedí más o cedí menos”. Creo que todos hicimos importantes acuerdos para llegar a esta postura a pesar de las diferencias y las divergencias. Pero siempre con mucha honestidad intelectual.

Este es uno de los valores principales que nos ha guiado durante este proceso que ha durado 15 meses. Así que, junto con todos los miembros de este grupo tengo plena confianza de que este informe sea un fundamento sólido para responderle a la comunidad de la ICANN

respecto de un remplazo para el sistema de WHOIS y realmente es un avance o es algo revolucionario en cuanto a internet y al futuro de internet.

También tenemos plena confianza de que este informe cumple con las directivas de la Junta Directiva de la ICANN y que es sólo el comienzo, es apenas el comienzo de un diálogo constructivo y un PDP exitoso dentro de la GNSO.

Dicho esto me gustaría darle la palabra a Fabricio para que nos explique por qué decidimos esta opción o cambio de paradigma para remplazar a WHOIS.

FABRICIO VAYRA:

Gracias Jean Francois. La pregunta era, ¿hay una alternativa al WHOIS que tenemos hoy en día? Y nuestro grupo decidió que sí. Hay una alternativa para el acceso anónimo a lo que normalmente son datos poco precisos. (inaudible) de nuestro pequeño tacho de basura. La comunidad nos está diciendo que WHOIS está lleno de basura.

Entonces, es el momento de mejorar, de optimizar, y esperemos que nuestra recomendación logre esto.

Qué dice este documento de 166 páginas, contiene más de 180 recomendaciones para nuevos servicios de registro de directorio, lo que tratamos de hacer es lograr un equilibrio entre precisión, acceso y responsabilidad.

Y uno de los mecanismos que sugerimos en cuanto a la responsabilidad tiene que ver con el acceso basado en propósito. Hoy en día uno puede tener acceso a los datos, quizás son datos basura pero podemos tener acceso en cualquier momento sin tener ninguna responsabilidad. Lo que sugerimos es un sistema donde todos estén en igualdad de condiciones

y hay responsabilidad de los que buscan los datos. Y tienen que buscar con un propósito específico.

Fines permisibles, nuestro modelo de datos con acceso restringido que quede afuera. Bueno, que quede afuera (inaudible) muy pocos datos con respecto a la información que identifica a las personas, es un correo electrónico.

Todo lo demás está protegido. Tenemos los datos del sistema, metadatos, los datos de registros, tenemos datos de registrador, de registro, cuando se creó el dominio, cuál es el DNS, etc. Si ustedes quieren información sobre el (registratario), deben ser autenticados, tienen que pasar por esta restricción de acceso una vez que pasaron esta restricción tienen que decir para qué quieren acceder a esos datos y por qué lo hacemos así, porque pensamos que la responsabilidad era lo que faltaba en todos lados. Mucha gente habla de responsabilidad de los que ingresan los datos a una base de datos pero también es responsabilidad para aquellos que acceden a los datos, para los que los almacenan, los que los divulgan, por lo tanto necesitamos una base de datos con propósito y con autenticación.

Y lo que van a ver obviamente cuando lean el informe, y sé que muchos todavía no lo leyeron, es bastante largo, hay dos nuevas partes en el ecosistema, lo que validan y los que gestionan o administran (inaudible) y van a ser parte contratadas. Esto lo van a encontrar en términos generales en el informe y espero que ustedes opinen igual que nosotros que esto es una mejora. Un gran paso adelante y un modelo necesario que por supuesto, necesita muchas correcciones. Y ahora le doy la palabra a Susan.

SUSAN KAWAGUCHI:

¿Por qué crear un nuevo RDS? ahora que – en ese momento WHOIS da acceso del mismo modo a todos los usuarios anónimos y sabemos que esto no sirve. Tiene poca responsabilidad, poca protección de la privacidad, pocas soluciones para los casos de uso indebido, poca capacidad de garantizar la integridad de los datos, difícil manejo de los contactos y comunicaciones ineficientes, así que estamos tratando de resolver todos estos temas y espero que encontremos soluciones para resolver todo esto. Entonces nuestra solución es el acceso con propósito.

Algunos datos de registro, de registración van a seguir siendo públicos para promover la estabilidad de la internet y satisfacer los requerimientos básicos de DNS, estos datos públicos cualquiera puede acceder a los mismos, con fines permisibles sin autenticación, entonces, sí, van a encontrar cierto nivel de información pero no van a encontrar toda la información a la que acceden hoy en día.

Entonces si comparamos lo que estamos sugiriendo con lo que tenemos hoy en día, el diagrama que tenemos arriba es lo que tenemos hoy en día.

Es el WHOIS actual, son datos públicos, si uno ingresa información correcta, precisa en un registro WHOIS, todo el mundo lo puede ver.

Y el acceso es totalmente anónimo. Los (registrararios) no pueden proveer datos contemporáneos o actualizados. Hoy en día hay muchas formas de contactar a las personas y el WHOIS actual no permite esto.

También los contactos no pueden impedir el uso fraudulento, alguien podría utilizar la información de mi vecino o de mi empresa, no hay nada que impida hacer esto. Entonces hemos analizado todos estos aspectos, estas cuestiones y con DRS con propósito creemos que

podemos evitar algunos de estos usos indebidos. Entonces tenemos los datos de nombres de dominio actuales y allí ven todas las flechas o las cruces, son datos protegidos. No consideren que es una restricción de acceso única, no es una enorme puerta donde uno entra y después llega a un pasillo con muchísimas puertas o muchas puertas pequeñas, no, dependen del propósito y lo que ustedes nos dijeron sobre ustedes para poder acceder a los datos, así que ustedes cuando uno llega a la puerta de entrada, uno no entra directamente, uno tiene que decirnos quién es. Y para qué usa los datos. Creo que esto es muy importante si queremos conocer los datos personales de alguien debemos proveer nuestros propios datos personales, entonces la mayor parte de los datos van a estar protegidos en forma predefinida, los datos de contactos se validan, las ID todos los datos están relacionados con identidad, es un número de 8 dígitos, es lo que hemos sugerido, vamos a ver qué funciona para la comunidad y esto es lo que obtienen en primer lugar, el ID de contacto. Este ID de contacto no significa que van a recibir el nombre, la dirección, el número de teléfono, nada de eso, esos no son datos públicos mínimos.

También hemos establecidos reglas adicionales, o estamos sugiriéndolas por lo menos. Hay diferentes objetivos para contactar a un (registratario) de un dominio y es se categoriza si quieren hacerlo, un (registratario) puede actuar con su propio objetivo o propósito, un PPC, pero hay una cantidad, un conjunto mínimo de datos que no están restringidos.

Así que cuando consideramos los datos públicos mínimos que vamos a ver en un minuto, hay tres categorías. Hay una categoría muy amplia a la izquierda, datos de nombres de dominio suministrados por el

registrador y el registro, son conjuntos de datos, fecha de actualización, estatus, información que otros quizás necesiten utilizar y ver.

Y a la derecha arriba tenemos la información de contacto del (registratario), hay un ID asociado con ese número con el (registratario). Pero hay una cantidad mínima de datos públicos disponibles. Y después en ese conjunto de datos mínimos tenemos el ID de contacto con propósito, tal vez un número, nada más que eso. Entonces si ustedes no nos dicen quiénes son ustedes o no le dicen a (...) quiénes son ustedes y por qué quieren la información no van a poder pasar por la puerta, pasar por esta restricción para encontrar más información.

Este es un ejemplo del diagrama verde que acabamos de ver. Así que pueden ver a la izquierda, tenemos los datos del (registratario) y del registro, esto es importante que todo el mundo lo vea, y no hay información personal allí del lado izquierdo.

Del lado derecho, tenemos el nombre de dominio, el servidor de nombres, el tipo de (registratario), que puede no informar, tenemos opciones aquí, si una empresa dice “sí, yo soy una empresa”, bueno, pueden presentarse como empresa en esa categoría, pero no es obligatorio, es opcional.

Ustedes reciben un ID de contacto de (registratario), que es un número una vez más, y después también pensamos que era importante conocer o saber cuándo se validó por última vez la información con respecto al (registratario).

Se hace una vez por año, cada seis meses, cada diez años. Es importante saber cuándo se actualizó por última vez.

Y después, la dirección de correo electrónico del (registratario). Todo el mundo necesita esa dirección. Incluso para la gestión técnica del

nombre de dominio. Los consumidores tienen que poder contactarse con el dueño del dominio.

Después, el país del (registrar), después en la presentación vamos a hablar sobre el motor de reglas. La posibilidad de poder asociar el registro de un dominio con la legislación aplicable en el país donde está el (registrar). Por eso tenemos este elemento de datos aquí.

Después tenemos los contactos con propósitos, los PBC, una vez más, sólo se recibe un número.

Esto es lo único que ustedes verán y después si necesitan contactarse con alguien, ya saben la dirección de contacto del (registrar), si quieren hablar con el contacto técnico, en ese caso tendrán que pasar por esas puertas, restricciones de acceso, pero tendrán que elegir la puerta adecuada para recibir la información que buscan y tendrán que dar información sobre ustedes mismos para obtener esta otra información.

Si quieren obtener los datos públicos mínimos ingresan al sistema y buscan el nombre del dominio, pero sólo van a ver los datos públicos, tienen que declarar un propósito si no declaran un propósito no van a poder acceder a los datos de acceso restringido. Y hemos establecido algunos de los propósitos, ahora no sabemos si tenemos todos los propósitos en la lista, probablemente no los tengamos. Realmente nos esforzamos aquí pero dudo que tengamos todos los propósitos posibles. Una vez más, lo que se devuelve de una consulta son los datos públicos, los datos públicos mínimos y le doy la palabra a mi colega.

ROD RASMUSSEN:

Gracias Susan. Hablemos de ese corredor de puertas. La pregunta no es una sola puerta, la restricción de acceso no es una restricción, es la

capacidad de proteger los datos a nivel adecuado, para los propósitos para que se los utiliza.

Si se fijan en las calidades, lo que describimos aquí desde el punto de vista de la ingeniería, es un sistema de control de acceso basado en roles. Que se usa mucho en el mundo corporativo, donde a veces no hay una sola forma de acceder. No tenemos un registro único. Yo me registro según el tipo de privilegios que tengo, puedo acceder a ciertos datos y no a otros en ese sistema; es bastante claro desde ese punto de vista.

Ahora, para nuestro sistema lo que sugerimos aquí está basado en una combinación de quién es la persona, cuál es su propósito declarado, cómo se lo autenticó, y las reglas del sistema propiamente dicho para brindar los datos.

Este control de acceso permite proteger los datos y también permite hacia las personas responsables por la forma en que utilizan el sistema. Y viendo como es el sistema de modo conceptual es bastante claro, tenemos una persona acreditada a un determinado nivel que tiene una credencial de acceso, accede al sistema (...) que puede tomar datos de registro, registradores, validadores, donde están almacenados y le devuelve los datos a la persona que los pidió en base al pedido que hizo. Puede haber múltiples métodos, es muy importante comprender esto.

No es necesariamente una persona sentada frente a una computadora, como vemos en la diapositiva, esto permite conectarse con otros sistemas de autenticación. Después vamos a hablar de esto cuando hablemos de la validación. Pero es muy importante saber que esto no es simplemente una persona que busca el nombre de dominio y una persona sentada frente a una computadora, esto es uno de los métodos, no el único.

Esto seguramente ya lo conocen, la mayor parte de ustedes que han visto el trabajo que hicimos en los últimos 15 meses, son los datos de registros, los propósitos permisibles, y agregamos en el último informe final, conceptos que tienen que ver con transparencia de DNS, ya que esto es importante para la ICANN y para toda la comunidad. Y es tener transparencia en cuanto a la forma en que funciona el sistema y también tenemos investigación sobre los nombres de dominio definidos en el informe. En el informe definimos qué esto, pero implica poder hacer el tipo de estudios y análisis que ha hecho la ICANN para brindar información sobre la calidad de la información, sobre cómo se utilizan los nombres de dominio, etc.

Esto es lo nuevo que quizá no hayan visto en el informe anterior. Todo lo demás ya no ha cambiado mucho con respecto a versiones anteriores.

Todos los propósitos permisibles tienen necesidades de datos que pueden ser diferentes según los nombres de dominio involucrados. Podemos obtener datos que sean públicos, ya hablamos de los datos que tienen que ver con la creación del nombre de dominio. Tenemos datos de acceso restringido, y también aquí tenemos algunas disposiciones con respecto a la información que está en WHOIS, que es información histórica, consultas inversas que permiten encontrar nombres de dominio que tengan que ver con un contacto determinado. Algunos de esos propósitos se utilizan ampliamente y tienen una cantidad de requerimientos mínimos para acceder a esa información.

En otros casos se requiere un proceso de acreditación muy formal, y esto pasa cuando los datos son más sensibles, en ese caso hay más controles de alguna manera, alguien controla las credenciales del que

pide los datos y se analiza también para evitar que se use de forma indebida.

Hablemos de los contactos con propósito.

La idea, bueno, hay muchas ideas aquí de hecho, en estos contactos con propósito. Esto permite un mejor control de la información personal por parte de un experto o una persona o empresa con respecto a su información personal. También permite una mejor portabilidad de los datos de contacto. Entonces tenemos el rol del (registratario) muy claro, es el que controla el nombre de dominio, pero también tenemos estos diferentes contactos con propósitos que incluyen usos muy comunes de dominios a quienes terceros externos quisieran contactar.

Entonces, por ejemplo un contacto técnico debería proveer respuestas a problemas técnicos, entonces, la persona (...) que debería ser el contacto técnico debería ser un ISP, una empresa que provee servicios de “hosting”, etc. Alguien que puede responder preguntas técnicas.

No es necesariamente la persona que ha registrado el nombre de dominio que quizás no sepa cómo se gestiona un sitio web y haya tercerizado estos servicios.

Bueno, con estos datos ustedes pueden acceder directamente a la persona que se ocupa de los aspectos técnicos. Lo mismo pasa con los otros tipos de contactos donde quizás haya temas legales, control administrativo del nombre de dominio. Los dos que tenemos a la derecha de ustedes, bueno, también a mi derecha en mi computadora, son opcionales. Según el tipo de (registratario) que sean. Si están utilizando un servicio de privacidad o representación pueden incluir este dato de contacto para recibir estos servicios de privacidad y representación, para cumplir el proceso de revelación o poder encontrar a la persona que esté atrás de este dominio. Si es una

empresa también pueden presentarse como empresa y vende información que haga que sea más fácil para los consumidores o clientes ponerse en contacto con ustedes para resolver algún problema si lo hubiera.

Estos son los contactos con propósitos.

Ahora, los datos de contacto que tenemos aquí, en gran parte estos datos están con acceso restringido, pero como dijimos, hay diferentes puertas por las que pueden pasar para llegar a diferentes tipos de datos. Y eso es lo que vamos a ver ahora.

No creo que lo puedan leer porque la letra es muy pequeña, les pido disculpas.

Estas diapositivas están en la página web de esta sesión, allí las podrán ver mejor y leer mejor.

En este ejemplo, alguien que quiere ponerse en contacto con alguien que está en contacto con un nombre de dominio por algún motivo legal, bueno, hablamos mucho de este tema.

¿Cómo funciona el proceso desde el punto de vista del control de procesos?

En primer lugar, vemos si el usuario está autenticado, si no, no le damos datos. Solamente los datos públicos como ya se dijo antes.

¿Está autorizado para este propósito, para entrar y pedir estos datos?

Supongamos que está - que entró al sistema del usuario y ha sido autenticado solamente para información técnica, entonces no podrá entrar y buscar los datos de contacto legales, porque tiene este otro rol.

Supongamos que sí está autenticado y autorizado para obtener datos y para obtener información legal. La pregunta es, ¿está pidiendo información sensible protegida?

Si no está pidiendo esta información o no está autenticado para recibir este tipo de información la respuesta será, la información que está bajo ese contacto que sería la parte de información más pública, entonces en este caso la información de contacto legal que incluye el nombre, ni siquiera yo puedo leer esta letra, el nombre, la dirección de contacto, todo lo necesario para presentar una causa, llevar a cabo un proceso legal.

Si piden datos de acceso restringido y han sido autorizados, bueno, si no están autorizados sólo le damos los datos públicos, si están autorizados para recibir estos datos restringidos, con respecto al contacto legal, bueno, le damos todos un conjunto de datos de acceso restringido.

¿Cuál es el proceso de aprobación? Bueno, esto está basado en políticas, y eso lo va a definir el PDP.

Este es el proceso, así es como se avanza. Uno entra por una puerta, una restricción de acceso, para llegar a diferentes elementos de datos que necesitamos para cumplir con nuestro propósito.

Y creo que ahora le doy la palabra –no, no le doy la palabra a nadie – tengo una diapositiva más.

Entonces, estos son algunos comentarios generales sobre lo que podríamos encontrar en cuanto a datos de contacto con propósito.

No son necesariamente los datos relacionados directamente con una persona (inaudible), información sobre servicios de privacidad y representación que están insertados allí.

Entonces uno puede utilizar servicios de representación y trabajar de esta manera.

Si uno no eligió esto y muchas personas no tienen ese tipo de contactos, no lo necesitan, pueden poner su propia información allí, es correcto, hay dos o tres tipos de datos que se pueden elegir para ingresar aquí. Y

la persona – cada persona que tiene información de contacto puede decidir si protege los datos o no.

Supongamos que yo soy un abogado y trabajo con muchas personas que tienen muchas carteras de dominios y yo quiero que se pongan en contacto con los dominios de mis clientes, yo publico toda esa información para que todos me puedan contactar si quieren hablar de un tema de UDRP o lo que fuera.

Yo, como abogado, puedo usar esa información de contacto y puedo poner esa misma información en todos los nombres de dominio de todos mis clientes, y si cambio mi número de teléfono o dirección sólo cambio una vez y aparece en todo el sistema.

Y ahora le paso la palabra a Lanre.

LANRE AJAYI:

Muchas gracias. Tenemos una serie de medidas nuevas, nuevos conceptos, para mejorar la calidad de los datos.

Un concepto importante de mejora es este acceso restringido que ha sido definido por las dos personas que tomaron la palabra antes de mí.

Pero quisiera señalar que los (registraros) tienen que prestar atención al hecho de que hay información sensible que se pone detrás de estas restricciones y cuando protegemos los datos sensibles, tendemos a mejorar la calidad de los datos.

Otro concepto importante es la separación del directorio de contactos del directorio de nombres de dominio.

Son dos directorios independientes.

Y ahora las empresas no pueden comentar sobre los datos que están en el RDS.

Y lo más importante es que hemos introducido un nuevo actor llamado “el validador”.

Si el (registratario) no maneja correctamente este concepto de acceso restringido para dar datos preciso, el validador está allí para hacer su trabajo, para garantizar que los datos que se ingresan a (...) hayan estado correctamente validados. Es un nuevo concepto y es muy importante para garantizar la calidad de los datos.

Y se reducen los casos de robo de identidades por el concepto de validación de identidad.

Voy a hablar más de esto después.

Los contactos (inaudible -31:46:3) también mejoran la uniformidad especialmente cuando hay un dominio muy grande se pueden actualizar los contactos una sola vez a través del validador.

Eso también ayuda a mejorar la calidad de los datos.

Y los contactos pueden utilizar cualquier validador, ya que esto cumple y esto se debe cumplir en cada caso, las leyes locales de protección de datos. Si se trabaja con un validador local se puede presentar quejas o reclamos bajo el paraguas de legislación de protección datos locales.

Estas son las nuevas medidas que estamos introduciendo en el RDS para mejorar la calidad de los datos.

Ahora, voy a explicar el proceso de validación.

Acá, en este diagrama, tenemos una persona con el nombre Z, que tiene una dirección de correo que es Z@isp.

La persona que presenta esto o presenta elementos de datos en este caso, la dirección de correo electrónico, al validador. Y este es el proceso de validación lo que vemos aquí.

En primer lugar se verifica si los datos son válidos, es decir, si el formato es correcto. En este caso, está ok. Y después se verifica si tiene la @, si

el formato es el adecuado pasa al próximo paso de la validación, que es la validación operativa. En este caso se verifica si se puede mandar un correo electrónico a esa dirección de correo.

Después, si el (registratario) desea que se valide su identidad se realiza este proceso y si la validación de identidad es correcta y es válida, se le asigna un ID de contacto y una credencial.

Si en algún paso de esto hay algún error o algún dato indebido el (registratario) recibe mensaje de error. Entonces este es el flujo del proceso de validación.

Entonces, tenemos que ver que hay tres tipos de validación. La validación del sistema que es obligatoria para todos los elementos de datos; la validación operativa que es obligatoria para alguno de los elementos de datos y la validación de identidad que es totalmente opcional.

La puede hacer la persona que quiera, pero no es obligatorio, como ya dije, hacer la validación de identidad.

Acá en esta diapositiva, vamos a centrarnos en la importancia del directorio de contactos (...) porque es un nuevo concepto y creemos que ayuda a mejorar la calidad de los datos.

El directorio de contactos RDS contiene datos del directorio de nombres de dominio, los (registratarios) y los contactos con propósitos mantienen –van a crear y mantener sus propios datos de contactos utilizando los validadores, como ya dijimos, antes de pasar al registro el nombre de dominio.

Pero separando la validación de los contactos del registro de los nombres de dominios, tendemos a lograr lo siguiente.

En primer lugar, eliminamos esta tarea compleja de validar los contactos.

Ya no lo tienen que hacer los registros ni los (registratarios). Esto no quiere decir que los registros y los (registratarios) no pueden actuar como validadores.

El objetivo de la validación es garantizar los datos, los (registratarios) pueden trabajar con validadores locales, que es muy importante, ya hablamos de idioma local y de todos esos temas. Y también es importante que hablemos de la legislación local aplicable y supongo que esto es todo antes de darle la palabra a Faisal.

Hay una pequeña ilustración arriba a la derecha, para subrayar la importancia del principio de ID de contacto.

En el primer recuadro tenemos el nombre de dominio para un (registratario), con la ID de contacto del (registratario). Uno, en el segundo recuadro tenemos el ID de contacto del (registratario) número 2, pero ambos ID actúan como su propio contacto administrativo.

Lo que tienen en común y si se fijan en el tercer casillero, tenemos el contacto técnico, el ID de contacto técnico, el número 3.

Lo importante aquí es que con ID de contacto 3, el contacto técnico, actualiza su información de contacto, ese cambio se refleja en todos los registros de dominio que tenemos en la base de datos. El contacto técnico no tiene que actualizar la información de contacto en todos los dominios, sólo lo hace una vez, y esta es la ventaja de este concepto de ID de contacto.

Y ahora le doy la palabra a Faisal Shah, que va a hablar sobre los diferentes modelos.

FAISAL SHAH:

El EWG analizó diferentes modelos, y cada uno de estos modelos difieren en cuanto a la forma en que se hacen consultas contra los datos o la forma en que se copian los datos en el (...)

Y específicamente analizamos el WHOIS actual y analizamos los elementos que tenían, después analizamos un modelo federado que era un modelo distribuido que toma datos de los registros y los validadores. Después analizamos un modelo sincronizado, y es aquí donde los datos se envían a un centro común, después se distribuyen a múltiples centros de datos.

Y pueden ver que tenemos en el modo sincronizado un asterisco.

Y hemos modificado, pasamos de conjunto reunido a sincronizado. Y después vamos a hablar de esto.

SCOTT HOLLENBECK:

Queremos hablar de esto porque después de la reunión de Singapur nos dijeron, ¿qué significa compilar, agregar?

Nos reunimos como grupo y tratamos de encontrar una buena definición y dijimos “bueno, tampoco nos gusta la palabra a nosotros”, entonces pensamos que sincronizado describe mejor el movimiento y administración de los datos y las funciones, de manera controlada, uniforme y segura.

Entonces, en lugar de justificar por qué utilizamos la palabra “reunido”, pasamos a “sincronizado”.

FAISAL SHAH:

Y para aclarar esto creo que de alguna manera es un nombre incorrecto porque no debe haber una distribución de datos. También hablamos de otros modelos, un modelo regional, donde (inaudible -22:43), el modelo

de exclusión voluntaria y el modelo de “by pass”, y los registros pueden elegir el modelo que quieren. Tenemos el modelo de “by pass” donde los datos se pasan de los registradores directamente al RDS, saltando a los registros y varios de estos modelos fueron mencionados por la comunidad, por eso los incluimos y los analizamos.

Y la clave para nuestro análisis en el EWG es que todos estos modelos, en todos los casos el (...) fue la fuente autoritativa que da acceso restringido a los datos.

La idea era (...) esos modelos con (...) distribuida con los datos incluidos en varias bases de datos de varios centros de datos.

Entonces tomamos todos estos modelos y EWG analizó todos los modelos, los comparamos con ciertos criterios, hicimos análisis muy estrictos incluyendo factores, como por ejemplo, ¿cuáles son las consecuencias de seguridad -con respecto a seguridad -con respecto a esos modelos?, ¿cuáles son los temas de privacidad y de competencia que tenemos que tener en cuenta?

Analizamos los requerimientos de implementación, ¿un sistema estaría mejor preparado que otro para cumplir con los requerimientos que pedimos y que tenemos en la lista de nuestro informe final?

Nos fijamos en los requerimientos de acreditación, también cuál sistema era mejor, y también analizamos los aspectos operativos.

Después de este análisis, y después de mucho tiempo, terminamos con dos modelos que se destacaban de todos los demás y estos son los dos modelos en los que nos vamos a centrar ahora.

Son el “federado” y el “sincronizado”.

Luego volvimos a analizar estos dos modelos específicos y le pedimos a un tercero externo, en este caso IBM, que analizara los costos, teniendo en cuenta estos dos modelos e IBM presentó su informe de análisis del

costo del modelo de implementación, y creo que esto se presentó el 6 de junio.

Y en base a este estudio de IBM y en base a nuestros análisis regionales y los requerimientos específicos que están descritos en el informe, EWG recomienda aceptar o adoptar el modelo sincronizado.

En la próxima diapositiva tenemos el modelo sincronizado y este modelo tiene algunos aspectos complejos, pero pueden ver que aquí están bien explicados, y si seguimos el flujo podemos ver que los datos de nombre de dominio son registrados por los (registraros) o por los registros. El validador guarda los datos de contacto y después los envía al RDS.

Y después los (registraros) al mismo tiempo envían los datos de nombres de dominio y los ID a los registros y en los registros lo mandan al RDS.

Susan habló antes de esto.

El modelo sincronizado, el DRS es responsable del almacenamiento de las copias de los datos validados, manejan todas las consultas públicas, autentica, autoriza acceso, aplica estas políticas de restricción de acceso a los datos, hace una auditoría y también da servicios adicionales.

Como por ejemplo, las consultas inversas, y servicios similares a los que tiene WHOIS.

Por supuesto hay diferencias entre el sistema federado y el sincronizado. Y quizás Scott pueda hablar un poco sobre esto ahora.

SCOTT HOLENBECK:

Sí, ojalá tuviéramos una copia del modelo federado para poder comparar ambos. Porque la mayor diferencia es que este otro modelo tiene flechas yendo en todas las direcciones, pero no las podemos ver.

Conceptualmente este es un modelo más simple, cuando decimos que “sincronizado” –si se fijan el movimiento de los datos y siguen las flechas, lo que vemos es que acercamos los datos que venden los contactos y los (registrararios), pasan al validador o registrador y a los registros, y los DRS que después utilizan los datos en el próximo punto. Se valida todo, y tomamos (inaudible -17:35.7) requerimientos y todo lo demás, y pensamos que este modelo sincronizado es el modelo que mejor sirve a nuestros propósitos y más fácil de implementar.

FAISAL SHAH:

Quisiera decir, yo soy realmente fanático de la informática y creo que es muy bueno estar sentado al lado de Scott que escribió el EPP, así que él conoce muy bien este tema, así que Scott si quieres hablar de la próxima diapositiva.

SCOTT HOLLENBECK:

Todavía no dijimos nada sobre protocolos. Y creo que uno de los puntos que quiero que se lleven de esta reunión es que mucho de trabajo de protocolo que hay que hacer para que este modelo funcione, o ya existen o están bien desarrollados, bien adaptados.

EPP se está utilizando como estándar de aprovisionamiento de nombres de dominio desde hace muchos años, todos los registros, gTLD lo están usando y, si bien identificamos que hacía falta agregar extensiones al protocolo no hace falta empezar desde cero.

INTERPRETE:

Habla alguien fuera de micrófono. Dice que “trajimos material para festejar”

SCOTT HOLLENBECK:

Además EPP está al lado del aprovisionamiento. No hablamos del lado de las consultas todavía, del lado de las consultas con WHOIS es el protocolo de WHOIS, un protocolo muy simple, que deja muchas áreas abiertas a la interpretación.

Entonces, durante estos 15 meses la IETF está trabajando en otro protocolo en un grupo llamado “WEIRDS”.

El nombre del protocolo es RDAP, protocolo de acceso a datos de registros. Y todavía no pueden ver lo que se está haciendo en el Grupo de Trabajo WEIRDS, o si no conocen RDAP les diría que lo consulten.

El grupo de trabajo va a empezar a presentar documentos en un par de meses a través de IETF, es decir que muy pronto vamos a tener un estándar sugerido o mecanismo para que este modelo funcione.

Y ahora pasemos al ejemplo más específico de cómo se puede utilizar EPP Y RDAP, tomando los ejemplos que mencionaron Rod y Susan antes. Supongamos que ustedes tienen todos estos datos que han sido llevados a estos depósitos de datos utilizando RPP, los otros que están allí han sido validados y todos los que quieren hacer consultas han sido validados y tienen las autorizaciones o credenciales. Entonces el usuario le manda una consulta al DRS utilizando RDAP.

Y esta consulta contiene información de identificación de manera que el DRS sabe quién está presentando la consulta y sabe con qué propósito piden la información. Entonces en este caso la persona dice que pide la información para resolver un tema técnico. Por ejemplo este sitio web no me permite resolver y quisiera hablar con alguien sobre esto.

Cuando el DRS recibe la consulta autentica a la persona que la presenta, suponiendo que la autenticación es aprobada, en el próximo paso se

compara el propósito mencionado con las autorizaciones que tiene esa persona para hacer ese tipo de consultas. Si eso es aprobado pasamos al próximo paso, entonces el DRS busca los datos adecuados para un nombre de dominio determinado que han sido autorizados para ser compartidos para resolver este tema técnico. Entonces el sistema busca la información de contacto protegida para incluir la información del (registratario) y la información de contacto técnico, lo junta de manera estructurada y envía esa información utilizando RDAP.

Muy bien, Carlton.

FAISAL SHAH:

Bueno. Sobre este tema verán que estamos buscando otros autorizados del nombre de dominio, el ID de contacto del (registratario), la información de contacto técnico y en modelo federado tendrá que entrar a varios lugares – en el modelo no federado tendría que entrar a varias partes para encontrar estos datos.

Acá está todo junto.

CARLTON SAMUELS:

Además de un conjunto muy pequeño de datos que están disponibles a través de un acceso anónimo o para acceso anónimo, el resto de los elementos de datos, sólo se divulgan con un propósito en base a un acceso permitido.

Y uno podría pensar, por lo tanto, o espero que hayan observado que esto está basado en la protección. Sabemos quién está accediendo a los datos, con qué propósito, así que sabemos que si hay algún problema podemos tomar acciones para resolver los conflictos o problemas. Los principios de protección de datos son el centro, el corazón de todo este

debate, hemos dedicado mucho tiempo a hablar sobre esto y ustedes verán que los resultados cumplen con estos principios y hemos trabajado en forma muy diligente y cuidadosa.

Otra razón muy importante que deberían recordar es el tema de “compliance”, “cumplimiento” de la legislación existente.

Si han estado bastante tiempo trabajando o en contacto con la ICANN verán que el esfuerzo que hemos hecho para trabajar con “compliance” ha sido muy intenso. El crecimiento de los espacios de nombres ha creado un mayor desafío.

La idea es que queríamos ver que con el crecimiento, la ampliación del espacio de nombre, WHOIS tal cual como está no sería adecuado ni siquiera podría cumplir con lo que se requiere.

Por lo tanto teníamos que ver cómo podíamos resolver con lo que pasaba con los nuevos gTLDs.

Entonces, debíamos adaptar mecanismos para facilitar la recolección y transferencia de datos en forma periódica y legal entre los DRS, todos los actores del sistema DRS y las personas que buscan y necesitan datos personales.

Y hemos buscado la forma de lograr esto y eso se podía lograr de diferentes maneras.

En primer lugar, a través de cláusulas contractuales estándares armonizadas con las leyes de privacidad y protección de datos, fíjense que hablo de políticas, esto se codificaría en políticas y se aplicaría a través de contratos.

Es un marco, el marco que ya tenemos hoy en día.

Y después tenemos un motor de reglas, que aplica la legislación de protección de datos teniendo en cuenta cada jurisdicción, cada zona.

Además tenemos también la localización de almacenamiento de DRS para implementar un alto nivel de protección de datos.

¿Qué queremos decir con esto? Dónde están localizados los DRS.

En ese lugar tenemos la mejor protección de datos disponible bajo el marco legal.

Le doy la palabra a Stephanie.

STEPHANIE PERRIN:

Quisiera decir que esto no ha sido un desafío sencillo construir otra vez este sistema, entonces además de cumplir con la legislación de protección de datos, también debemos dar lugar a los servicios acreditados de privacidad y representación, ya se habló de esto, y tengo el honor, como lo tiene Carlton y Michelle de trabajar en ese grupo de trabajo que se está ocupando de ese tema.

Y un servicio de credenciales protegidos, seguro y acreditado. Esto es un nuevo servicios – y en la próxima diapositiva hablamos de esto – podemos pasar a la próxima diapositiva, muy bien, este servicio va a estar disponible para las personas que corren riesgo, que podrían llegar a una Corte, un Tribunal especial, explicando que están en riesgo, y pedir lo que se mencionó hace un par de meses, una credencial anónima para el registro de nombres de dominio.

Yo sé que hay personas aquí que sabrán que realmente está amenazado el sistema de registro de nombres de dominio, es lo que menos nos preocupa, y eso es cierto.

Sin embargo sigue siendo un pequeño elemento, una pequeña parte de la protección por la cual ICANN es responsable. La ICANN tiene la responsabilidad –en mi opinión por lo menos tiene la responsabilidad – de ayudar a esta persona.

Entonces, sugerimos esta estructura que permite a las personas a obtener una credencial segura. Hay varios proveedores en el mercado que ofrecen esto y pedir un nombre de dominio, probablemente a través de un tipo de servicio de representación y después podrían obtener la credencial segura y llevarlo a un proveedor de servicios de privacidad y representación. Que sería una capa adicional. Una persona en riesgo puede pasar por varias de estas capas.

Ven que tenemos cinco categorías de personas. (...) si uno es un periodista de New York Times y uno está en un país hostil, el diario se va a ocupar de conseguir las credenciales que necesitamos.

Es más difícil si una persona trabaja en un grupo que defiende los derechos de las mujeres en un país y está amenazada, ahí la cosa es más compleja.

Pero estamos comunicándonos con la sociedad civil tratando de ver cómo podemos ayudarles y cómo podemos acreditar a estas personas. Y eso es todo por mi parte.

CARLTON SAMUELS: Le damos la palabra a Michele.

MICHELE NEYLON: Gracias Carlton, Stephanie. Espero que todavía estén despiertos. Acá hace bastante calor. Les vamos a dar una remera que va a decir “lean este informe”. Tiene 160 páginas, es muy largo, muy complejo, no les vamos a mentir. Pero hay otros temas, si alguien me puede pasar la próxima diapositiva para que sepan de qué estoy hablando, hay muchos otros temas que hemos incluido en nuestro informe.

Algunos de los principios que tienen que ver con la acreditación de usuarios, cómo vamos a manejar cosas como acceso para las autoridades de aplicación de la ley, cómo vamos a manejar el cumplimiento de la legislación, los servicios de representación y privacidad, costos, los costos son un aspecto importante; y hay mucha información allí, todo esto está incluido y bien detallado. Supongo que lo puedo decir así. Y por supuesto otro elemento que incluimos es, los beneficios que obtienen si se compara lo que tenemos ahora con respecto a RAA de 2013 y el WHOIS.

Las diapositivas de esta presentación, como ya dijimos antes, están en la página de la agenda, así que si no pueden entender algunos de nuestros gráficos, bajen el PDF y hagan lo que tengan que hacer en su propia computadora.

Entonces, lo (...) es, ¿qué va a pasar ahora?

¿Hacia dónde vamos con esto? ¿Qué hacemos?

Transformamos el informe y lo usamos como escalón para alcanzar algo o lo usamos para algo más interesante, por ejemplo, la implementamos. En el futuro cercano tendremos más sesiones sobre este tema, hoy estamos presentando el tema, pero hay una sesión sobre preguntas y respuestas donde pueden hacer preguntas, amables por favor, hagan preguntas “amables”.

Y también vamos a tener “webinars” y otro tipo de formas a través de las cuales la comunidad se puede comunicar con nosotros.

La idea es discutir, debatir y darles la mayor información que necesiten. Como la Junta Directiva, el CEO de la ICANN nos pidieron que hiciéramos este trabajo, bueno, depende un poco de ellos qué vamos a hacer de aquí en más.

Supongo que ellos van a analizar el informe en detalle en los próximos meses y después lo van a pasar a la GNSO o no, no sé, a alguien que está haciendo ruido, la voy a ignorar.

Obviamente que la pregunta que muchas personas hacen. ¿Esto que sugerimos es mejor que el WHOIS actual?

Es una pregunta abierta. Por favor lean el informe y decidan.

Y por supuesto pueden estar en desacuerdo con nosotros. Yo sé que Kathy – perdón Kathy justo está sentada frente a mí – no pude resistirme.

Y si lo que nosotros sugerimos no es una buena respuesta o no contiene algunos elementos que ustedes consideran debe estar en una buena respuesta, bueno, habrá que ver el WHOIS que tenemos hoy en día.

¿Sirve para lo que buscamos?

Estas son las preguntas que planteamos, en los últimos 16 meses hemos estado trabajando en esto. Mi opinión con respecto al futuro es volver a mi vida anterior.

Muchas gracias. Los quiero muchísimo a todos pero sería bueno ver un poco a mi propio personal y a mi familia.

Entonces hoy tenemos una sesión de preguntas y respuestas. Si no llegan hoy hay otra sesión de preguntas y respuestas temprano el miércoles a la mañana. Y yo sé que el concepto de hablar de WHOIS a las 08:00 de la mañana es cruel y es un castigo.

Pero quizás para las personas que estén en otros husos horarios sea más adecuado, no lo sé. Para aquellos de ustedes que están en otros husos horarios quizás les vendría bien.

La mayoría de los miembros de este grupo de trabajo están aquí sentado al lado mío y con mucho gusto vamos a discutir cualquier parte del informe con ustedes.

Jean Francois quiere decir algo.

JEAN-FRANCOIS BARIL: Muchas gracias Michele por cerrar esta primera parte de esta sesión pública.

Antes de –

[FIN DE LA TRANSCRIPCIÓN]