Ciudad de México, 16 de mayo de 2017.

Versión estenográfica de la Sesión Especializada "Riesgos Cibernéticos Implicaciones para las Aseguradoras", dictada por Martín Hoz, en el marco de la 27 Convención de Aseguradores, llevada a cabo en el Salón Diezmo 2, del Centro Banamex, en esta ciudad.

Clemente Cabello: Buenas tardes. Esta sí que es una sesión íntima, no se dirá lo contrario, pero muchas gracias a quienes están aquí.

Yo, más que *sponsor* diría que soy una persona que acompaña a los miembros de este Comité que, como me imagino que muchos de ustedes saben, coordinan por el lado de AMIS Ángeles Yañez y Mauricio Arredondo, que creo que están haciendo un trabajo estupendo.

Tenemos, por el lado de las compañías, a Germán, quien es el Copresidente de este Comité representando a las empresas que operan en base a canales no tradicionales. Puede haber empresas que operen canales no tradicionales y también tradicionales, pero su expertise y los esfuerzos que coordinan y dirigen, que están orientados a canales no tradicionales, en tanto que Víctor Felpman, que ahora por causas de fuerza mayor verdaderamente no nos puede acompañar, él es también Copresidente y encargado de los temas relacionados con los canales tradicionales.

Este Comité es, creo, el más joven en AMIS, desde tiempos inmemoriales en la AMIS se ha trabajado y ha habido una interacción cercana entre las compañías de seguros en temas sobre todo técnicos, de los diferentes ramos de seguros, el Comité de Gastos Médicos tiene muchísimo tiempo de operar, el de vida, autos, en fin, todos ellos.

Algunos temas operativos, de sistemas y demás, pero en realidad este Comité, el que ahora ha tomado el nombre de expansión de los mercados y cuyo propósito principal en realidad es el desarrollo de los canales de distribución, es relativamente nuevo, porque es una materia que tradicionalmente ha sido complicada, un poco tabú, el tratar entre las compañías participantes en el sector, cosa que a mí en

lo personal me parece un error, es decir, en este tema lo que habitualmente se daba es que cada quien pensaba o piensa que sus estrategias de comercialización, de desarrollo de canales, etcétera, son la cosa que les incumbe solo a ellas y no había esta oportunidad de intercambio que ahora se empieza a dar.

A mí en lo personal me parece que es muy importante que lo hagamos, en realidad, si ustedes piensan, el avance que hemos logrado en la penetración del seguro está muy lejano todavía al potencial del mercado y parte, creo, tiene que ver con esto, el no haber tenido la voluntad de, como sector, hacer esfuerzos para desarrollar de manera más activa, más proactiva los canales de distribución.

Afortunadamente se ha creado este Comité. Hay una participación, observamos entusiastas y, por lo menos, se ha dado ya un primer paso importante, que es que las compañías estén abiertas al diálogo, que se empiece a obtener confianza entre los participantes y enriquecer las experiencias de todos a través del intercambio de ideas.

Los objetivos del Comité, pues aquí está muy claro que es promover el desarrollo de políticas públicas de iniciativas sectoriales. No se dice en la lámina, pero es claro y la modernización del marco regulatorio en materia de canales de distribución para lograr una mayor penetración del seguro.

Y esto se pretende hacer a través de una serie de iniciativas fundamental, una serie de iniciativas orientadas a promover el sano crecimiento y profesionalización de los canales existente.

Yo creo que todos ustedes están conscientes que en esa materia tenemos áreas de oportunidad enormes. Desafortunadamente el número, hablando de los canales tradicionales, el número de agentes de seguros, no solo no ha aumentado, sino ha disminuido con los años. El grupo ha envejecido. La edad promedio arriba de los 50 años que es absolutamente ilógico en un país como el nuestro, que no quiere decir que no existan muchísimas personas de esa edad, que son profundamente exitosas.

Pero lo que está atrás de todo esto es que no estamos siendo capaces de atraer nuevas gentes a nuestro sector, o no los hemos podido desarrollar y profesionalizar adecuadamente, de manera que cuando llegan a esta actividad permanezcan en ella.

Íntimamente ligado con esto están las iniciativas que permitan el desarrollo de nuevos canales de distribución. Entonces los cambios que se están dando en nuestra sociedad en el mundo, en las aplicaciones de la tecnología, el uso de internet, etcétera, hace necesario que el Sector Asegurador también se asome y desarrolle nuevos canales de distribución. Es un tema en donde Germán, en particular, ha estado muy involucrado y seguramente nos va a poder platicar algo de esto.

Una tarea que también se ha asignado a este Comité es promover la construcción de indicadores que midan con objetividad el servicio al cliente. Esto pareciera que es un tema colateral o ajeno, pero no, al final de cuentas también en buena medida el desarrollo del sector depende, por supuesto, de qué tan satisfechos están nuestros asegurados.

No es tarea de este Comité crear las condiciones para que se dé esa satisfacción, porque esto tiene que ver más bien con otros aspectos, por ejemplo, que se refieren ya a la manera como se operan los diferentes ramos del sector.

Pero este Comité, este grupo sí debe de poder encontrar la manera de obtener indicadores que les den señales claras a quienes tienen la responsabilidad de prestar los servicios, de cuáles son las áreas de oportunidad, cuáles son los problemas, cuáles son las cuestiones en donde nos estamos desarrollando bien.

Y después hacer recomendaciones en materia de las mejores prácticas internacionales. Yo creo que una de las cosas que no podemos pretender es inventar el hilo negro. Por supuesto, habrá desarrollos que sean únicamente mexicanos, pero en el mundo de los seguros se están haciendo ya hoy en día cosas que son importantes, que nos pueden ayudar a crecer más, y entonces es tarea de este Comité identificar esas buenas prácticas, que tienen que ver con muchas cosas, incluyendo, por ejemplo, los relativos al desarrollo de la

fuerza productora, los modelos o las prácticas que están dando resultados para reclutar, formar agentes, también en materia de nuevos canales, etcétera.

Y esto, compartir estas experiencias con las compañías para que ellas las apliquen en la medida en que se adecúen mejor a sus propias estrategias.

Y, finalmente, hacer estudios relacionados con el tema de CRM, que está muy relacionado con lo anterior, basados en experiencias de nuestros asegurados.

Entonces, diríamos que en términos generales estos son los objetivos del Comité, y si les parece, le voy a ceder el micrófono a Germán para que nos platique un poco más en concreto de los proyectos ya concretos en que se está trabajando y después nos hablarán un poco del programa en la sesión.

Germán Aguado: Gracias. Buenas tardes. Gracias, Clemente.

Los proyectos, como ven ahí, son encaminados, justamente, al crecimiento del seguro. Entonces el primero diría que tiene que ver con el famoso, crear la cultura del seguro, o sea, que las personas quieran comprar un seguro, que entiendan la necesidad del seguro, entonces tenemos una serie de iniciativas de inclusión financiera, que tiene que ver, obviamente, también con los servicios financieros.

Luego todo lo que es fortalecimiento de los canales de distribución. Entonces, tenemos un tema de mejores prácticas, de ver lo que se puede lograr con el intercambio de las mejores experiencias de las compañías y algo que se nos ha vuelto, la verdad, una prioridad es la relación con CONDUSEF porque, como ustedes saben, con las nuevas reglamentaciones que le dieron más poder a la CONDUSEF, ha entrado a reglamentar, por ejemplo, la venta de seguros por teléfono y nos ha puesto a trabajar bastante, a generar mucha creatividad a las compañías de seguros para poder vender con calidad.

Y hay un tema de evaluación de la calidad de las compañías de seguros y en el Comité de Expansión del Seguro le damos atención a la relación con CONDUSEF.

Y lo último, el último proyecto en el cual estamos encaminados es el tema del Centro Certificador, que tiene que ver justamente con la nueva ley que mediante la circular le da la facultad a que sea de una manera, vamos a decirlo, más sencilla o por lo menos más expedita, la certificación de los agentes de seguros que antes todo se hacía a través de la comisión, ahora podemos certificar a gentes de una manera más proactiva.

Entonces, esos son los proyectos en concreto que tenemos, y para la tarde de hoy tenemos cuatro ponencias, que pretenden, como siempre, generar esta inquietud sobre aumentar la distribución de seguros.

En primer lugar, tenemos a Martín Hoz, Vicepresidente de Ingeniería de Sistemas para América Latina y El Caribe, de Fortinet, quien nos va a hablar de riesgos cibernéticos, que está muy de moda por estos días, entre otras cosas, y luego tenemos a Alejandro Julián y a Adolfo Díaz, que nos van a platicar de la función del promotor en el desarrollo ente del canal tradicional de agentes.

Y luego tendríamos un panel con algunos de los pioneros del tema de vender seguros con internet y seguros en canales directos, que transformarían a la gente de seguros, y finalmente Mauricio Arredondo, aquí de AMIS, nos va a dar una plática sobre cómo atraer y retener a los clientes.

Entonces, pues vamos ya media hora retrasados con respecto al Programa, pero esperamos que sea interesante para todos.

Entonces, los dejo con Martín Hoz, del tema de riesgos cibernéticos.

Muchísimas gracias y buena tarde.

Martín Hoz: Muchas gracias por la introducción, muchas gracias por la presentación, gracias a la AMIS por el espacio que nos ofrecen esta tarde para charlar un poquito sobre ciberseguridad.

Bien nos comentaban, es un tema que en los últimos días, ha dado mucho de qué hablar.

Y lo que me gustó es que comparte algunos conceptos, como parte de los objetivos que mostraban ahí en las láminas de cómo acercarnos más a los clientes, de cómo es que podemos mejorar la experiencia en usuario, cómo es que podemos mejorar la satisfacción del usuario a través de la tecnología.

Y es que para poder hablar de ciberseguridad, tenemos que tener el contexto de que nuestra sociedad está cada vez más embebida con tecnología.

Y para comenzar con la charla, yo quiero hacerles a ustedes una pregunta: ¿Cuánto tiempo pasa entre que ustedes se despiertan y toan por primera vez el celular ustedes? ¿Cuánto tiempo pasa entre que se despiertan y toman por primera vez el celular las personas con las que comparten su casa, su habitación?

Realmente hoy tenemos nosotros una gran dependencia de la tecnología, y el hecho de que prácticamente nos sintamos conectados al mundo, a través del celular, es una gran sensación de dependencia.

A juzgar por la audiencia y después de las preguntas que hacían en la mañana de más o menos las edades de la gente que estaba por aquí, sin querer balconear a nadie, pero no veo a nadie que tenga 18, 20 años, alguna que otra dama por ahí sí, creo que todas, casi todas, pero entre los caballeros, creo que la mayor parte de nosotros tenemos arriba de 18 años.

¿Qué nos quiere decir esto? Nosotros no nacimos en una época donde la tecnología fuera requisito para vivir y aun así hoy somos dependientes de la tecnología, ha cambiado prácticamente la forma como vivimos, está presente en cada aspecto que tenemos en nuestra vida, está presente en la educación, está presente en el trabajo, está presente al momento de salirnos a divertir, porque quién no se tomó una *selfie* con su celular y la compartió en redes sociales.

¿Cuántos de ustedes ya hicieron eso el día de hoy? ¿Cuántos ya mandaron por Whatsapp a los amigos, a los vecinos, a los familiares donde están y lo que están haciendo el día de hoy? ¿Quién de ustedes ya recibió invitaciones inclusive a eventos profundamente tradicionales como bautizos o bodas a través de redes sociales, de nuevo, a través del Facebook, a través de Whatsapp, a través del correo electrónico, inclusive?

Eso nos dice mucho cómo ha cambiado la sociedad y cómo ha cambiado nuestro mundo a partir de la tecnología. Nosotros hemos cambiado con la tecnología al momento en que la tecnología también se empezó a adaptar a nosotros y a veces ni siquiera lo percibimos. Les voy a dar un ejemplo, estar de espaldas en una conversación con alguien ¿es de buena o mala educación? ¿Qué nos enseñaron cuando en la familia, cuando éramos muchachos? Es mala educación, ¿verdad? O sea, si yo ahorita me pongo a hablar y doy la espalda muchos de ustedes van a decir: “Bueno, ¿y a este cuate qué le pasa?”

Sin embargo, quiero que veamos esta imagen, la imagen ya data de algunos meses, pero es de la candidata presidencial a Estados Unidos, la señora Hilary Clinton, donde había un grupo de personas de múltiples edades que se estaban tomando una *selfie* con ella. ¿Alguno de ustedes cree que ella se sintió que alguien le faltaba al respeto? Si yo me volteo y hago lo mismo con ustedes, ¿si hago esto, alguno de ustedes sintió que les falté al respeto? No, ¿por qué?, porque los tiempos han cambiado, así como la tecnología ha cambiado la forma como percibimos el mundo, también ha cambiado la manera como interactuamos socialmente y cómo es que vemos los nuevos vehículos de negocio, inclusive los nuevos satisfactores que tenemos como personas y como sociedad.

Esto a veces, de manera transparente, no es tan perceptible para nosotros, nos hemos vuelto muy exigentes. ¿Quién de ustedes se espera 20 minutos para recibir un correo electrónico que dicen que acaba de salir? ¿Quién de ustedes espera que una página web le cargue cinco minutos? ¿Quién de ustedes se espera un minuto desde que enciende el celular y quieren que la aplicación esté ahí?

Queremos que sea instantáneo, queremos sacar el celular y que la aplicación ya esté ahí. Quiero que la oferta que me están haciendo

llegar sea una oferta adecuada para mí, si yo soy un millennial y soy una persona que está acostumbrada a la tecnología, quizá tenga una perspectiva del mundo distinta, quizá tenga, y esto seguro ustedes lo han analizado dentro de las perspectivas de cómo hacer *marketing* y cómo encontrar los canales de distribución hacia las nuevas generaciones, quizá vamos a encontrarnos con gente que no está tan ligada con las organizaciones donde trabajan, como lo estaban las generaciones anteriores.

Les comparto, tengo 10 años trabajando para Fortinet, pero si bajamos la escala para ver cuál es el tiempo que una persona que tiene entre los 18 y 30 años pasa en promedio en una empresa, vamos a encontrar que el tiempo es menor a los dos años, y eso tiene que ver con la instantaneidad, eso tiene que ver con la instantaneidad, eso tiene que ver con lo que yo quiero hacer con mi vida como persona, y es un cambio que se da a partir de la tecnología, y a veces como seres humanos no nos damos cuenta.

Los que tienen la oportunidad de convivir con generaciones más nuevas, con aquellos que tienen 10, 15, 20 y hasta 25 años se van a dar cuenta que, inclusive, las normas de qué está bien y qué está mal socialmente han cambiado. Está bien si nos damos la espalda para tomarnos la selfie, pero está mucho mal visto que nos dejen en visto. O sea, que hayan mandado el mensaje y que lo haya visto y que no lo haya respondido, y eso ya es motivo de una discusión a veces, entre amigos, entre parejas, entre muchas personas. Está, mal a veces, que me publiquen en redes sociales, sin mi permiso.

Entonces esta manera en cómo vamos cambiando, cómo vamos evolucionando como sociedad, gracias a lo que la tecnología nos permite, impacta la manera en cómo las personas perciben el mundo, y esto tiene un nombre. Seguro van a escuchar cada vez más de términos como la Tercera Plataforma o la Transformación Digital o la Cuarta Revolución Industrial, porque justamente estamos pasando por eso.

Al día de hoy ya los medios que nos permiten generar riqueza no van por quién posee más tierra o quién posee los mecanismos de producción, como era en las primeras revoluciones industriales. Hoy quién es capaz de generar más riqueza, va más ligado con quién tiene

la inteligencia y la información, el acopio de la información, el análisis de la información para poder producir ofertas adecuadas para quienes lo están recibiendo.

Y de aquí para adelante esto va a ser muy relevante, porque la gente que va a venir a engrosar nuestras organizaciones, para colaborar con nosotros y crear más beneficios para todos. La gente que va a tener también el poder adquisitivo es esa generación que no conoce un mundo sin internet. De la misma manera en como nuestra generación hoy no concibe un mundo sin electricidad. Imagínense, por un momento, que no tengamos electricidad, yo creo que capaz que a alguno de nosotros nos da un infarto.

Así los jóvenes no perciben el mundo sin conectividad, sin movilidad, sin internet, sin redes sociales. Esto es algo que hace parte de la vida.

Y eso es interesante si lo empezamos a analizar desde otra perspectiva también. Si nosotros ponemos o vemos cuál es el empeño que están poniendo las organizaciones de todos los segmentos de mercado, para invertir en tecnología y entender mejor a sus usuarios, y proveerles canales de entrega que se ajusten a sus necesidades, que sean inmediatas. Vamos a encontrar que ese es un mercado de 7.8 trillones de dólares, trillones gringos, o sea billones nuestros, de dólares el año pasado, que todo mundo está poniendo en investigación y desarrollo para saber cómo es que vamos a entregarle productos, ofertas, servicios a estas nuevas generaciones.

Vea que por aquí tenemos, por ejemplo, también al mercado de ustedes, seguros basados en uso, por ejemplo. Seguros de autos que se modifican a partir de otros riesgos y ahorita vamos a ponerles un video de qué queremos decir con otros riesgos.

Realmente el mundo que conocemos hoy es un mundo en transformación, y somos muy privilegiados al pertenecer a la generación que está siendo el enlace entre un mundo que recibimos nosotros, que no tenía movilidad, que no tenía internet, que no tenía cómputo, que no tenía conectividad y vamos a dejar un mundo donde todo eso es parte casi, casi un derecho humano. Es parte de lo que todo mundo espera, de lo que todo bebé espera al momento de nacer.

Entonces vamos a dejar un mundo radicalmente distinto y para esto va a ser importante que las organizaciones entiendan, que los modelos de negocio van a tener que, sí o sí, aprovechar la tecnología para entregar estos valores de los que hablábamos al principio, entregar inmediatez, entregar conectividad, entregar una personalización en la oferta, algo que me llegue a mí; una publicidad que sea dirigida a mí, que me diga: “Martín, tú eres una persona con estas necesidades, ésta es la oferta de producto que te encaja a ti y a nadie más, y es algo que va a estar adecuado inclusive a tu capacidad de pago, que va a estar adecuado a tu modo de vida, que va a respetar tus creencias, que va a respetar tu identidad como persona, de nuevo, algo que cada vez más va a ser relevante y va a estar muy ligado a eso la percepción de valor que tengamos.

La experiencia de uso de la cual hablaban también está muy ligado a eso, es cómo hacemos llegar la oferta más rápido, cómo es que nos aseguramos que las interacciones entre las personas y nuestras organizaciones ocurren en una velocidad en donde no hay tiempos de espera. Porque así como nosotros somos exigentes y queremos que el App esté listo, los clientes, sus clientes, nuestros clientes y cualquier otro cliente se está volviendo cada vez más exigente en eso, menos tolerante a las esperas.

¿O alguno de ustedes va al súper, por ejemplo, y se encuentra fascinado para ver, bueno, vamos a escoger la fila que tiene más personas para pagar? ¿Todo mundo va al súper y hace eso, va y se forma en la caja que tiene más personas? No, buscamos la que tiene menos personas.

Y retail está buscando soluciones para que a través de los teléfonos inteligentes podamos predecir cuántas personas máximo tienen en la fila, por ejemplo, y que podamos dar salida a esas personas muy rápidamente.

Aquí tiene que ver con la experiencia de usuario, estoy seguro que todos los ustedes mueren de deseos para ir a un banco, a una caja, a un retail, a cualquier lado para que cuando les toque su turno de pasar a la caja les digan: “No hay sistema”.

Esto todo mundo está ávido de tener esa experiencia; no, ¿verdad? Los clientes tampoco.

Y cuando hablamos de experiencia de usuario, justamente, es esa disponibilidad de los servicios, es esa inmediatez en los servicios y es ese acercamiento que nos genera la tecnología para entender mejor a los clientes y poderles entregar el servicio que ellos esperan.

Esto, ya en lo han entendido algunas organizaciones como Amazon, como Uber, como Netflix, casos que estoy seguro ustedes han visto hasta la saciedad, pero se trata de eso; a veces es, simplemente, buscar cómo conectar mejor a los usuarios, con quienes les están proveyendo el servicio, y eso fue lo que hizo Uber, por ejemplo.

Los taxis, es una industria muy tradicional, existe desde antes del automóvil y, sin embargo, vino la tecnología a revolucionar el modelo de servicio, la experiencia de usuario, y se trata un poquito de eso.

A final de cuentas para poder llegar a ese escenario donde el cliente está contento, donde el cliente está satisfecho, donde siente que se le atienda rápido, donde siente que se le atiende con una oferta orientada a cada uno ustedes, a cada uno de los clientes, se requiere de confianza y es ahí donde empezamos a hablar de seguridad y de ciberseguridad.

Pero no podemos hablar de nuevo de seguridad y de ciberseguridad si es que no tenemos el contexto de por qué la tecnología es tan relevante para las personas y tan relevante para la sociedad.

A final de cuentas esa confianza es la que deben de sentir los consumidores al momento de transaccionar conmigo; esa confianza fue la que permitió, poco a poco, que cada vez más personas tuvieran la oportunidad de hacer pagos por internet.

¿Hoy cuántos de ustedes hacen pagos a su tarjeta de crédito, cuántos de ustedes hacen pagos a proveedores por Space hacia sus familiares o hacia negocios desde su casa?

Levanten la mano, ¿quiénes de ustedes lo hacen? Perfecto.

Si yo les hubiera preguntado lo mismo hace 10 años, quizás la respuesta hubiera sido muy distinta, y les apuesto que parte de las razones por las cuales no lo hacían, es la falta de confianza y es parte del por qué la ciberseguridad tiene que estar presente, es la generadora de esa confianza y es la mitigadora del riesgo de negocios que tenemos por hacer negocios, por establecer un canal de comunicación con el cliente, que no es el tradicional, donde no intervienen personas y donde a final de cuentas requirió un cierto período de adaptación, un cierto período de credibilidad para que esto tomara los tintes que tenemos hoy.

Pero a final de cuentas se trata de tomar en cuenta, para poder tener este negocio, como lo queremos, como lo necesitamos, productivo, cercano al cliente, produciendo inclusive más negocio por cada transacción, requerimos de la ciberseguridad, requerimos de encontrar cómo vamos a proteger, no sólo la información, no sólo los activos con los cuales manipulamos la información, sino cómo vamos a proteger inclusive a las personas que están interactuando con los sistemas.

Es por eso que hoy la industria de la ciberseguridad, habla justamente de ciberseguridad, porque no es solamente protección de los datos, no es solamente seguridad del Internet, es protección de todo en su conjunto, incluyendo normas, regulaciones, incluyendo forma de pensar de la gente en cómo vamos a hacer que la gente se aproxime a los sistemas y tenga la confianza para hacer transacciones por ahí.

No es casualidad que tengamos hoy bancos que operan 100 por ciento a través de Internet. A final de cuentas, la tecnología también nos permite reducir muchos costos.

Con esto también es importante entender cómo es que el riesgo ha evolucionado.

Lejos están los días en los cuales, y aquí quisiera hacerles alguna pregunta, alguno de ustedes es tecnólogo o está relacionado con, le toca administrar algún aspecto administrativo o técnico de redes, computadoras y eso. ¿Alguien aquí?

Ok, perfecto, gracias, no muchos.

Entonces, esta lámina es importante.

Lejos están los días en los cuales el tener un virus de computadora, significaba que yo iba a perder horas-hombre, y que yo iba a perder la información que estaba en un disquete, recuerdan los disquetes de 3 ½, 5 ¼, un disco duro y que no iba a poder tener acceso al sistema y que yo iba a perder eso.

El impacto que teníamos ahí, sí efectivamente era la pérdida de trabajo de horas-hombre, pero era mucha la frustración. No puedo usar la computadora, porque tiene un virus, y hasta ahí se quedaba.

El riesgo fue evolucionando, y después tuvimos la oportunidad de que gracias a que me escribía una linda rusa que había visto en mi perfil en línea y que me encontraba muy atractivo y entonces quería iniciar una conversación conmigo, o que tenía la suerte de que el hijo de un finado Heke africano quería compartir 20 por ciento de sus 20 millones de herencia conmigo, qué suertudo, empezamos a tener también estafas por internet.

La cosa fue evolucionando, y a medida que empezamos a tener tecnología vestible, que empezamos a cargar toros con el celular, la cosa fue poniéndose cada vez más distinta.

Cuando empezamos a incorporar tecnología en sistemas tradicionales, encontramos situaciones que a veces no hubiéramos pensado hace algunos años, y es ahí donde tenemos la situación, por ejemplo de esto.

Los dejo con el video.

(Proyección de video)

En un par de minutos regresamos el video para tocarlo una vez más, pero lo que es el video básicamente es un reportaje de 60 minutos en Estados Unidos. Hace ya un par de años se encontró una vulnerabilidad en los autos de una marca, no quisiera ser muy específico, pero si ustedes buscan en Google “*hacking* de autos”,

seguramente van a encontrar mucho detalle con esto y más información.

Lo interesante es que la señora que está ahí en el auto sabe que está haciendo la prueba de un auto, ella no sabe que está participando en un ejercicio donde alguien le va a *hackear* el auto y el *hackeo* es muy simple, una persona con una laptop a unos metros de distancia desactiva el sistema de frenos del coche. Ustedes vean la desesperación con la que la persona dice: “No puedo frenar. Dios mío, esto da mucho miedo”.

Efectivamente, los pongo a reflexionar tantito y quiero que se imaginen por un segundo estar en una situación donde ustedes están conociendo un auto y no tienen control de él. Esto parecería de ciencia ficción, de hace unos 10, 15 años, pero esta es una realidad que puede suceder hoy con las condiciones adecuadas.

Bien decían que hay más cosas de las cuales podemos tener miedo. ¿No sé si quieran regresar el video, por favor, una última vez?

(Proyección de video)

Es una situación real. Ahora, la pregunta es: Este tipo de situaciones se van a empezar a presentar con otro tipo de elementos, ¿cómo que es que una industria que trabaja en función del riesgo considera esto al momento de calcular su exposición, al momento de calcular cuál es la posibilidad que alguna cosa de estas ocurra?

Por ejemplo, ¿cuántas personas deberían considerar esto como algo válido en un producto tan tradicional como el seguro de autos? Para poder decir: “Quiero estar protegido contra este tipo de eventos también” No es lo único. Seguramente escucharon de esto que sucedió el viernes, afortunadamente nos dieron la oportunidad de actualizar con esta *slide* y la que sigue la semana pasada para traerles esta presentación, pero seguramente se enteraron de esta situación que sucedió jueves, viernes, salió en las noticias, le dieron un montón de cobertura, pero se trata de un randsomware. ¿Qué es randsomeware? Es un programa malicioso que cifra mi información, es decir, que protege mi información, porque esta tecnología de cifrado

también se utiliza para protección, de tal manera que no puedo acceder más a esta información.

Si yo quiero acceder a mi información me piden un rescate, en el caso de estos señores era 300 dólares vía una moneda virtual, aquí no se vale cheque, no se vale tarjeta de crédito, no se vale Spei, no se vale nada, es vía Bitcoins, con los cuales voy a pagar para que me den una llave para poder acceder a mi información.

Ahora, muchos decían hace algunos años que no tenían información relevante, que no eran el pentágono, no eran un banco, sino un simple mortal, pero les recuerdo que aquí todos traen información que no les gustaría que nadie más supiera, chats, correos, y me refiero a cosas profesionales y personales, no estamos hablando de infidelidad, estamos hablando de la organización de la fiesta de fin de año, cumpleaños de alguien más, pero todos tenemos aquí información que no queremos que nadie más vea.

Todos tienen aquí fotografías que no les gustaría perder y la pregunta para ustedes es: ¿Cuándo fue la última vez que verificaron el respaldo? Estoy seguro que aquí todo mundo está hablando de riesgos, todo mundo respalda la información en su celular diariamente, por lo menos cada semana estoy seguro que lo hacen, pero quién probó que esos respaldos funcionaran.

Y cuánto pagarían por recuperar esa foto, esa copia del documento, ese texto que tienen guardado aquí, y es en eso en lo que se basa en *rasonware*, que la gente a medida que la tecnología se hace parte de la vida de las personas. La gente está dispuesta a pagar por la información que coloca no solo en su laptop, no solo en el servidor de la compañía, pero en tablet, en su teléfono y es un riesgo con el cual también tenemos que vivir, y es un riesgo que reconozco que ahí soy un completo neófito e ignorante, no sé cómo se calcula eso desde el punto de vista para saber cuánto vale, pero seguramente aquí hay muchos expertos. Conocen expertos y eso quizá pueda ser interesante para algunas personas que aprovechan la tecnología para estar todos los días trabajando.

Esas fueron algunas estadísticas, esto lo sacamos el viernes. Fue cuando tuvimos la oportunidad de actualizar la presentación. Quiero

que vean esto. Esta es la vulnerabilidad, así se le conoce técnicamente al desperfecto, digamos, que se aprovecha para tener acceso a los sistemas.

La vulnerabilidad, es una vulnerabilidad conocida desde marzo. Desde marzo sabíamos que esto existía y no se había aprovechado. Vean cómo hay por aquí algunas incidencias y de pronto llegamos al 12 de mayo y pum. Vean que esto fue muy poquito, a más de siete millones de acceso en algunas horas, y estos son los sistemas sobre los cuales nosotros pudimos detectar esto.

Hay muchos sobre los cuáles no. Por aquí si se fijan México está en los top ten de entre los cuales, primero, tuvimos el ataque, la visibilidad nosotros. Esto es algo que nos debería preocupar y nos debería ocupar en un mundo donde la tecnología se está usando para cada vez más cosas.

Hay algunos ataques que fueron registrados contra marcapasos, por ejemplo. De nuevo, yo estoy seguro que más de alguno de ustedes dice: Esto me lo están sacando de la película, y ahí rellena el espacio en blanco. No, eso es una realidad. Tenemos ataques en marcapasos, tenemos ataquen en bombas de insulina, a dispositivos médicos que están conectados con personas.

Y es de nuevo cuando la palabra ciberseguridad cobra más relevancia, no es solamente proteger la tecnología, los activos, la información, es proteger la vida de las personas, cómo esto está considerado en los productos que atienden salud, que atienden vida en las personas que lo tienen.

Les digo que yo, les cuento brevemente mi caso personal. Soy sobreviviente de cáncer, tuve una situación con eso hace algunos años, y hoy parte de los seguros que vienen, me dicen: “Sí, pero qué de enfermedades has tenido, ¿cuál es tu riesgo en la familia? ¿Quiénes han tenido diabetes y demás?”. Lo que nos hacen a todos cuando contratamos un seguro que está bien.

¿Cuántos tienen en el cuestionario en la parte de cálculo de riesgo este tipo de situaciones? Y va a tener que hacerse. Y va a tener que hacerse porque cada vez más personas van a venir adoptar esto.

Entonces no es solamente cómo vamos a hacerles el seguro adecuado para ellos, cómo es que se los vamos a entregar más rápido, cómo se lo vamos a entregar de la forma más personalizada, pero también que cubra las necesidades en un mundo que aprovecha la tecnología de formas que no lo habíamos visto antes.

Si a esto le ponemos por delante que existe al día de hoy toda una organización criminal. Muchas organizaciones criminales que según algunas estimaciones iguala o supera las ganancias que genera el narcotráfico, para compararlo con otra estructura criminal.

Vamos a ver que hay gente que está muy interesada en hacer dinero a través del cibercrimen, y es algo que si ustedes ofrecen seguros contra secuestros, de nuevo. Seguros contra los cibersecuestros, contra el *rasonware*, que el mundo finalmente se enteró de que existía el viernes pasado y en algunas ocasiones nos enteramos de una muy mala manera.

Y prevenirlo es relativamente muy simple, guardemos copias de seguridad de nuestra información, respaldos. Tan simple como eso. Llegan, me encriptan la información, listo; quédate con la información, reinicio el dispositivo y recargo mi respaldo, pero la mayor parte de la gente no lo sabe y es parte de las cosas que a veces este cibercrimen organizado está utilizando, el robo de identidad.

Seguro que ustedes conocen de esto, pero cómo es que esto se controla en un ambiente donde tenemos de nuevo pequeños de ocho años con tablets y con celular, posteando fotografías, posteando identificaciones, posteando datos privados en redes sociales.

Quiénes de nosotros a veces, a pesar de estar con conocimiento del riesgo digital tenemos el espacio con la familia para decirle: “Mira, ten cuidado con el Facebook, ten cuidado con el WhatsApp, no creas todo lo que te mandan, no andes compartiendo cadenas porque por ahí puede ir oculto un bicho, muchas veces no lo hacemos y es parte de.

Aquí, entonces, en este punto es donde quisiera yo hacerles la invitación a reflexionar en cómo la ciberseguridad puede tener cabida en dos grandes mundos o en dos grandes áreas en el mundo de los

seguros; cómo es que la tecnología y la ciberseguridad me apoyan para darles una propuesta más acertada, más personalizada, más rápida a mis clientes y cómo es que también este tipo de escenarios tienen que modificar las tablas de riesgo con las cuales yo calculo primas, calculo la exposición y calculo otra serie de cosas, con las cuales yo hago mis cálculos tradicionales.

Cómo es que le podemos hacer para crear inclusive productos nuevos, está muy de moda que tengamos un grupo poblacional que le gustan mucho las mascotas, cómo ponemos un seguro para ellos.

Sabemos que hay gente que le gusta el estilo de vida vegano, cómo es que ponemos un seguro para ellos, con descuentos o con incrementos, según esto.

Entonces, cómo es que vamos adaptándonos con la tecnología a este nuevo escenario que tenemos como sociedad.

Nosotros lo que creemos en Fortinet es que todo esto a final de cuentas es parte de una sola filosofía y es parte del mensaje que queremos dejar con todos ustedes, que es importante que no consideremos la seguridad solamente como la parte que protege los datos.

Y si vamos a ver los datos, no solamente la parte de los datos del cliente, cómo es que la seguridad y la ciberseguridad se encargan, de nuevo, de generar esa confianza con el cliente, cómo es que ponemos seguridad para los ambientes legacy, que todas las organizaciones tienen.

Estoy seguro que ustedes tienen muchos sistemas que no han sufrido modificaciones por los pasados cinco, diez años, y alguno de ustedes seguramente lleva por ahí más tiempo que eso, que han visto el mismo sistema desde que entraron. Eso quiere decir que los sistemas no han sido actualizados y posiblemente esté fluyendo información crítica por ahí. Hay que protegerlo, hay que protegerlo porque hoy ustedes vieron las noticias, las gente que sufrió el ataque con el ransomware tuvo un impacto mediático, es un impacto mitigable, es un riesgo mitigable pero hay que trabajar en eso, independientemente de cuál sea.

Aquí lo que quisimos poner es cómo es que nosotros podemos tener un ambiente donde realmente existe mucha investigación y muchos ataques, que están sucediendo allá fuera.

Estos son algunos números de cómo lucen, según nuestras investigaciones los ambientes de seguridad y arriba tenemos, por ejemplo, cada minuto 60 mil accesos en el mundo, por cada minuto, de gente que está intentando hacer cosas maliciosas; 375 mil intentos de intromisión cada minuto; cada minuto hay 60 mil programas de malware que están siendo neutralizados; esto es en el mundo, si nosotros vamos a ver cómo es que están las cosas en México.

Aquí está el Snapshot de un día, en un día cualquiera vamos a encontrar que en México va a estar siempre en el Top-15, en actividades de intentos de intrusión, en actividades de intentos de control remoto de equipos, en actividades de intento de código malicioso a nivel mundial.

Estos son los números de acceso que tenemos en un día, como en este caso sacamos la estadística el 25 de abril, tenemos tiempo trabajando en la presentación, pero si alguien está interesado en ver estadísticas más recientes, o llevárselas más adelante, los esperamos con mucho gusto mañana en nuestro stand, pero es para darles una idea.

Esto no es ajeno a México, esto no es ajeno a América Latina. A veces pensamos que esto le pasa a Estados Unidos solamente y efectivamente a Estados Unidos le pasa mucho y casi siempre está en el número uno, pero México no está muy lejos de eso.

Estamos siempre en el Top-15, por el grado de penetración que tiene internet, por el grado de tecnologización que tenemos en nuestra sociedad, por el grado de adopción tecnológica que daremos nosotros como personas todos los días.

La ciberseguridad tiene que estar presente.

Esta ciberseguridad es una ciberseguridad que se lleva de la mano con muchas entidades en el mundo.

Hay gente como la Interpol, hay gente como la OTAN, hay gente en México como el UNAM Sert, hay entidades de gobierno privadas y públicas que se encargan de en conjunto hacer la inteligencia que permite tener la tecnología de protección.

Es válido que como sector asegurador, tal vez, existen enlaces con estas entidades, que les permitan entender mejor cómo es que funciona el riesgo digital, y cómo es que funcionan los ataques en un mundo digital.

Este intercambio de inteligencia, es el que permite, por ejemplo, tomar y ese fue un caso solamente de hace algunos meses, de un amigo nigeriano, amigo entre comillas, un joven de 40 años, que había hecho muchas estafas a través de ataques cibernéticos, y que le habían dejado 15.4 millones de dólares, algo así, como tres o cuatro meses.

A veces es muy redituable estar del lado negativo, no es una invitación, pero es también para ver que del otro lado se mueve dinero y como les decía hace algunos momentos, el cibercrimen realmente es algo que está en boga el día de hoy, sobre todo porque es muy difícil que podamos a veces detectar y que la legislación nos permita detener a las personas que son responsables por esto.

Siguen siendo delitos de cuello blanco, la legislación existe en México para poder proteger contra riesgos digitales, contra amenazas, contra los operadores, contra la tecnología, pero todavía existe mucho por avanzar, en término de procuración de justicia, cuando hablamos de ese tipo de crímenes.

Eso no va a impedir que los criminales estén actuando, eso no va a impedir que nos robe la identidad, eso no va a impedir que venga una máquina e inclusive un nacional, suelte alguna variante de ranson where y esté por ahí.

Simplemente les quería dejar para reconocimiento de la marca, Fortec es una empresa líder en ciberseguridad, tenemos presencia en México desde hace muchos años, tenemos una oficina muy grande donde tenemos investigación y desarrollo local también, y la invitación es para que mañana, por favor, si es que tienen la oportunidad, nos

acompañen en nuestro stand y si quieren charlar un poquito más de alguno de estos temas, que tengamos esa discusión abierta, que podamos entablar ese diálogo, que podamos ver cómo es que nosotros vemos como especialistas, la parte de seguridad en estos tiempos, donde de nuevo ya no es un lujo, ya no es solamente el tener seguridad, porque alguien me dice que debo tenerla, sino que es una necesidad, porque sin ciberseguridad, mi riesgo está muy alto.

Muchas gracias.

No sé si tenemos espacio para alguna pregunta. No sé si alguien tenga alguna pregunta, alguna duda, algún comentario, aprovechando el tiempo.

Pregunta: Yo tengo una duda: ¿Cómo se resolvió este ciberataque del día 12 y qué posibilidades hay que se repita pronto?

Martín Hoz: Es una excelente pregunta. Realmente al día de hoy no está resuelto. Cuando tenemos un *randsomware¸* el día 12 o cualquier otro, cualquier otro programa malicioso, regularmente el código se dice que es autorreplicable, busca propagarse y es por eso que en tiempos pasados se llamaba virus, porque emulan a los virus que buscan propagarse a través de diferentes equipos y a través de diferentes redes.

Entonces, eso no es fácil de detener porque es una cosa que es automática, las organizaciones, muchas, lo que hicieron el pasado viernes, fue apagar sus laptops, sus PCs, dar de baja sus servicios, para empezar a colocar en medio, entre su red y las laptops, mecanismos que les permitieran determinar dónde estaba el problema, a eso se le llama contención en el lenguaje de respuesta de incidentes.

Lo que se buscaba primero era contener el problema y poner estos aislantes que nos permitieran ir segmentando, para determinar cuáles equipos eran los infectados. Desafortunadamente para un equipo que ha sido infectado y que se le ha cifrado su información, debido a que el cifrado es una tecnología que también se usa para protección, lo que se busca es que no se pueda descifrar. Una vez que se ha cifrado la información es prácticamente imposible regresarla.

Es ahí donde cobraban importancia los respaldos, las organizaciones grandes que regularmente tienen una política de respaldos continua, tenemos respaldos completos, incrementales y demás, que cada organización establece cómo lleva los suyos, lo que hicieron fue, "¿sabes qué? de una máquina infectada vamos a recuperar el último respaldo disponible", y esa es la manera con la cual se lidia con este problema en específico, pero al día de hoy, les digo, infelizmente no pude actualizar las estadísticas, pero el domingo salió otra variante, ayer salió otra variante, hoy en la mañana salió otra variante que fue de otro tipo de sistemas, ¿cuál va a ser el efecto final de eso? Todavía estamos por verlo, pero si están pendientes de las noticias van a ver que prácticamente todos los medios están anunciando esto, porque es la primera vez que vemos un ataque a tan gran escala y tan divulgado, pongámoslo así.

Pero hoy el problema en sí no está resuelto, ¿cómo se pueden proteger ustedes? Que puede ser la siguiente pregunta, uno, no se olviden de los respaldos, dos, pídanle a su gerente de sistemas amigo que les ayude a revisar que sus máquinas estén actualizadas con parches, como se les llama, con la última pieza del código que corrige el problema conocido y por supuesto instalar tecnología de seguridad, hay mecanismos específicos que en la jerga de ciberseguridad se conocen como *firewalls* y como *sandboxings*, que nos permiten detener ese tipo de amenazas antes que se conozca con precisión cómo funcionan, pero existen tecnologías de inteligencia artificial que permiten también anticiparnos a estos ataques y que se puedan desplegar.

¿Alguna otra pregunta?

Sí, por favor.

Pregunta: Martín, después de escucharte mi antivirus era un juguete de niños, o sea, ¿no sirven de nada?

Martín Hoz: Los antivirus son una pieza fundamental en los esquemas de protección de las organizaciones. Ahora, el antivirus que tenemos al día de hoy no es el mismo que teníamos hace 10, 15 años, las tecnologías con las cuales lo antivirus funcionan en un principio, en

lenguaje técnico se le llama reconocimiento de patrón, es decir, buscar de manera estática y reactiva cuando hubiera un ataque, los nuevos antivirus utilizan maquinas heurísticas y algunas técnicas de inteligencia artificial para ser más proactivos, pasaron de ser reactivos a proactivos y de ser estáticos a ser dinámicos, para entender cómo trabajan los flujos de información y te puedo decir que el antivirus sigue siendo un componente esencial.

De hecho el antivirus es parte de *sandboxing* del cual yo les hablaba. O sea, sandboxing es una nueva técnica que tiene un programa, se recibe y se ejecuta y se simula que está trabajando y se simula que ha pasado tiempo, y se simula que se le pone información a la máquina, se simulan muchas cosas para entender cómo un programa va a reaccionar ante cierto ambiente.

Y si genera algún comportamiento extraño, por ejemplo, si encripta un archivo sin pedir permiso, si accede a algunas áreas de sistema sin pedir permiso, si establece comunicación hacia fuera cuando no se espera, se dice: “Epa, este es un archivo sospechoso”. Y pasa a otra serie de mecanismos más avanzados para detectar eso.

Eso es el sandboxing. Lo primero que hace un sandbox, debería hacer un sandbox es pasarlo por el antivirus para poder entender cómo funciona de manera genérica esa muestra. Entonces el antivirus sigue siendo una pieza fundamental para proteger tecnológicamente sus laptops, sus máquinas, sus teléfonos, pero es una tecnología que solita hoy no puede hacer todo. Es el equivalente en el aeropuerto a cuando solamente teníamos los detectores éstos de metales. Ahora tenemos detector de metales también en la mano, tenemos los rayos X. Vamos a Estados Unidos y nos pasan con la camarita ésta que es otro tipo de rayos. Entonces esa es la evolución que ha tenido también el antivirus.

Una última pregunta y los invito a mantener la conversación después.

La pregunta es ¿si cada vez serán más frecuentes estos ataques? La respuesta es: “Sí”. Digamos que para entender el porqué tendríamos que entender que la motivación ya cambió también. Hace algunos años un atacante, un hacker lo que buscaba era la gloria personal,

decir: “Yo tuve las habilidades y el conocimiento para burlar las defensas de algún sistema”.

Hoy los atacantes están organizados en bandas de cibercriminales para ganar dinero. Esto que se hizo el pasado viernes fue con la finalidad de ganar dinero, y lo que se estima es que debido cómo fue lanzado, digamos que técnicamente tenemos que hacer una discusión más amplia, pero parece que había ciertos detalles que hacen suponer que esto fue más bien una especie de estudio para ver cómo las organizaciones reaccionaban, y que viene un ataque preparado cubriendo esos gaps, cubriendo esas partes que hoy fueron fallas. Te doy un ejemplo, la primera versión tenía un switch de apagado, el switch de apago era que existía un dominio en internet, y también esa era la noticia de un chico en Inglaterra que hizo un registro de dominio, que es algo muy sencillo y con eso consiguió mitigar el ataque.

Si tú quieres que esto se replique tantas veces como sea posible y que cause más daño como sea posible porqué le pones este switch para apagarlo, no tiene sentido.

¿Por qué le apuntas a Windows, que es una versión del sistema operativo que no es la más expandida? Hoy la más expandida es Android, por ejemplo.

¿Por qué apuntas hacia una vulnerabilidad que es sobre un protocolo de red, que prácticamente ya no se usa, solamente en ciertas organizaciones?

Entonces hay una serie de cuestionamientos atrás de esto que hacen suponer, hoy decían que tiene ligas con Corea del Norte, otros después de haber visto las investigaciones que hicimos por nuestros laboratorios no creemos que vaya por ahí. Pero definitivamente esperar más ataques como éstos va a ser cada vez más común.

Hace algunos meses escuchábamos de un ataque que aprovechaba vulnerabilidades en cámaras y en dispositivos conectados a la red, que generó negaciones de servicio.

Entonces, la cadencia con la cual se van a presentar esos fenómenos seguramente va a ser mayor, difícil de predecir todavía porque no

tenemos suficientes datos hacia atrás, pero las condiciones nos dicen que sí va a ser así.

Yo les quiero agradecer, para no abusar mucho del tiempo, su paciencia, la gentileza de haberme prestado su atención.

Les recuerdo, mi nombre es Martín Hoz, soy Vicepresidente de Ingeniería de Fortinet para América Latina, y me da mucho gusto conversar con ustedes el día de mañana en nuestro stand, si es que nos hacen el favor de regalarnos unos minutos y charlar más a detalle con ustedes.

Muchas gracias.

----o0o----