MONTREAL – Sesión de presentaciones de NextGen
Martes, 5 de noviembre de 2019 – 13:30 a 15:00 EDT
ICANN66 | Montreal, Canadá

DEBORAH ESCALERA: Permítanme un comentario adicional para todas las presentaciones y todas las reuniones. Sin celulares. Si toman notas, por supuesto, pueden tener la laptop. No envíen mensajes, no tengan los celulares, mientras alguien está presentando.

Son las 13:30. Vamos a comenzar. Quisiera agradecerles a todos por estar aquí. Soy Deborah Escalera. Bienvenidos a la presentación de NextGen ICANN66. Vamos a comenzar a tiempo. En primer lugar quisiera darle la bienvenida y agradecer a los embajadores que están conmigo y que me brindan su apoyo en esta reunión. Joao Pedro Martins, de ICANN63; Jaewon Son, de ICANN64 y Stefan Filipovic, de ICANN63. Muchas gracias por su apoyo y por volver a trabajar como mi apoyo en ICANN66. Vamos a comenzar con la primera presentación. Abdeali Saherwala. Abdeali, por favor, toma la palabra.

ABDEALI SAHERWALA: Soy Abdeali Saherwala y soy estudiante en la facultad de Estudios Ambientales en la Universidad de York. Estoy aquí para hablar de un tema fundamental de la sociedad actual: la posverdad y sus implicancias políticas. Antes de comenzar quisiera leer primero un reconocimiento que se reconoce como custodios de la tierra.

Esperamos tener que sigan las relaciones con los pueblos aborígenes de la comunidad de Montreal.

En el siglo pasado se empezaron a revolucionar las maneras de comunicarnos con la gente en todo el mundo y también a través de ellos puedo saber los logros de amigos y familia. En segundo lugar, puedo conocer las actividades sísmicas y de todo el mundo que se dan por todos lados: crisis económicas y problemas de los distintos lugares. Ese es el poder de los medios sociales, de las redes sociales. Nos permiten cambiar y enterarnos de nuestras cosas en tiempo real y a partir de poca información podemos cambiar totalmente y podemos dividirnos sin saber los hechos. En Estados Unidos o en Canadá o en Europa, un adolescente puede buscar el apoyo de gente que está con islamofobia, terrorismo… Se puede trabajar con instrumentos fundamentales para mejorar la vida de maneras impensadas. Hay movimientos tales como los antivacunas, que es una de los top 10 amenazas contra la humanidad según la OMS en este año.

Hablemos de los elefantes en la sala. Donald Trump ha traído factores ocultos al conocimiento general. La gente de pronto no cree que se aterrizó en la luna pero con la cobertura general esto ha pasado a ser una realidad. La gráfica que nos muestra esta diapositiva, alguien dice que pienso luego existo. En base al conocimiento, podemos moldear quiénes somos. Por otro lado vemos a Juan Pérez que dice que alguien cree que algo es verdad y que por ende pareciera que es verdad. Según el diccionario Oxford, la posverdad se relaciona o denota circunstancias en las cuales los hechos objetivos son menos

influyentes en darle forma a la opinión pública que la apelación a las creencias personales y lo emocional.

La verdad no está en la sociedad como antes porque no se confía ya en gobiernos, universidades, partidos políticos, organizaciones tales como la ONU, por la falta de percepción de la realidad en todo el mundo. Hay otros elementos sobre la elevación y la instalación de la posverdad en la sociedad. Los medios, las redes sociales, estas empresas son las más grandes: Facebook, Whatsapp, YouTube, Instagram. De una manera aprovechan las noticias falsas. Hay mucha gente en el mundo con redes sociales. Muchos tenemos múltiples cuentas en las plataformas. Yo tengo Facebook, Twitter, Whatsapp, Instagram. Muchos tienen distintas cuentas en la misma plataforma. En 2018, Facebook tiene 2.000 millones de personas. YouTube anda cerca. Instagram 1.000 millones. Twitter tiene unos 300.000. En 2008, Facebook solamente tenía 100 millones de clientes y en una década creció 26 veces.

Una de las ideas filosóficas más grandes viene de Spiderman, que con el gran poder viene gran responsabilidad. Esto tiene que ver con el encarar la responsabilidad para evitar la mentira en general, las noticias falsas y el odio. Aquí vamos a estar inundados de gráficos y de hechos de las personas de los distintos grupos etáreos que reciben las noticias a través de las redes. De acuerdo a Peer Research Center, la mayoría de los adultos obtiene sus noticias de Facebook y dos tercios de las redes sociales. En Oriente Medio, el 28% de la gente la recibe de Whatsapp y casi la mitad desde Facebook. En el Reino Unido, la segunda fuente de noticias es Facebook y el consumo en general de las

redes sociales subió del 2018 a 2019. Muestran un crecimiento importante.

En el mundo real, la consecuencia de la eliminación de las mentiras de la redes se vio relacionada con Rohingya en Myanmar. Una de las personas más prominentes responsable del desplazamiento y el genocidio. Ashin Wirathu, como podrán ver ahí en la diapositiva, en toda su vida ha subido mensajes islamofóbicos, mensajes falsos sobre la gente Rohingya. Hay entrevistas en las que dijo cosas horrendas y sin embargo Facebook se tomó más de un año y medio para sacar su perfil de la plataforma. Facebook fue un factor fundamental en esta atrocidad contra los derechos humanos.

En Francia y en Alemania han tratado de mitigar este tema como por ejemplo en España también. El gobierno exige acciones de Facebook para reducir las noticias falsas. En el Reino Unido hay investigaciones múltiples y también se está tratando de aprobar legislación. Macron en Francia está tratando de prohibir las noticias falsas en los medios sociales durante las elecciones. En los Estados Unidos más o menos el 50% de la población apoya investigar a las empresas de las redes sociales por la interferencia posible en la elección de 2016.

Facebook ahora está considerando la ampliación de los grupos privados o semiprivados que han explotado en su popularidad en los últimos años en la promoción de comunidades y esto es una plaquita de Petri de abuso y radicalización. YouTube ha alterado los algoritmos para que sea más difícil encontrar los vídeos problemáticos. Finalmente, el departamento de defensa ha creado oficialmente un

programa para eliminar entre muestras de vídeos y de fotos que sean falsas. Mi recomendación es que los consumidores de las redes tienen que poder reconocer las noticias falsas. Las empresas tienen que contratar mucha gente, ejércitos de personas que puedan comprender la lingüística de los textos no ingleses. Los gobiernos tienen que hacer responsables a las empresas de redes sociales por el uso de bots y de herramientas para evitar la violencia, la destrucción entre la gente. Muchas gracias.

DEBORAH ESCALERA: Muchas gracias. ¿Hay alguna pregunta de la sala? Muchas gracias.

DAVID MARGLIN: ¿Facebook está actuando maliciosamente en cuanto a amasar poder?

ABDEALI SAHERWALA: No sé cómo responderlo. Creo que podrían hacer más para verificar que personas tales como las que les mostré no existan en la plataforma considerando sus antecedentes así que sí.

LUKAS BUNDONIS: La pregunta tiene que ver con la posverdad. Hay algunos ejemplos históricos diversos. Hay momentos en los cuales la apelación a la emoción predominaba sobre la verdad. La iglesia católica lo vino haciendo en Europa años y años. La propaganda nazi y stasi en Europa. ¿Qué tienen que decir sobre la precisión del uso de la

posverdad? ¿Es simplemente lo mismo que vimos antes con una nueva cara?

ABDEALI SAHERWALA: Es lo mismo. Lo que pasa es que en lugar de tener una sola entidad como la iglesia católica que controlaba mucha información o toda, los gobiernos o los grupos ahora están tratando de crear una realidad propia o parte de la realidad y las nuevas empresas de redes llevan ese contenido a gran cantidad de gente con la pasión de Internet. De pronto en el continente africano puede haber miles de millones de personas.

DEBORAH ESCALERA: ¿Alguna otra pregunta? Muchas gracias, Abdeali. El siguiente orador es Akshay Broota. ¿Akshay?

AKSHAY BROOTA: Muchas gracias, Deborah. Buenas tardes a todos. Estoy aquí para presentar sobre GDPR. Es una revisión de alto nivel de qué se trata, las consecuencias y el efecto en la Unión Europea. Me voy a presentar. Soy Akshay Broota. Soy estudiante de una maestría en la Universidad de Boulder, Colorado, en ingeniería. Tengo un curso de comunicaciones. Me presentaron el tema del GDPR y me interesaron sus impactos, sus efectos. Vamos a comenzar. No está funcionando.

Antes de GDPR había una ley que se llamaba directiva de protección de datos aprobada en 1995, que existía antes de la explosión de Internet y

aparecieron los teléfonos inteligentes en la sociedad. No era efectiva y le faltaban muchas cosas respecto de la protección de datos del consumidor. El objetivo principal de esta directiva consistía en proteger los datos personales del uso inadecuado. GDPR remplazó a la directiva y la primera versión apareció en 2012 y la aprobó el Parlamento Europeo en 2016 y se empezó a hacer valer en el 2018.

Ahora que sabemos cuándo apareció, veamos qué es. Es una ley que regula la manera en que las empresas deben proteger los datos personales para armonizar las leyes de privacidad de datos en la Unión Europea. El GDPR trataba de cubrir los huecos de la directiva brindando transparencia en la manera en que las empresas manejan los datos. Las empresas tratan de cumplir con las normas y si no lo hacen hay sanciones tales como una multa sobre la facturación de la empresa hasta 20 millones de euros anuales.

¿Por qué GDPR? Como les decía, teníamos normas antiguas en la directiva de protección de datos que existían desde antes de la invención de los teléfonos inteligentes sin cubrir ninguno de los temas más nuevos sobre datos personales. Faltaba un marco transparente y detallado sobre las empresas y su manera de acceder a los datos de los usuarios personales y trataban de vender productos específicos a los consumidores. La gente no tiene control sobre sus datos personales. Estos son los objetivos del GDPR. Darle poder al consumidor sobre sus datos personales y ver cómo controlarlos con el derecho a estar informado de acceso, eliminación, objeción, portabilidad de datos, restricción de procesamiento y rectificación. Como vengo de ingeniería de red, y yo soy usuario de muchas plataformas de redes y

proveedores de servicios e ISP, me voy a centrar más en la portabilidad de datos.

¿Qué quiere decir esto? Antes de empezar en realidad con el detalle hablemos un poco de los problemas de GDPR. GDPR trataba de cubrir los vacíos de la normativa previa. Sigue habiendo algunos que esperamos se cubran en el futuro. No menciona, por ejemplo, el formato particular de los datos. Respecto de la portabilidad de datos solamente habla del formato legible por una máquina. No dice si es CSV o PDF. Había una falta de detalle, de explicación del formato de los datos más utilizado en la sociedad, que puede transferir datos con mayor facilidad de un país a otro.

Otra cosa sobre GDPR es que no menciona cómo terceros acceden a los datos y el tiempo para acceder a un lugar. Cuando hablamos de la portabilidad de datos de una empresa a otra estos datos transferidos no sabemos si provienen de la empresa A o la empresa B. GDPR dice que el consumidor no es responsable de los costos de estas transiciones pero no dice nada sobre si debería ser de la empresa A o la empresa B.

Volvamos al tema de la portabilidad de los datos. Es la capacidad de la gente de reutilizar sus datos en distintos dispositivos y servicios, como se dice en el artículo 20 de la norma. Siendo yo usuario, utilizo los servicios de una empresa A durante cierto tiempo y quiero pasar a la empresa B. Puedo invocar mi derecho de portabilidad y que la empresa A que recopiló los datos sobre mí puede mandarlos a la empresa B en formato legible por computadora. Cuando volvemos a

esta directiva y a GDPR, en términos de portabilidad por temas de tiempo, GDPR dice que se tiene que llevar a cabo dentro de un mes. El costo es del controlador de datos pero no dice qué empresa tiene que afrontar los costos de los datos. El formato es legible por computadora. Tiene que ser un formato ampliamente utilizado pero no dice cuál. La responsabilidad es un tema complejo. No sabemos qué parte es responsable en caso de pérdida de datos durante la transición.

En general, GDPR ha sido el desarrollo más consecuente en política de la información. Ha tenido éxito hasta ahora pero hace un año y medio que se ha implementado nada más. Hay alguna preocupación dado que se implementó y apareció una cantidad de mails sobre las actividades relacionadas. La gente empezaba a recibir mails sobre GDPR y como que tenía que cambiar la configuración de privacidad respecto de X recopilación de datos, por ejemplo.

Ha habido phishing y estafas similares con este email del que les hablo. No sé si conocen a Max Shem. Es un activista austríaco. En 2018, cuando se lanzó GDPR, demandó a Google porque estaba forzando a los consumidores a dar su aprobación a las prácticas de recopilación de datos. Si no consentían, no podían utilizar el servicio.

El impacto del GDPR fuera de la Unión Europea ha sido muy importante. Yo vengo de un país asiático, de la India. Estoy viviendo en los Estados Unidos en este momento y sabemos que en California hay una nueva ley de privacidad de los consumidores de California que va a entrar en vigencia a partir del 4 de enero del año que viene. Esta ley

del estado de California tiende a que los residentes de California sean más responsables y controlen mejor sus datos y define cómo manejan o cómo pueden manejar los datos Facebook y Google. El impacto ha sido importante y deberemos esperar y ver en qué medida tiene éxito el GDPR.

El GDPR lleva los datos personales a un entorno complejo pero esto se aplica a los ciudadanos de Europa también que están fuera de Europa o a las empresas que tienen sede en Europa. El GDPR tiene cierta flexibilidad. Permite que los miembros de los poderes legislativos introduzcan algunos cambios. Tenemos que esperar y ver en qué medida el GDPR tiene éxito en los años futuros. Muchas gracias.

DEBORAH ESCALERA: Gracias. ¿Hay alguna pregunta del público? No hay preguntas. Muchas gracias. Ahora le damos la palabra a Ariane Nakpokou Houessou.

ARIANE NAKPOKOU: Muchas gracias, Deborah. Hola a todos. Muchas gracias por estar aquí. Yo me llamo Ariane Nakpokou y es un placer estar aquí siendo miembro NextGen de ICANN66. Acabo de recibirme con un título de Administración de Empresas. Mi título de pregrado fue en Contabilidad. Estoy estudiando en un programa centrado en la inteligencia artificial. Trabajo para una empresa en este rubro.

Como vengo del mundo de las empresas, fue una aventura interesante aprender los supuestos básicos de la inteligencia artificial y entrar en este mundo. Quiero decirles que vamos a hablar de aspectos generales

de la inteligencia artificial, lo que sabemos sobre esto. Después vamos a hablar sobre las amenazas al DNS y cómo la inteligencia artificial puede ayudarnos a evitar fraudes que son muy comunes en el mundo DNS. Después vamos a hablar del tema candente en la reunión de la ICANN66 que es el conflicto entre el WHOIS y el GDPR. Posteriormente voy a analizar lo que está haciendo la ICANN para resolver estas cuestiones. Estamos aquí desde el sábado. Aprendí más sobre estos temas. Fui escuchando lo que dicen las distintas personas. Voy a explicarles un poco qué se está diciendo y haciendo ahora.

Después vamos a pasar a mi tema favorito dentro de la inteligencia artificial que es ética por diseño. .AI fue muy bienvenido en el mundo. Hay muchos proyectos basados en este concepto. Si no saben, se están haciendo importantes inversiones en este campo porque diversas empresas quieren ser jugadores importantes en este campo.

¿Qué es la inteligencia? Es la capacidad de razonar, de percibir relaciones y analogías, de calcular, de aprender de otros y de adaptar nuestra respuesta a una situación. Eso es lo que hacemos todos los días con nuestra inteligencia. Es lo que esperamos ver en un sistema basado en la inteligencia artificial. Por lo tanto, es un tema en el cual no sabemos hasta dónde podemos llegar con la tecnología y qué podemos esperar de esto. Es claramente un concepto del año 2020. Cuando hablamos de inteligencia artificial, el campo es muy amplio. Hay muchos detalles a tener en cuenta pero para hacer un breve resumen diría que hay diferentes áreas de investigación. Procesamiento de lenguaje natural, sistemas expertos, redes neuronales, robótica, sistemas lógicos fuzzy y las áreas más difundidas

y más usadas son los sistemas expertos y las redes neuronales. ¿Qué es un sistema experto? Un sistema experto es un sistema que puede replicar la experiencia y los conocimientos humanos. Eso se puede utilizar en finanzas, para hacer diagnósticos médicos. Por ejemplo, las redes neuronales son las que se usan para reconocer patrones para aprender y para adaptar las respuestas en base a lo aprendido.

Para usar estos sistemas hay diferentes técnicas. Tenemos el aprendizaje por máquinas. El aprendizaje por máquinas utiliza algoritmos para analizar los datos y los sistemas toman decisiones informadas en base a lo ya aprendido. El aprendizaje profundo es un subcampo del aprendizaje por máquinas. Es aprendizaje por máquinas pero ahora se crea una red neuronal artificial que puede aprender y tomar decisiones inteligentes. La diferencia entre los dos es que en el aprendizaje por máquinas podemos poner un solo elemento de datos y esperamos recibir una única y la misma respuesta cada vez que hay algo parecido. En el aprendizaje profundo hablamos de un proceso automático y continuo. Por eso necesitamos big data. Necesitamos muchos datos para que se puedan hacer las conexiones y las analogías.

¿Qué hacemos con esto en el mundo del DNS? Tenemos que hablar de seguridad porque la inteligencia artificial es una herramienta muy poderosa que permite a los proveedores de alojamiento reducir o mitigar los riesgos cibernéticos. Esto ayuda a detectar y reconocer patrones de ataques cibernéticos. Se aprende de esto para mejorar la defensa del DNS por ejemplo. Además, también se pueden implementar medidas inteligentes y se puede alertar a los

consumidores y a los registradores cuando hay ataques cibernéticos. También se puede utilizar la inteligencia artificial para proteger los nombres de dominio. Es decir, si hay alguien que está intentando comprar o registrar un nombre de dominio similar al de un tercero, se brindará información a este tercero de que alguien está intentando comprar su dominio y esto puede ayudar a proteger a la empresa, la reputación en línea. Si alguien está tratando de falsificar o hacer falsificaciones o defraudar a terceros utilizando el sitio web de un tercero, ese tercero, al enterarse a través de la inteligencia artificial, podrá responder rápidamente a esa amenaza.

La inteligencia artificial también es importante en relación con la performance de los dominios porque los que brindan alojamiento utilizan tecnología de inteligencia artificial para analizar datos históricos para analizar el posible desempeño futuro de un dominio y para darle a cada usuario el nombre de dominio que más se adapte a su contenido y a su tráfico, etc.

Cuando usamos la inteligencia artificial para administrar el sistema de nombres de dominio logramos integridad en la Internet y tendremos un WHOIS más exacto y preciso. Por eso relacionamos estos temas, WHOIS e inteligencia artificial y GDPR. A veces hay mucha superposición. ¿Dónde ponemos el límite para el derecho a saber? Deberíamos saber quién es responsable de pedir la información o de brindarla pero al mismo tiempo la información personal puede utilizarse para perjudicar a las personas o para afectar algunos derechos fundamentales como la libertad de expresión, la seguridad y la privacidad.

Si pensamos que la protección de la información solo la hace una empresa con un know how específico, hay una enorme concentración de poder aquí que estamos aceptando. Esta herramienta podría ser utilizada por un régimen totalitario para manipular a la población para impedir su acceso a Internet. La ICANN está tratando de hacer lo siguiente. GDPR introdujo la privacidad por diseño. El sistema WHOIS tiene que ver con el derecho a saber. Entonces, obviamente hay un conflicto y la ICANN está trabajando a través del comité específico para conciliar ambos puntos de vista para ser reconocida como autoridad de coordinación del sistema de WHOIS y para asegurarse de que los registradores y los registros puedan seguir cumpliendo con la legislación brindando información a través del sistema WHOIS.

Hablemos ahora de ética por diseño. Sé que ya me pasé del tiempo que me asignaron y voy a responder después cualquier pregunta que puedan tener. Me queda una sola diapositiva. El GDPR incluye la privacidad por diseño. Algo muy importante aquí es seguir cumpliendo con los principios éticos cuando desarrollamos un sistema. Es importante tener orientación ética para garantizar que no estamos llevando nuestros sesgos al algoritmo a fin de que la oportunidad que brinda la inteligencia artificial no sea una repetición de otras desigualdades que ya vemos en nuestras sociedades. Muchas gracias por escucharme.

DEBORAH ESCALERA: Gracias, Ariane. ¿Hay alguna pregunta para Ariane? Adelante.

JOAO PEDRO MARTINS: Joao Pedro, de Portugal. ¿Esto significa que la ICANN ahora es responsable de alguna manera de empezar a pensar en la forma de crear algoritmos éticos? Yo sé que usted viene del mundo de los negocios o de las empresas pero podríamos decir que los que están creando el producto deberían autorregularse. Yo estoy estudiando este tema. Para esto hace falta mucha investigación, mucho tiempo. En general, creo que este es un nuevo tema que debería tratar la ICANN. ¿Qué opina usted?

ARIANE NAKPOKOU: Cada vez que presentamos esta pregunta trabajamos sobre el supuesto de que la ICANN se ocupa del contenido de las cosas. No puedo darle una respuesta exacta con respecto a qué es lo que se incluye en los datos. Vamos a avanzar. Necesitamos más políticas sobre muchos temas. Canadá acaba de adoptar una política sobre cómo actuar de manera ética en el área de la inteligencia artificial. Quizá algún día el GDPR prevalezca sobre algunas políticas de la ICANN. La idea es que cuando estamos haciendo políticas sigamos teniendo en cuenta el bienestar del ser humano.

DEBORAH ESCALERA: Adelante.

LUKAS BUNDONIS: Hola. Soy Lukas, de los Estados Unidos. Ariane, en primer lugar, muchas gracias por su fascinante presentación. La inteligencia artificial es muy importante por muchos motivos. Hay muchas

oportunidades a través de la tecnología. Es interesante ver cómo se usan diferentes campos pero muchas empresas ahora están llamando a sus productos, que no usan inteligencia artificial, lo llaman con el nombre de inteligencia artificial para vender más. Usted, como una persona del mundo de los negocios, ¿le preocupa que personas que no tienen conocimientos técnicos utilicen o compren soluciones que tienen inteligencia artificial y que no entienden?

ARIANE NAKPOKOU: Hemos visto esto. Somos una empresa que trabaja con inteligencia artificial y me resultó un poco difícil entender qué es y qué no es inteligencia artificial. Me llevó mucho tiempo entender esto. Como ser humano que está en el mundo de los negocios, sí, este es un tema que preocupa porque es muy difícil desarrollar una solución y vender un producto. Cuando hay personas que le ponen el nombre inteligencia artificial a un producto que no lo es, bueno, están actuando de mala fe y será un caso de competencia desleal.

LUKAS BUNDONIS: ¿Tiene alguna idea de cómo se puede comunicar o enseñar esto a la comunidad de negocios?

ARIANE NAKPOKOU: Podría responderle pero es muy difícil esto.

DAVID MARGLIN: David Marglin, de los Estados Unidos. Usted habló de algunos usos positivos de la inteligencia artificial. Usted conoce mucho este tema pero muchas personas dicen que quizá la tecnología es neutra, el tema es qué hacemos con la tecnología. También podemos decir que las armas no matan. Las personas matan otras personas. Me pregunto si usted piensa que la IA hoy por hoy es algo que tiene un resultado netamente positivo o piensa usted, como me preocupa a mí, que la mayoría de los usos de la inteligencia artificial tienen que ver con vender más productos o quizá más bien tengan efectos negativos, volviendo a la presentación que escuchamos antes.

ARIANE NAKPOKOU: Es como todo. Cuando hay algo nuevo, siempre hay temas que nos preocupan, hay incertidumbres porque no sabemos qué podemos esperar pero esto ya está aquí. Tenemos que asegurarnos así como lo hicimos con la Internet de establecer principios o guías amplios. Tenemos que asegurarnos de poder seguir controlando la situación. Cuando empecé a trabajar en la empresa en la que estoy trabajando en Montreal realmente me impresionó lo que se podía hacer. Yo uso anteojos y los voy a usar de por vida. Hay una solución extraordinaria para personas como yo utilizando la inteligencia artificial que permite hacer cosas maravillosas para las personas como yo. El tema de Internet es lo mismo. Hay que ver cómo se usa. Se trata de elegir cómo se usa. Continuamente hay que ir eligiendo como sociedad y estar seguros de que se van a aprovechar estas tecnologías. Seguramente harán cosas negativas con ellas pero debemos asegurarnos de establecer los límites adecuados en este campo.

DEBORAH ESCALERA: Gracias. Tenemos una última pregunta. Muchas gracias.

KUSHAGRA BHARGAVA: Soy Kushagra, de la Universidad del Sur de California en Los Ángeles. En primer lugar, muy linda presentación. Mi pregunta tiene que ver con la investigación, los investigadores tales como los universitarios que uno encuentra constantemente. Cuando decimos el derecho de saber, la privacidad por diseño, ética por diseño, ¿qué piensas? Es una pregunta de final abierto. ¿Qué piensas sobre estos tres? ¿Van siempre juntos? Privacidad y ética por diseño. ¿Van juntos? Cuando tienen direcciones divergentes, ¿qué pasa?

ARIANE NAKPOKOU: Creo que la privacidad por diseño es más estrecha que la ética por diseño porque uno puede respetar la privacidad poniendo datos en un algoritmo. Uno puede poner un sesgo propio, transportar las ideas propias porque uno técnicamente le dice a una máquina: “Esto es una banana”. Es tu percepción de lo que es una banana. En ética por diseño también habría privacidad por diseño porque tenemos que verificar que al consumidor lo tenemos en cuenta al diseñar el algoritmo pero uno puede tener privacidad en el diseño a través de la manera en que la gente se comporta éticamente. No sé si lo estoy explicando.

KUSHAGRA BHARGAVA: Muchas gracias. Es una buena respuesta.

DEBORAH ESCALERA: Gracias, Ariane. La última presentación va a ser una presentación doble de Austin Bollinger y Lilia Herdegen.

LILIAN HERDEGEN: Uno, dos, tres. Hola. Hola a todos. Muchas gracias por estar en nuestra presentación. Este es el mundo maravilloso de DNSSEC que vamos a presentar. Yo soy Lilia Herdegen. Estoy en la Universidad de Ferris State, en una maestría en seguridad de la información e inteligencia.

AUSTIN BOLLINGER: Yo soy Austin Bollinger. Ambos somos del área de Michigan, en Grand Rapids. Soy analista de seguridad informática y estoy estudiándola en el Community College de Grand Rapids. Vamos a ver brevemente un poco de historia y los problemas y ventajas de DNSSEC. Quisiera comenzar diciendo que toda la información de la presentación es solo con objetivos educativos e informativos. Es importante notar que cualquier protocolo si está mal configurado le abre la puerta al peligro.

LILIA HERDEGEN: No estamos tratando de molestar a nadie. Simplemente lo estamos viendo y comentando con ustedes. Lo hemos visto en ICANN en los últimos años. ¿Por qué DNSSEC? En los 90, Steve Bolovin demostró algo que se llamaba envenenamiento de la caché de DNS. Esa es una de las maneras. Aquellos que trabajaban en DNSSEC al principio

proponían como solución la firma de la solicitud de DNS. Hay ejemplos de qué es el envenenamiento. Es cuando un usuario manda una solicitud que afecta al resultado del resolutor. Va a un caché envenenado en un sitio malicioso o un caché limpio que es el que uno preveía. Si uno se quiere ir a un sitio de pronto de la facultad o de la escuela y quiere ingresar el usuario y la contraseña, si está envenenado puede ser similar o exactamente igual a lo que debería ser pero puede ser un sitio malicioso que se queda con la información. Ese es un ejemplo de envenenamiento de la caché.

AUSTIN BOLLINGER: Aquí tenemos índices de adopción de DNSSEC. La gráfica es interesante. Proviene de información en 2015. Los dominios con DNSSEC eran 40.000 con una trepada importante en el 2018 a 200.000. Muchos de estas firmas de dominio están vinculadas directamente con la concientización de DNSSEC para resolver el problema del envenenamiento de la caché de DNS. También hay algunas cosas relacionadas que están sucediendo a la vez. Creo que es muy importante observar en detalle.

LILIA HERDEGEN: Asociado con estos índices de adopción tenemos la amplificación de DNS. En 2019 había casi 66% de las negaciones de servicio. Eran por amplificación de DNS. En 2018 hubo un 1040% de incremento en los ataques. En 2019, en el primer trimestre un incremento de un 31%. Este es un ejemplo rapidito de la comparación del 66% en

comparación con otros ataques: inundación de HTTP, inundación de HTTPS y demás.

AUSTIN BOLLINGER: DNS puede utilizarse TCP o UDP, fundamentalmente UDP. Es importante saber que con el protocolo TCP hay un protocolo de enlace tridimensional tal como los que vemos aquí. Con UDP no lo hay para verificar que la IP correspondiente es la que debería ser porque un ataque puede usurpar la dirección original y causa el ataque reflejo. Esto es un ataque de amplificación el que estamos viendo en pantalla. La usurpación de IP se puede llevar a cabo en el puerto 53 que es el que utiliza DNS. En el caso de DNSSEC, si está implementado, permite un ataque más fuerte. Lo vamos a ver luego.

LILIA HERDEGEN: Aquí tenemos un ataque de amplificación de DNS. A la izquierda vemos al atacante. En este caso envía miles de bots para abrir los resolutores de DNS con solicitudes de DNS. Si no están bien configurados, no bloquean ninguna de estas IP usurpadas y contestan las bandas, las solicitudes a la víctima y esto resulta en la negación de servicio para cualquiera que quiere ir al sitio bajo ataque. Algo más sobre amplificación de DNSSEC. En 2015 [inaudible] encontró grandes cantidades de ataque a dominios configurados con DNSSEC junto con el impulso de implementación de ICANN de DNSSEC.

AUSTIN BOLLINGER: Con esa gráfica que mostramos antes de 2018 donde vimos 200.000 DNSSEC en los dominios imagínense. Tenemos en el informe de CSO MAG de 2019 un 1000% de incremento de los ataques de amplificación de DNS. Esta información se da de la mano y cuando explota dentro del protocolo se pueden amplificar los ataques por DNSSEC, que pueden llegar a incrementarse de 36 a 70 veces. Es problemático. Agrega información adicional al protocolo, lo que potencialmente permite que los ataques incrementen la fortaleza del ataque. Es seguridad que agrega algún inconveniente adicional.

LILIA HERDEGEN: OWASP top 10, para los que no lo conocen, es un proyecto de seguridad y aplicación abierta. Gente que toma información de Internet. Recopila la información y cada par de años ponen los top 10 vulnerabilidades, los riesgos que representan. Considerados los top 10 de 2017, que es la última información que tenemos de ellos, aparecen malas configuraciones de seguridad y esto va junto con DNS. La configuración de DNS tiene que estar restringida a las fuentes confiadas porque pueden no ser seguras y normalmente no lo son en cualquier proceso por omisión.

AUSTIN BOLLINGER: Allá por el 2013, ICANN recomendó mitigar la amplificación de DNS. Parecía eliminar la recursión de los servidores de nombres autoritativos, limitar la de los clientes autorizados y las respuestas de los servidores de nombres recursivos. Estas mitigaciones se proponían de manera temprana y era importante que al recomendar activar

DNSSEC se recomendara estas resoluciones para mitigar las configuraciones por omisión que permiten ataques más fuertes.

INX subió a su sitio de Internet sobre las caídas de DNSSEC junto con fallas de validación. Esto potencialmente puede causar problemas a futuro para los dominios pero es importante que educom.edu básicamente tenía entradas falsas para delegación de DNSSEC durante más de cinco años. Era como que la gente lo estaba probando y publicando los resultados. Es interesante ver el potencial de falla. Hoy por hoy, la gente implementa HTTPS y TLS. Es curioso ver cómo la gente no puede mantener HTTPS hasta la renovación del certificado y cómo se va a llevar adelante esto a futuro. Si quieren seguir adelante con un sitio que está fallando con DNSSEC, eso daría una falla tipo serve fail. Tiene que deshabilitar la verificación DNSSEC. Me gustaría ver a futuro cómo los buscadores manejan la validación DNSSEC.

LILIA HERDEGEN: Algunas lecciones para llevarnos. Hemos encontrado que hay una amenaza mínima respecto de los servidores DNS si están bien configurados. DNSSEC mitiga el envenenamiento del caché de DNS.

AUSTIN BOLLINGER: DNSSEC no es encriptamiento y en la comunidad se sabe que HTTPS/TLS, ese encriptamiento existe en la comunidad. DNSSEC es más autenticidad. También es importante saber que el énfasis principal sobre este tema es que las configuraciones por omisión pueden abrir la puerta a la vulnerabilidad y permitir ataques.

LILIA HERDEGEN: Esa es nuestra presentación. Si quieren contactarse con nosotros, esta es la información. Tenemos ahí el código QR de la presentación y también hay colegas que están viendo de otros lados. Por ejemplo, de Michigan. Hola a todos. Eso es todo. Gracias por escucharnos. Gracias a ICANN por todo lo que hace por nosotros. Se lo agradecemos.

AUSTIN BOLLINGER: Estamos muy contentos de estar aquí con el grupo de NextGen y es una bendición y ambos estamos muy agradecidos de estar aquí. Quisiera mencionar algo más. No estoy en contra del problema. Hay importancia en DNSSEC pero es importante… Creo que por ejemplo le podemos decir a alguien que correr es sano pero tiene que hacer otras cosas a la vez.

DEBORAH ESCALERA: Hermosa presentación. Muchas gracias. Tenemos preguntas. Empezamos aquí.

AKSHAY BROOTA: Soy Akshay, de Colorado, Estados Unidos. Gracias por la presentación. DNSSEC es tan seguro como puede serlo. Hay mayor complejidad y también hay mayores cantidades de paquetes y ancho de banda. ¿Qué sugieren al respecto? Si ponemos DNS en una red permitimos mayor uso de ancho de banda para tráfico de DNS que tráfico normal. ¿Qué pueden comentar al respecto?

AUSTIN BOLLINGER: Estoy tratando de entender la pregunta. Creo que la importancia fundamental es no utilizar la configuración por default o por omisión en el servidor. Entiendo el mayor uso de ancho de banda y eso es importante. Permitir el mal uso del ancho de banda, el uso malicioso del sistema DNS, por ejemplo, indirectamente causa un problema de preocupación porque no todos tienen la configuración bien hecha. La seguridad puede ser un problema. Recomendarle a la gente la autenticidad sin tener una buena configuración de DNS es la preocupación principal. ¿Le ayudó el comentario o quiere refrasear la pregunta?

AKSHAY BROOTA: Me preguntaba respecto del uso de ancho de banda. ¿DNSSEC es la única solución o hay algún otro método que podemos utilizar? No todos pueden tener la flexibilidad de implementar DNSSEC por la restricción del ancho de banda.

AUSTIN BOLLINGER: Es una pregunta interesante. Diría que es una preocupación de redes diría yo. Diría que centrándonos en DNSSEC se centra en la resolución del envenenamiento del caché de DNS. Con el encriptamiento del DNS se resolvería el tema a la vez. En términos del mayor ancho de banda que vemos que utiliza DNSSEC, quizá hay un papel para HTTPS. Sé que Firefox está tratando de utilizar Cloudflare, reduciendo el uso de ancho de banda. Va a tener más sentido utilizar CDN para ese tráfico. Podría

ser una solución. Esto es interesante. DNSSEC junto con el encriptamiento del tráfico de DNS que viene a la vez implica mayor trabajo en conjunto porque tenemos la parte de encriptamiento y la de autenticidad. Centrándonos en conjunto en un solo grupo sería muy útil en lugar de separar encriptamiento y autenticidad. Tienen que ir juntos y se tiene que trabajar en equipo.

DEBORAH ESCALERA: ¿Algún comentario en línea? De GRCC. Lynn L. "Simplemente quiero decir excelente presentación". ¿Alguna pregunta de la audiencia?

ABDEALI SAHERWALA: Para la gente no técnica como yo, ¿qué es caché y envenenamiento de caché?

AUSTIN BOLLINGER: Básicamente, cuando tienen un caché… Le voy a dar un ejemplo de un caché de un buscador para que sea sencillo. Uno va a un sitio en Internet y hay datos que se baja, archivos, imágenes. Se puede guardar en un caché. Mantiene los archivos, imágenes en el buscador en una máquina local para no tener que ir a buscar los archivos todas las veces. DNS puede tener una manera de manejar el caché para que uno no esté yendo todo el tiempo con consultas por toda la red de DNS. Cuando tiene caché de DNS, resuelve los registros y los guarda. En caso de envenenamiento de caché, el ataque está en medio y le da a usted información incorrecta. Es un ataque de hombre en el medio donde una persona se coloca entre el usuario y el caché inyectando

una dirección maliciosa. Tiene la información de caché pero es equivocada. Tenemos un ataque de hombre en el medio y el atacante puede mandar información incorrecta.

ABDEALI SAHERWALA: ¿Lo hacen a través del sistema?

JOAO PEDRO MARTINS: Volviendo a la hermosa charla que estamos teniendo. Hablabas de asociar dos requerimientos críticos de seguridad. ¿Formularías quizá un nuevo protocolo que implemente ambos? ¿Implicaría mucho rediseño, mucho redesarrollo en una mesa conjunta o podría decir que combinando dos herramientas existentes o protocolos sería más eficiente desde el punto de vista de estar listo en términos de continuidad y a largo plazo sería menos eficiente?

AUSTIN BOLLINGER: Probablemente esa es la mejor pregunta. Gracias. En segundo lugar, la reunión de SSAC. Hablaron de seguridad en ICANN. Una persona comentó la tecnología de blockchain para incluirla en DNS y cómo sería potencialmente. Creo que la descentralización del DNS es compleja y lo sería para ICANN. ICANN es muy centralizada en el manejo de los dominios. Hay alguna división aquí y allá pero creo que la idea principal que yo tendría para la introducción de autenticidad es que se maneje con blockchain sin centrarse en una zona de ruta que esté bien firmada. En caso de guerra de pronto, un país diría todos estos dominios, me meto ahí. Tenemos que pensar que a futuro es

muy poderoso poder ir a la zona raíz y poder hacerse cargo de todo lo que tiene el enemigo.

En términos de un nuevo protocolo, es una idea linda. Llevó 20 años llegar a donde estamos. Los cambios de protocolo de Internet llevan mucho tiempo. Es un poco lento y está cambiando todo el tiempo a la vez. No estoy muy seguro sobre cómo responder bien la pregunta pero pareciera que dentro de 20 años se podría llegar a cambiar algo.

DEBORAH ESCALERA: ¿Hay alguna otra pregunta? Muchas gracias entonces por su presentación. Con esto terminamos las presentaciones del día de hoy. Quiero agradecerles a las personas que hicieron sus presentaciones. Estaban muy bien preparados. Vi que no estaban nerviosos. Muy bien. Felicitaciones. Muchas gracias a los embajadores por su apoyo hoy. Quiero recordarles a todos que tenemos una segunda ronda de presentaciones mañana, que va a empezar a las 15:15 en la sala 512G. Por favor, difundan esto. Espero ver más participantes entre el público mañana. Muchas gracias por estar con nosotros hoy aquí.

[FIN DE LA TRANSCRIPCIÓN]