Ciudad de México, 25 de mayo de 2022.

Versión Estenográfica de la sesión especializada de "Cyberseguridad en la nueva normalidad" de la 31 Convención de Aseguradores AMIS, efectuada hoy en Expo Santa Fe.

Francisco Díaz: Hola, qué tal, bienvenidos. Mi nombre es Francisco Díaz.

Quiero darles la bienvenida a esta plática que se titula "Cyberseguridad bajo la nueva normalidad".

Esta plática forma parte de las sesiones especializadas, sobre innovación y tendencias en la 31 Convención de Aseguradores de AMIS.

Y para esta buena ocasión, esta gran ocasión tenemos una gran invitada, Lorena Bravo.

Lore, bienvenida.

Lorena Bravo: Gracias, Francisco. De verdad, encantada y es un gran honor estar aquí con ustedes.

Francisco Díaz: Encantados de tenerte.

Lorena es Head of Technology, Transformation en Oracle. Es una ejecutiva senior, con más de 25 años de experiencia en la ejecución de innovación y migración a la nube de grandes arquitecturas, clientes y proyectos de nube híbrida.

Seguro muchos de ustedes la han tenido como proveedora y saben lo bien que se trabaja con ella.

Es responsable de la transformación digital, incluye tecnologías disruptivas como inteligencia artificial, blockchain, machine learning, digital assistant, inter of things, data-driven, data-analitics, data-sciences, data-machine, en fin, todos los temas de innovación y de actualidad.

Además de esto, es especialista en diseño de negocios digitales y en soluciones de experiencia en cliente, ventas, marketing y comercio electrónico.

Lore estudió Sistemas en el Tec, tiene una especialización de Inteligencia Artificial por el MIT, además de estudios gerencial en el IPADE, el Harvard, un master en Marketing Digital y actualmente se sigue actualizando, por si fuera poco, se sigue actualizando y especializando en transformación digital con la Universidad de Columbia.

Estoy seguro que encontrarán de muchísimo interés todo lo que Lore tenga que contarnos sobre este tema de Ciberseguridad.

Y nuevamente te doy la bienvenida, Lore, con muchísimo interés y gracias por estar con nosotros.

Lorena Bravo: Al contrario, encantada. El día de hoy tenemos temas que están siendo tendencia y sobre todo a *warners* para todas las empresas del sector asegurador, puesto que hay noticias importantes que vamos a compartir con todos.

Les presento a la agenda, vamos a iniciar cuáles son los desafíos que estamos viviendo en la industria de seguros y sobre todo la actualización en los proyectos que se están viviendo en transformación digital, de proyectos disruptivos, innovación, los temas de ciberseguridad, cómo es que a raíz de la transformación digital vamos a empezar a trabajar esas brechas y también qué es lo que hoy día estamos trabajando como arquitecturas, mejores prácticas, soluciones.

Vamos a conocer qué es lo que está haciendo la industria en este sentido y terminamos con estrategias de prevención, para pasar a las preguntas que ustedes tengan para nosotros.

Para eso vamos a trabajar un video, en el cual nos va a mostrar qué tendencias se está dando en el tema de ciberseguridad desde el punto de vista datos, porque para nosotros, las aseguradoras, los datos se convierten en el enlace más importante que podemos empezar a cuidar.

(Proyección de video)

Intervención: ¿Qué les pareció?

La Data se convierte en el patrimonio de nuestro negocio y saben que los ciberatacantes tienen dos objetivos en este momento.

Buscar esa Data y sobre todo los datos sensibles de nuestros clientes, empleados, proveedores y también la identidad.

En un proyecto de transformación digital en cuanto a las tendencias que tienen las aseguradoras ustedes pueden ver proyectos de omnicanalidad, personalización inteligente con los clientes, el trabajar valor en cada una de esas soluciones, incluso todas estas tendencias que vamos a ver como disruptivas a través del poder conseguir *inside*, queremos saber qué necesitan nuestros clientes, en qué momento vamos a llevar ese producto de valor en su vida.

Para esto también están las regulaciones y sobre todo sin olvidar nuestros agentes.

Entonces, ante estas ventanas los clientes me preguntan ¿qué va a hacer un proyecto de omnicanalidad? Pero también alineado a ciberseguridad, es posible hacer eso y también quiero tener *inside* en tiempo real, pero quiero prevenir riesgos, fraudes, necesito cuidar a los datos de mis clientes.

En este pilar que les muestro de tendencias ustedes ven claro el concepto de ciberseguridad como parte de esas tendencias y ese es parte de las soluciones que vamos a empezar a ver hoy.

Estoy construyendo un proyecto de transformación, quiero hacer omnicanalidad, quiero incorporar inteligencia artificial en el entendimiento en tiempo real, pero no olvidar que uno de esos eslabones importantes caminando en paralelo va a ser la ciberseguridad.

Vamos a ver ahora un ejemplo de cómo se ve la transformación digital en la industria, estos son casos que nos han compartido aseguradoras

en otros países y lo dividen en tres pilares: el primer pilar es experiencia del cliente.

Por aquí les puse un concepto que se llama figital y ustedes lo pueden encontrar ahí, estamos viviendo esa interacción, nuestros clientes ya viven en un mundo que es digital y físico.

Hemos visto, por ejemplo, cuando vamos a un centro comercial, estás usando tu canal digital para saber opiniones, incluso para pagar ahí, es mucho más fácil y vas, tomas tu producto y continuas o estás de viaje y necesitas adicionar un servicio a tu póliza de seguros.

Eso lo vamos a hacer de una forma digital, pero lo estás viviendo, entonces, en cualquier punto ahora estamos trabajando proyectos donde en cada paso que dan nuestros clientes, sea el giro que sea, vamos a estar con ellos desde el punto de vista físico y digital y esto va acompañado de nuevas tecnologías, porque queremos saber emociones, sentimientos, necesidades, qué pasa con su entorno, qué les preocupa. Hay proyectos muy avanzados de ese lado.

Un siguiente paso es toda la optimización de las operaciones. La eficiencia operativa y para eso vamos a incorporar dentro de esta plataforma digital todas las herramientas con analítica avanzada, que ahí tenemos ya casos a nivel mundial importantes.

Y el crecimiento, el modelo de negocios nuevo, acompañado de estas nuevas tecnologías que me permitan incorporar nuevos servicios, que pueda saber con anticipación que están necesitando mis clientes.

Ustedes pueden ver abajo tres pilares: el primero es la escalabilidad, que pueda yo darle a mi negocio, sobre todo, el hacer crecer las áreas de negocios con un modelo SaaS Service, pero un SaaS Service completamente avanzado, con inteligencia artificial, que me pueda llevar al time to market en un tiempo acelerado y, sobre todo, el pilar azul, la cyber seguridad y ahí es donde vamos a abordar ahora con los siguientes desafíos que ha provocado este paradigma.

El primero, con todos los nuevos modelos. Tenemos más amenazas que se están presentando, por ejemplo, ustedes seguramente están trabajando el modelo para Ramsomware, en México que está

creciendo. Este año, les cuento, tenemos un 200 por ciento de crecimiento, mayor anonimato, aumento del escrutinio regulatorio en la data y eso es algo que a nosotros nos va a llevar a la base de los modelos de negocio nuevos.

Tenemos la información en silos y sobre todo, en las diferentes áreas de negocio que trabajamos. Hay aseguradoras que me mencionan: es que no tengo automatizado los procesos y necesito conectarlos para poder, uno de los modelos, por ejemplo: prevención de riesgos, de fraude y ahora que está muy fuerte el tema del cyber crimen.

Ahora, la detección oportuna, investigaciones manuales. ¿Ustedes creen que con una investigación manual pueda adelantarme ante una situación de ataque? Y les voy a mostrar qué está haciendo el cyber crimen para que ustedes me respondan esta pregunta y sistemas basados en reglas.

Esos nos van a ayudar mucho. Les traje una tecnología nueva, que se llama grafos, que además para quien tiene base de datos, Oracle Enterprise ya está incluidos, solamente empezarla a utilizar y finalmente hablamos de la gestión de operaciones, falta de procesos automatizados, típicamente tenemos soluciones on primice y estamos ya creado ese *journey* hacia la nube.

Entonces, esto me está dando como resultado costos crecientes y sobre todo, abriendo la ventana a la inseguridad. Aquí es donde ya le damos por prioridad el trabajar con la cyber seguridad.

Estos son algunos ejemplos de los proyectos que se están trabajando con tecnologías disruptivas. Ustedes pueden ver con plataformas de maching learning, inteligencia artificial. Ahí, por ejemplo, tienen a Lemonade en su proyecto de omnicanal, tienen plataformas P2P, drones, hay casos donde trabajamos drones ya en siniestros de automóviles, hay OUT, AUT Bloched, realidad virtual, hay un ecosistema gigantesco y cada uno de ustedes seguramente ya tiene un proyecto y aquí les pregunto, ya tienen esta innovación ¿qué están haciendo para cuidar la seguridad de sus datos, la seguridad de sus identidades? ¿Existe un proyecto en paralelo?

Solo por recapitular, hace dos años teníamos un ataque cada 19 segundos, hoy es cada 11 segundos, que decimos en este año, lo que va de enero a mayo, estamos sobre 200 por ciento en ataques de *rams*, como ustedes lo pueden ver, justo hace un año teníamos el 150 por ciento de crecimiento en ataques a las empresas mexicanas, estos datos que les estoy dando son datos para México.

También el tema de suplantación de identidad es algo que nos preocupa porque estamos igual duplicando el crecimiento, hablamos de una economía que representa seis trillones a nivel mundial y sigue creciendo, de hecho los analistas nos proyectan que para 2025 y esto se vuelve sumamente importante, va a crecer a 10, se imaginan a 10 billones, esto, esto nos va a llevar a una situación de riesgo mucho más importante.

El 81 por ciento de las organizaciones en México al menos ha sufrido cuatro ataques. Ante esto, vean ese dato, suplantación de identidad 292 por ciento y sigue creciendo, entonces, estos son datos alarmantes que realmente nos preocupan y más que estamos haciendo un proyecto de innovación, de transformación para nuestro negocio.

Otro dato importante, para México ya se están incorporando estos nuevos servicios de seguros para *rams* (…) estamos en un 46 por ciento de uso, si ustedes lo ven, comparado con los diferentes países, más menos llevamos una tendencia muy parecida con excepciones especiales, pero esto nos va a llevar al crecimiento que se proyecta este año es mucho más alto.

Aumentaron 40 por ciento en promedio el uso de estos seguros y se experimenta que para este año va a haber un 400 por ciento de incremento, lo cual nos va a dar más del 80 por ciento de otras industrias, va a empezar a utilizar eso y sabemos que hay también nuevas regulaciones en el uso de estos productos.

Estos nos lleva a resumir cuáles son exactamente las preocupaciones en la industria de las aseguradoras y aquí las violaciones de datos han aumentado, ese es una de las más importantes, continúan en aumento los ataques dirigidos para las aseguradoras, las estafas en medios sociales para empleados o para los usuarios de las aseguradoras

Phishing y Ransomware, esos son de los principales, pero les tengo una noticia, el Phishing trae novedades, no es el que conocemos y aquí es donde viene la preocupación y Ransomware también se modernizó y trae otras alternativas que están paralizando la operación, dándonos lugar típicamente a un proceso de Ransomware, tarda 12 días en lo que vamos resolviendo, en lo que se hace los diferentes, se pagan penalizaciones, ahora están haciendo que sea en menos tiempo porque paralizan la operación del negocio.

Y, ¿qué es lo que está provocando todo esto? Bueno, pues tienes amenazas internas, a esto le llaman los *insiders* y típicamente vienen de empleados negligentes, agentes internos, empleados descontentos, pero saben también qué encontramos, a raíz de los ataques que se están haciendo de phishing hay robo de credenciales, puede ser que por ahí digan: Lorena entró a las 3:00 de la mañana, quién sabe qué hacía y quería accesar datos de la nómina y quizás Lorena ni siquiera sabe que sus datos ya fueron comprometidos, pero Lorena hoy recibió una foto de gatitos y le dio clic, algo pasó y ya sus credenciales están siendo utilizadas.

Entonces, ahí viene el empezar a entrenar a nuestra gente para no baja cualquier archivo que les está llegando porque hay un ataque dirigido a la empresa.

¿Qué cosas me pueden llamar la atención a mí como Director de Tecnología, como Director de una Aseguradora? Solicitudes de acceso inusuales.

Por ejemplo, Lorena está en un café o está en un IP desconocida, está haciendo un *copy.*, o sea, eso es extraño, intentos para que me den más privilegios; Lorena, que está en tecnología ahora me está pidiendo accesar a Recursos Humanos; son cosas extrañas.

Entonces, ese tipo de situaciones son alertas para que ustedes empiecen a considerar que no es usual, es un patrón de ataque.

Amenazas externas, en este caso en ransomware, que se los señalé en rojo porque es una de las estrategias dirigidas a esta industria, las nuevas modalidades de phishing, ahora les voy a mostrar, ataques de gestión de claves, hay nuevas herramientas para que se pueda

accesar el PIN de WhatsApp, de hecho se tarda 59 segundos, y para poder obtener las credenciales de los sistemas de trabajo, de redes sociales a nivel personal. Pero lo que busca es tener las credenciales de su trabajo.

La suplantación de identidad, incluso les voy a mostrar un video donde estamos mostrando la nueva herramienta, donde con machine learning cambian, toman todo lo que los ángulos de tu cara, cada punto, y hacen una suplantación perfecta, tu voz, tu movimiento, pero con mensajes distintos y pueden hacer campañas de desinformación, campañas posicionando algún producto, pidiendo que den clic para robar tus credenciales o incluso campañas para hacer algún fraude.

Todo esto me lleva a que vamos a recibir por parte de los atacantes intenciones de corrupción de datos.

Ustedes saben que en el mercado negro se están haciendo ventas de base de datos y los últimos ataques que se han presentado. Tienen el caso que ahora se está viviendo en Costa Rica.

Y la venta de esas bases de datos es completa, están ubicando contratos, están ubicando Estados Financieros, tienen un perfecto respaldo de todo el control de negocio y está en venta.

Entonces, imagínense que los datos sensibles de su negocio llegan a estar en ese mercado negro, estamos exponiendo no sólo a nuestro negocio, a nuestros clientes.

Y aquí mi pregunta, ¿cómo están protegiendo esos datos, ¿qué están haciendo para identificar los datos sensibles y poderlos proteger?

La denegación de servicio es lo que se le llama DDOS, es otro de los ataques. Por ejemplo, hay aseguradores que me dicen “No puedo aceptar pagos, no puedo hacer que funcione mi servicio a través de mi web para poder dar atención vía estrategia mi canal a mis asegurados”, ¿Por qué? Porque está bloqueado ese servicio, y entonces van a empezar a vivir, de hecho los últimos ataques que se han hecho con aseguradoras ha sido la denegación de servicio, ha sido la parte de ransomware y por correo electrónico.

Entonces, eso nos va a llevar, incluso en las oficinas están haciendo ataques físicos, están robando las identidades de los *bach*.

¿Qué está haciendo el cibercrimen? Y esto, de verdad, es impresionante, porque el cibercrimen está trabajando con tecnologías que me están llevando a esa inteligencia.

Por ejemplo, el Dirty Business Card Reader sólo con un correo y el nombre de la persona pueden tener toda la historia en sus redes sociales, absolutamente toda.

Y hay otra herramienta que se llama OSINT. Ese OSINT hace un cruce con patrones de reconocimiento que te va a traer no sólo qué está haciendo la persona, sino con quién está interactuando, hasta llegar a sus credenciales y tener una copia perfecta de información de su negocio.

Esta es una metodología completamente avanzada con las últimas herramientas, entonces, cuando se tiene un objetivo de ataque trabajan todas estas herramientas para hacer paso a paso cada uno de estos objetivos.

Ahora, partiendo de eso una de las herramientas fundamentales para poder atrapar esas credenciales son *Fake News*, noticias que son extrañas, pero van enfocadas a lo que nosotros saben que nosotros saben que leemos o, por ejemplo, si saben que a Lorena le gusta comprar tenis, ah, bueno, 90 por ciento en tenis y Lorena: “guau, esa marca nunca la ponen”.

Bueno, vamos a mandarle una campaña o, por ejemplo, a Lorena le gusta comprar moneda digital, “mira, está ahorita esta promoción”, entonces, pero todo esto es para poder robar tu identidad digital, tus credenciales y lo logran, realmente porque te conocen.

Les voy a enseñar ahora cómo están haciendo suplantación de identidad a nivel video y lanzando campañas donde envían mensajes completamente para poder engañar a la gente, vamos a verlo, se llama *Deepfake*.

(Proyección de video)

Lorena Bravo: ¿Qué les pareció? Increíble, ¿no? Se imaginan, de hecho, ya lo hicieron con políticos, lo hicieron con personas del medio artístico, te imaginas que tu empresa esté enviando un mensaje a través de un video con una supuesta promoción o engaño y la gente lo va a aceptar como que fue una realidad y realmente no eres tú, tomaron los rasgos de tu cara, de tu voz y lo hicieron con *Machine Learning*, este ejercicio les lleva cinco minutos y es una de las grandes preocupaciones para esta industria porque lo van a empezar a ver ya mucho más seguido.

Bueno, ¿qué estrategia estamos trabajando para protegernos de estos ataques, de hecho, en Phishing, por ejemplo, hablando de los nuevos ataques en Phishing, acaban de liberar uno que se llama Triton y ese Triton es peor de letal que Ransomware, ¿por qué? Porque cuando te envía un mensaje por correo o a través de una fotografía, un mensajito en tu herramienta de mensajería, eso lo que hacen es llevar este código malicioso para poder detener la operación, de operación, por ejemplo, emisión de pólizas o que no funcione el sistema que está levantando siniestros.

Realmente la operación de tu negocio, llevándote a una situación de negociación acelerada.

Hay otra herramienta que se está usando también con esta nueva modalidad que se llama *Devil,* en la cual están atacando vía correo electrónico con mensajes falsos, pero a nivel volumen y esto lo están sufriendo ya las aseguradoras, ya hubo casos extremos y es el inicio para poderte distraer a una contingencia de Ransomware, que este es uno de los puntos más importantes que se está buscando con las aseguradoras.

Ahora, en temas de qué mejores prácticas están usando en la industria. Bueno, primero la detección de ataques dirigidos, para eso necesitamos una herramienta que esté monitoreando las amenazas externas, internas, listas negras. Toda esa data que viene, poder analizar e identificar patrones que pudiera ser un ataque, el perímetro de seguridad, pero hablamos de que sea completamente 360, integrando agentes externos, oficinas, atención al cliente, necesitamos

tener ubicado y también, con esa data integrando para reconocer algún patrón malicioso.

Seguridad en la nube híbrida. Importante considerar este firewall, que permita, no importa las nubes que tenga, no importa si me conecto con los sistemas de mi empresa. Tener esa inteligencia para las redes aisladas, sobre todo un monitoreo con inteligencia artificial.

Se los mencioné varias veces y de verdad, se los pido, el poder identificar y poder proteger su base de datos sensibles. El principal reto que hemos vivido, cuando les preguntamos ¿sabes cuál es todo tu catálogo de bases de datos sensible? La respuesta es: lo estoy actualizando. Y bueno ¿cómo lo estás protegiendo?

El otro punto es la identidad, los accesos. Hoy día el foco principal es la data y llevarme tus credenciales para empezar a sembrar ese código y prepararnos para Ramsomware.

El programa de concientización para la gente. Existe entrenamiento y de hecho hay mucho entrenamiento gratuito, ahora mismo Oracle tiene un plan de entrenamiento gratuito, con certificación para que nuestra gente se prepare y no cualquier mensaje que reciba lo aplique, que esa es la parte importante y el trabajar de forma inteligencia un back-up. Porque, acuérdense que ante una contingencia de Ransomware necesitamos habilitar aplicaciones y base de datos y en Ransomware se están llevando los back-ups.

Entonces, esa es otra de las partes que nos ha ayudado a rescatar las empresas ante esta contingencia.

Bueno, del lado de Oracle ¿qué estamos haciendo? Trabajamos la seguridad, la base de datos, una nube, un premice. Trabajamos la seguridad en las nubes y lo que hablamos cómo proteger la identidad y el acceso en cualquier plataforma, bajo las certificaciones del cumplimiento, regulaciones que ustedes conocen que eso es importante y, sobre todo, hablando de algo que se llama defensa en profundidad y esto no es más que poner seis capas a la base de datos.

¿Se imagen seis capas? Voy a hablar del enmascaramiento. Si se llevan mi base de datos y Lorena anda por ahí haciendo copia *.* se va a llevar basura, porque no le va a servir y la clave es un enmascaramiento. Si se dan cuenta del enmascaramiento hasta la data, hay seis capas y esta es la parte clave que les pido consideren, porque de esta forma vamos a proteger la data de nuestro negocio.

Ahora, la gestión de identidades y control de acceso va conectada a recursos humanos, va conectada al perfil, va conectada al tipo de función que tiene la persona, por eso ustedes lo pueden ver ahí y si hay alguna actualización se va a hacer inmediata, ¿saben qué nos hemos encontrado? Que la persona ya está en otro rol y sigue con sus mismos privilegios, la persona ya se fue y muchas de esas personas siguen con privilegios y accesos y saben el riesgo que nos pone, incluso la actualización, muchos de estos procesos se realizan manuales y ya no nos da el tiempo para hacer.

Vamos ahora a las mejores prácticas, ya estamos por terminar la sesión. Hablamos de ser otros y esta es la base con el cual hacemos el trabajo desde control de acceso, la administración de claves, auditoría, encripción, enmascaramiento que ya lo vimos y se convierte en la base fundamental de nuestra arquitectura, una arquitectura de máxima seguridad, aquí el equipo de Oracle les ayuda a trabajarla y de hecho lo estamos haciendo sin costo para poder ayudarlos y es una arquitectura completamente agnóstica.

Otra arquitectura es, no, no, a mí no me aplique esa, yo tengo nube y tengo un (…) muy bien, trabajamos también una arquitectura completamente híbrida y les voy a traer algo muy bonito y que les va a impactar, que son las predicciones utilizando grafos, redes y *machine learning*.

Esa prevención de fraudes que hablamos la hacemos con grafos y estos grafos es una herramienta que está en la base de datos, no necesito comprar si yo ya la tengo, es parte de, solamente utilizarla, esos grafos lo que hacen es con patrones de fraude que se ha trabajado en otras investigaciones se incorporan como alto riesgo y esos empiezan a mapearse con las combinaciones que se van dando con la data que ustedes van recibiendo.

Hacemos también *blockchain* para proteger la identidad digital, tenemos escenarios, por ejemplo, *blockchain* en la retina, esto nos ayuda en algunos ejercicios que hemos hecho para la emisión de pólizas digitales 100 por ciento a través de una plataforma unicanal y eso nos ayuda a proteger la identidad digital de nuestros usuarios.

El poder trabajar de forma preventiva el cibercrimen a través de los analíticos con grafos, a través de *machine learning* para poder identificar detecciones anómalas es fundamental, esto es una tecnología nueva que está manejando Oracle, si ustedes están interesados, bueno, hay *webinars*, hay *workshops* que están muy avanzados en cibercrimen, de tal forma que podamos habilitar, de hecho, ya está la plataforma lista, con las tecnologías avanzadas, simplemente incorporarlo, aquí no tienen que desarrollar nada.

Las lecciones aprendidas para hoy, primero, es importante descubrir y clasificar nuestros datos, ¿cuáles son sensibles?

Segundo, encriptar, enmascarar la base de datos, por favor, y eso de verdad es lo más importante y la prioridad en este momento, la gestión de claves de cifrado, cómo estoy protegiendo los privilegios, las identidades, los accesos, qué estoy haciendo para llevar de forma automática ese proceso para que pueda proteger la identidad digital de mi gente y mi negocio y finalmente, monitorear, alertar y bloquear.

Y aquí, pues nos llevamos con el mensaje de cómo estamos protegiendo las credenciales y las identidades de nuestros clientes.

Y bueno, pues vamos a las preguntas, espero que este tema les haya gustado.

Francisco Díaz: Lore, nos gustó muchísimo, lamentablemente los videos no pudimos escuchar sonido, pero yo creo, ya no vimos qué obligaron a decir a Lola Flores, pero yo creo que ya vimos en el pasado todos a la Princesa Leia actuando después de que se había muerto Carrie Fisher.

A mí lo que me pareció increíble es cómo esto ahora se hace de alguna forma mucho más sencilla y se puede hacer mucho más rápido, con una inversión de tiempo mucho menor.

Entonces, muy interesante, muy interesante es también todos los ejemplos que nos pones.

Voy a tratar de pensar en preguntas que hubieran preguntado mis colegas de la industria si estuviéramos estado presentes.

Lo primero, hablas mucho de mejores prácticas, entonces todas estas mejores prácticas yo creo que son muy relevantes, muy obvias y cosas en las que nosotros hemos pensado como tenedor de datos. Pero, primero te quisiera preguntar qué mejores prácticas has visto y cómo se han transformado con la nueva normalidad ahora con la gente trabajando desde casa, accesando desde diferentes puntos, ¿qué cosas nos podrías comentar ahí?, ¿cómo viste que evolucionó en los últimos dos años?

Lorena Bravo: Es muy importante esa pregunta.

Cuando iniciamos nueva normalidad, la gente habilitó su oficina en casa, el teletrabajo. Una de las principales ventanas de riesgo fue la utilización de la VPN, que la mayoría no la está utilizando, sino que tenía el canal abierto hacia las redes sociales.

Dos, se incorporaron herramientas para administración de trabajo remoto y esas herramientas las empresas, algunas consideraron gratuitas y tenían también el acceso hacia código malicioso.

Entonces, se abrió la ventana de riesgo, eso fue lo más importante, y ahí es donde se incrementaron los ataques.

Inmediatamente las empresas se dieron cuenta y empezaron a trabajar ya con mensajes mucho más enfocados en poder proteger a través del uso de VPN, limitar con reglas el poder incluso solicitar información temprana.

Entonces, la evolución prácticamente en los primeros seis meses fue cuando estaba la adaptación.

Posteriormente, empresas como Oracle y otras en el mercado empezaron a llevar este tipo de mecanismos para poder trabajar alertas, entrenamientos a la gente.

Al año ya las empresas ya tenían controlado sobre todo la ventana de riesgos, que esa era la parte más importante, y la incorporación de herramientas de seguridad.

Por ejemplo, el múltiple factor de autenticación, en algunas también los biométricos conectados con las herramientas que tenían de seguridad.

Por ejemplo, Oracle, con una alianza a nivel global con Cybereason, Cybereason es una empresa que hoy día tiene un portafolio de soluciones muy fuerte para poder proteger ataques de ransomware. Entonces, se empezaron a incorporar estas herramientas.

Voy a hablar de un caso que viene de estos primeros días de Zoom. Zoom estaba con alrededor de 10 millones de conferencias y hubo una situación de seguridad en este día a día, y hace un movimiento hacia la nube de Oracle.

La nube de Oracle tiene esas capas de seguridad ya como parte de la plataforma y estaba creciendo a 300 millones, o sea, crecimos en ese primer bloque de la nueva normalidad crecimos con las conferencias de 10 millones a 300 millones al día, incorporando elementos de seguridad.

Entonces, realmente a partir del segundo año lo que hemos estado haciendo ya es llevando herramientas más enfocadas a prevención, que ahorita lo más fuerte como mencionamos es el ransomware, es la suplantación de identidad, es el robo de datos. Pero la gente hoy día está recibiendo muy bien las nuevas herramientas.

Sólo que sí vemos como una ventana de oportunidad es concientizar a la gente del uso de las redes sociales y de los mensajes que les llegan. Ese es el desafío que no se ha todavía logrado y eso lo vamos a hacer con mensajes, con entrenamiento, con los niños, que eso es muy importante, para poder llevar, que todas las herramientas corporativas puedan ser de la funcionalidad que estamos buscando.

Francisco Díaz: Es increíble pensar cómo ya logramos no contestar un teléfono que no conoces, pero abrimos todos los mails que no conoces, por otro lado, eso es un poco una dicotomía de cómo están las cosas y dónde hay que hacer mucho entrenamiento.

En cuanto a tema de datos, el tema de datos, como bien dijiste, es una de las materias primas principales para la industria aseguradora sin los datos, sin las tendencias de los datos nosotros no podemos construir nuestros productos y cada vez conforme va pasando el tiempo requerimos más datos de nuestros clientes para producir nuestros productos y producir productos que se ajusten también a esta nueva normalidad y a los riesgos que la gente quiere proteger.

¿Cómo nos ayudan las empresas de tecnología a proteger estos datos y a usarlos? Para poder esa seguridad de pedirlos y poderlos utilizar en la construcción de nuestros productos.

Lorena Bravo: Las herramientas que mencioné de prevención del cibercrimen o algo bien básico, la mayor parte de los clientes tienen, por ejemplo, la base de datos Enterprise, en esa base de datos hay una herramienta que se llama *graph analytics* o incluso si ustedes tienen otra plataforma seguramente con otra marca, seguramente hay herramientas en su plataforma que manejen grafos.

Estos grafos te trabajan patrones; es decir, relacionan eventos, un evento aislado no te sirve, hay que integrarlos con toda la información, las listas negras, los incidentes que ocurren, las peticiones extrañas, todo.

Y también algo importante que lo que se va a manejando como en la industria como conocimiento se integra y se hace un aprendizaje, ahí es donde los algoritmos de inteligencia artificial van aprendiendo y nos van mostrando cuál es ese patrón extraño y que realmente sí tiene un foco de ataque.

Entonces, estos algoritmos ya están disponibles, no es algo caro para implementar, de hecho, lo pueden hacer de una forma muy sencilla, incluso ustedes tienen más ventaja porque estos algoritmos, lo he trabajado con actuarios y para ellos es su día a día, simplemente es

mostrarle las mejores prácticas y facilitarle las herramientas, hoy hay capacidad, por ejemplo, Oracle ponía a su disposición créditos para que puedan poner ahí sus laboratorios, entrenamiento y es algo que te puede permitir construir tu labor, laboratorio con inteligencia, si el cibercrimen, ustedes vieron OSINT, es un laboratorio que usa *Machine Learning*, inteligencia artificial, yo no tengo eso, hay una desventaja.

Entonces, si de verdad los motivo a que integremos esa Data y aquí tienes dos beneficios: uno para prevenir y otra ya modelos avanzados donde estamos integrando las emociones y comunicarnos uno a uno con el cliente como si fuera mi VIP, conozco todo de mi cliente.

Entonces, mira, tienes dos ventajas para trabajar la Data y de forma segura.

Francisco Díaz: Sí, sí, interesante.

En cuanto a los números, hablabas de cómo han crecido los ciberataques y el efecto y el impacto que esto tiene en la economía, yo solamente parametrizarlo, en (…) lo hemos medido de diversas formas y sí, coincidiendo con los números y con las proyecciones de números, solo para darle un poquito de matiz.

Ese número al que se va a llegar en 2025 es más que el 50 por ciento del PIB de México y es casi el 2 por ciento del PIB mundial, no es un número enorme, es un número inmenso que aparte de esto, aparte de las organizaciones alcanza o va a alcanzar más o menos a mil millones de personas en el mundo.

¿Por qué comento esto? Porque nosotros como aseguradores tenemos un doble rol, tenemos que proteger los datos, tenemos que proteger nuestra actividad, de nuestra propia actividad aseguradora, a nuestros clientes, pero también tenemos que dar, hablaste en algún momento de primas de seguro cyber, tenemos que dar soluciones que permitan a nuestros clientes, junto con ustedes, con compañías de tecnología, un binomio para que esa cobertura sea mejor.

Entonces, cuando nosotros estamos generando un producto que puede dar cobertura a ciberseguridad, qué nos recomendarías que debería de ser las cosas principales que debemos de evaluar en un

cliente, para saber si ese cliente está llevando una buena gestión de riesgos o no.

Lorena Bravo: Hoy hablamos de un plan de ciberseguridad, que es tu base inicia y cuando hablamos con un cliente, la pregunta que hacemos: ¿pudieras mostrarme ese catálogo de datos sensibles? Es la base.

Porque, si tú tienes clientes y son millones de clientes los que estás trabajando en el día a día y de ese cliente manejas tipo de sangre, que es un dato sensible, la dirección, el teléfono. Estás hablando de un riesgo gigantesco.

Entonces, ¿cuál es ese catálogo y qué campos tiene ese dato? Es lo importante.

Segunda pregunta. ¿Cómo lo estás protegiendo? ¿En qué recursos está? ¿Qué servidores? ¿Qué procedimientos usas para trabajar ese blindaje ante un acceso no autorizado?

El segundo tema son las identidades. Nos hemos encontrado y eso se los comento. Vamos a tener un evento de ciberseguridad muy grande en la región, estos días y ahí se va a mostrar un ataque en vivo.

Cuando hicimos el ejercicio, entrando a la data web, había un despliegue importante de datos con incluso pasaportes, estaba toda la data en venta.

Una semana, dos semanas después, ya ves que se hace el ataque de Ransomware, porque ahora ya se están llevando estados financieros, contratos, están haciendo una copia del negocio para poder bloquearte.

Entonces, el cliente le pedimos que tenga un plan de ciberseguridad y no estoy hablando de cómo asegurar mis end points o mi password o mi antivirus. No. Es un plan de negocios donde pueda tener la mitigación de riesgos.

¿Qué pasa si yo tengo un ataque de Ransomware? ¿Tengo algún plan de mitigación ante la comunicación? ¿Qué le voy a decir a los

clientes? ¿Qué voy a hacer si me atacan en Ransomware? ¿Pago o no pago?

Entonces, ese plan, que de hecho podemos compartir con ustedes, trabajando con los expertos de la industria, nos han llevado a esa mejor práctica de qué es lo que debo considerar en mí, mi mínimo del plan para incluso mostrarlo, por ejemplo, ante una certificación, la Ley de Protección de Datos Personales en México existe un check list, alineado a ISO-27000.

En ese check list son cerca de 130 puntos, donde el cliente va viendo. Son puntos de procesos, de tecnología, de comunicación, de entrenamiento y esa es la base del plan. Entonces, esa sería la recomendación en el sentido de lo que están usando los expertos de la industria.

Francisco Díaz: Gracias, Lore.

Una última pregunta. Nos estamos casi quedando sin tiempo. En esta función, en la que nosotros damos protección también a las personas, a las empresas que están expuestas a esto, pues creo que todos estos son muy evidentes, todos estos controles y estos mecanismos son muy evidentes para grandes corporativos, para empresas que manejan muchas cosas que tienen un tamaño crítico muy relevante.

Pero, también hay un riesgo para las Pymes y hay un riesgo para todos nosotros como usuarios individuales ¿no? Entonces, ¿qué nos recomiendas ahí y qué nos recomiendas también como aseguradoras para hacer los cambios que se tengan que hacer y las protecciones que se tengan que hacer sin afectar la omnicanalidad de la que hablabas y la experiencia del cliente?

Lorena Bravo: Hablamos de esos proyectos de omnicanalidad y la práctica que están realizando en la industria no están considerando la ciberseguridad y uno de los factores más importantes es, en la omnicanalidad el centro del proyecto de la plataforma es el cliente, entonces, ese cliente va en una base de datos en un proyecto omnicanalidad es vital, ustedes es parte del proyecto, es cómo aseguro mi base de datos y hay dos temas aquí, cómo identifico cuando se da de alta un dato sensible porque incluso existen

aseguradoras que contratan grandes consultoras para hacer su catálogo e identificar los datos sensibles.

Hay herramientas que te permiten, ahora contiene una, es una audi que hace la auditoría en tiempo real y te dice: “mira, hay un dato sensible, lo protejo” entonces, auditar, saber cuáles son y enmascarar, mi básico, mi básico, mi proyecto, el *core* es el cliente, ese cliente tiene que estar.

Hablé de seis capas o seis niveles en una arquitectura de base de datos en profundidad, ese es el paso número uno para poder trabajar un proyecto de omnicanalidad sin que se pueda ver afectado o expuesto mi cliente y ya, hay otros pasitos ahí básicos que también podemos compartir una herramienta, pero ese sería el mínimo para poder trabajar.

Francisco Díaz: Lore, estamos con el tiempo encima. Te agradezco muchísimo tu participación, temas muy sensibles y que podrían dar miedo, pero creo que existen muchos mecanismos, muchas herramientas y muchas maneras de prevenir y de actuar en contra de esto. En la industria aseguradora estamos acostumbrados a prevenir estos nuevos riesgos.

Y, pues algo súper interesante, creo que con empresas de tecnología la industria aseguradora puede hacer buenos binomios para llevar productos al mercado que protejan ante todos estos nuevos riesgos crecientes.

Muchísimas gracias, un placer haberte tenido aquí y seguramente habrá nuevas interacciones o prontas interacciones.

Gracias por tu tiempo y por tu interés y por todos tus *insights*.

Lorena Bravo: Encantada, Francisco y les vamos a compartir los links para los eventos a la expedición hacia la bar web y herramientas para que si ustedes están iniciando sus proyectos de omnicanalidad, así como entrenamientos y certificaciones en ciberseguridad que hoy día ahora Oracle está promoviendo sin costo.

Encantada y muchísimas gracias por la invitación.

Francisco Díaz: Muchas gracias, hasta pronto.

Lorena Bravo: Gracias.

Presentadora: Muchas gracias a Lorena, a Francisco por su oportuna intervención sobre este tema para proteger nuestros datos y operacines virtuales.

No se desconecten, en breve regresamos.

--ooOoo--