Ciudad de México, 24 de mayo de 2023.

Versión estenográfica de la sesión "Amenazas Cibernéticas, Desafíos y Oportunidades", durante el Segundo Día de Actividades de la 32 Convención de Aseguradores de la Asociación Mexicana de Instituciones de Seguros (AMIS), realizada en la Expo Santa Fe.

Presentador: Son 10:50 de la mañana, vamos a dar inicio a nuestra siguiente charla.

Ya estamos de regreso aquí para tomar nuestras charlas de la Sesión o de la Sala de riesgos.

Aquí me queda presentar a Peilin Corbanese, ella es Vicepresidenta Analítica en EXL Service, es una empresa global enfocada en la consultoría en analítica avanzada y transformación digital.

Peilin tiene una amplia experiencia en la industria de seguros, dirigiendo campañas de innovación, analítica y transformación usando datos para mejorar retornos de inversión.

La charla que nos va a traer el día de hoy Peilin es: Amenazas cibernéticas, desafíos y oportunidades.

Por favor Peilin.

Peilin Corbanese: (Interpretación de inglés a español)… Ciberseguridad, porque mi nuevo amigo Pablo me acaba de decir que ustedes recientemente tuvieron una violación a los sistemas cibernéticos del Gobierno, es decir, se trata de algo bastante grave. Entonces hoy hablaremos del porqué es tan importante la seguridad cibernética y qué tenemos que hacer al respecto para aprovechar las herramientas con las que contamos para que todo esto mejore.

Primero que nada, quiero compartir con ustedes un video. Disfruten el video.

(Presentación de Video)

Nunca olvidaré que fue el 27 de junio cuando me despertaron a las 04:00 de la mañana, la llamada llegó de la oficina y me dijeron que habíamos tenido un ataque cibernético en nuestro *software*,

entonces se inició un proceso del cual hablaré ahora antes de entrar en los detalles del ataque, bueno, les puedo decir que AP Moller es una de las empresas de distribución de logística más grandes del mundo y nosotros, bueno, tenemos una parte significativa de nuestra infraestructura que hace que el mundo opere entonces cada 15 minutos en promedio, un contender llega a alguna parte, entre 10, 20 contenedores cada 15 minutos, entonces con eso entenderán la criticidad en nuestra infraestructura.

Nosotros fuimos atacados por un virus que generó daños colaterales, probablemente fue una situación de un ataque bastante grande y el impacto de este ataque fue que básicamente encontramos que tuvimos que reinstalar toda nuestra infraestructura… (Falla de Transmisión)… Tomar seis meses y, finalmente, se resolvió todo en 10 días y fue un esfuerzo heroico y tengo que agradecer a nuestros compañeros, a nuestros trabajadores.

Imagínense una empresa en donde se hace un embarque de 10, 15 contenedores que entra un puerto cada 15, 20 minutos y durante 10 días, no hay ningún sistema informático en operación, es casi imposible casi de imaginar.

Logramos sobreponernos a este problema con gente muy resiliente que pudo sobreponerse, sobre todo porque nada más hubo una caída del 20 por ciento en nuestro volumen, es decir, logramos manejar el 80 por ciento del volumen manualmente. Y los clientes, la verdad, apoyaron muchísimo para obtener estos resultados.

Vamos a los aprendizajes. Esto fue algo muy significativo, algo que nos hizo despertar en la organización.

Podemos decir que fue una alerta muy costosa, nos costó entre 250, 300 millones de dólares, sin embargo, argumento que sigue siendo una llamada de atención muy importante.

Primero que nada estábamos en un promedio, en lo que se refiere a seguridad cibernética como muchas empresas, esta señal de alerta al principio nos hizo darnos cuenta que no éramos tan buenos, tuvimos que mejorar nuestra habilidad de mejorar nuestra seguridad cibernética, porque eso se convierte en una ventaja competitiva, y esa es la ventaja que tenemos.

Número dos, entablar un diálogo muy abierto con lo que estaba pasando desde el primer día, empezamos a publicar en Twitter qué es lo que estaba pasando y lo comunicamos a nuestras empresas, y esto fue muy importante porque dicha apertura, con esta experiencia que tuvimos, muchas otras empresas nos pueden ayudar y me parece que tuvimos un nivel bastante significativo, un gran aumento en la comprensión de este problema.

Debemos dejar de ser tan inocentes en lo que se refiere a la seguridad cibernética, el tamaño de una empresa no necesariamente ayuda, me parece que es algo muy importante.

La tercera y última conclusión que tengo… (Falla de Transmisión)… por lo tanto, la criticidad en la infraestructura se convierte en algo todavía más urgente y no podemos sobreponernos a estos factores de resiliencia.

Teniendo esto presente, el internet se inventó en 1989, no para el uso que tenemos en mente actualmente, sino que existe una necesidad de que se mejore radicalmente la infraestructura; hay que entender que debe haber más colaboración entre las empresas, las empresas de tecnología y las áreas de procuración de justicia, ojalá y esto no nada más afecte a nuestra empresa y no sea una lección para nosotros, sino para todos los que tengan algo que ver con tecnología, presumiría que son prácticamente todas las empresas en la actualidad.

Peilin Corbanese: (Interpretación de inglés a español) Tengo una pregunta para ustedes: ¿cuántos de ustedes, cuántas de sus empresas tienen datos en la nube? Levanten la mano.

¿Cuántos de ustedes acceden a los datos de la nube? Ustedes mismos.

Muchos de ustedes.

¿Cuántos de ustedes acceden a sus datos en la nube a través de un dispositivo móvil?

Miren esto. Entonces todo ahora es digital, la nube tiene mucha automatización… (Falla de Transmisión)… Las violaciones a la seguridad cibernética… (Falla de Transmisión)…Todos nuestros datos, todos nuestros dispositivos están en la nube.

Hay una historia que no se ha contado sobre esta empresa, se trata de una empresa de varios miles de millones que maneja tanto tráfico en el mundo por el mar, entonces si todos sus sistemas se caen, no pueden trabajar ningún contenedor, ninguna mercancía se entregaría en ningún país en el mundo.

Saben ustedes, entonces, ¿cómo se dio esta historia?

De acuerdo con CEO, era una empresa bastante promedio, tenían un seguro cibernético, tenían una buena red para asegurarse de atrapar a los *hackers*, pero ¿saben qué se les olvido? Se les olvido este pequeño detalle, una pequeña computadora que estaba en una tienda de regalos en Copenhague.

Entonces, resulta que esa pequeña computadora no la habían actualizado. En tecnología de la información siempre tenemos varias cosas en IT que tenemos que hacer, pero no tenemos el tiempo de hacerlas, esta es una de esas cosas.

Entonces, esta pequeña computadora fue como el hacker, envío este virus y así cerró el mundo y cerró a la empresa y la pérdida para ellos son 250 a 300 millones de dólares, ¿pero pueden imaginarse las veces y el costo para la economía? Eso da bastante miedo, eso es el número 1.

El número 2, si lo piensan bien es que lo segundo que menciona él es que tuvimos que ser transparentes, cuántas violaciones de datos conocemos que la empresa o la organización han tardado una semana en comunicarlo, se han tardado una semana o más tiempo en enterarse. Levanten la mano si ustedes creen que a lo mejor hubo una violación, una vulneración a sus sistemas y se enteraron ustedes de manera inmediata. Ven, nadie, ¿por qué? Porque casi todas las empresas deciden tratar de determinar cuál es la situación antes de informarle al público, pero eso significa que el daño puede ser incluso más severo y la comunicación son los consumidores no sería la mejor.

Entonces, voy a mostrarles ahora qué es lo que podemos hacer en términos de seguridad cibernética.

Obviamente esta es una gran amenaza y ustedes pueden ver que estos son los incidentes y su frecuencia, vean qué tan grandes son

los números, 5.5 miles de millones. Miren esto, 4.35 millones, ese el promedio de una violación cibernética en 2022, 5.5. millones, 5 mil 500 millones de dólares en malware, ese es el costo.

Y en el *ransenwert*, quiere decir que entonces el hacker lo que quiere es dinero a cambio de liberar los sistemas, eso es muchísimo dinero. Si lo piensan bien, imagínense en lo que va atravesar una empresa, esto da miedo, vean estas barras. Estas barras pertenecen a algunas de las organizaciones más grandes que ustedes conocen, por cuestiones de privacidad decidimos no compartir con ustedes los nombres, pero vean. Estas son plataformas de marketing digital, de servicios de internet, de servicios financieros y de servicios de consumo.

¿Cuánto cuesta una vulneración, una violación? Y vean aquí que la responsabilidad promedio potencial por registro es de 180 dólares por registro. Pensemos en datos, como pienso en datos he comprado seguridad cibernética y también hemos hecho pruebas cibernéticas a través de Google, para entender qué nivel de seguridad tiene cada quien, para poder comprar sistemas de seguridad cibernética.

Y hace algunos años, hace tres, cuatro años hicimos esto y en aquel momento la responsabilidad promedio por registro era de 180 dólares.

En el transcurso de algunos años esto ha subido y aquí yo haría algunas matemáticas y estudien en su cabeza. Supongamos que tienen 100 registro que están en la nube, y supongamos que cada registro ha sido vulnerado.

Entonces, imagínense que la mitad de ellos tienen problemas, ahora tienen que pagar a esas personas, a esos 50 registros que han sido vulnerados, cada registro vale 180 y hay que pagarlo para rectificar, para mitigar los riesgos.

Entonces, multipliquen eso y estoy seguro de que sus registros de los clientes no solamente son 100, probablemente ustedes tienen millones, varios millones de registros. Multipliquen ese número y van a ver cuál es su nivel de exposición.

Y esto, solamente es el costo de la mitigación y del riesgo, y esto no hace nada para mejorar la reputación de una empresa, porque la

reputación de su empresa se va ver dañada y no se trata, no es lo que queremos, no queremos asumir ese tipo de riesgo.

Vamos a definir qué es seguridad cibernética: Es la práctica de defender computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes y datos de ataques maliciosos. Hay tantas áreas diferentes, tantos aspectos diferentes a los que hay que prestar atención en el área de seguridad cibernética.

Por supuesto, está la seguridad de la red, tenemos que construir una barda para que nadie entre a nuestra red, y esa barda tiene que tener seguridad para las aplicaciones, porque cada aplicación puede convertirse en un problema.

Después tenemos la seguridad de la información, datos; ya hablamos de los datos, ¿qué va pasar con esos datos?

La información de identificación personal, tenemos la seguridad operativa y la recuperación ante un desastre.

¿Tienen ustedes un procedimiento para recuperarse ante un desastre? ¿Tienen redundancia? ¿Tienen su información en diferentes lugares, está en diferentes ubicaciones geográficas? Esta redundancia puede entrar a funcionar muy rápido, es cierto, ¿lo saben?

¿Alguno de ustedes tiene algún centro de operaciones con redundancia? Levanten la mano. No está mal, nada mal. Eso cuesta dinero, por supuesto.

Y, finalmente, está el costo de educación al usuario final. La verdad es que yo no he sido muy buena, porque muchas veces se me olvida, cuando estoy muy estresada cometo errores y violo también algunas de estas políticas que las empresas nos capacitan para no hacer.

¿Quién sería responsable de la seguridad cibernética? Todos. ¿Pero saben quién es el más importante? Estas personas, los CDO’s, los CIO’s, los ETO’s y los CISO’s, es decir, esos son los funcionarios de seguridad cibernética, el CFO.

Si no tenemos seguridad cibernética no podemos ganar dinero y después todos los demás, todos los que están aquí, todos tienen que saber qué deben hacer.

Aquí están los problemas principales y las prioridades principales de su cibernética, en número y aumento de delitos cibernéticos, 52 por ciento o más ahora; preocupaciones de privacidad para construir confianza con el consumidor. Cada vez que hay un tipo de vulneración, la confianza que el consumidor tiene en tú empresa se pierde, y esto le cuesta a la empresa muchos dólares en un futuro, el valor de la empresa se ve afectado.

Entonces, si continuamos viendo la lista, vamos a encontrar diferentes temas que tenemos que abordar.

Ahora, para los CICO's, la prioridad es proteger los activos críticos. Todas las computadoras, los dispositivos, los datos, los datos del consumidor, por ejemplo, y minimizar la disrupción, porque esto simplemente cuesta dinero a diestra y siniestra, ¿cómo vamos hacer esto entonces?

Aquí están los retos que tenemos. Las empresas aseguradoras son objetivos muy atractivos, porque todos nosotros tenemos mucha información personal de nuestros clientes: Datos de salud, datos de tráfico, información personal, datos de pagos, todo eso permitiría a un hacker recibir un cheque enorme.

Y, finalmente, tenemos muchos aumentos en nuestras exposiciones cibernéticas, porque cada vez hay más delitos en torno a estas áreas y estas vulneraciones van aumentando consistentemente todos los días, entonces, esto sucede en todas partes.

Si ustedes son como todos los demás, tienen muchos diferentes prestadores de servicios que trabajan para su empresa y también ustedes tienen diferentes sistemas, diferentes servidores, muchos sistemas operan de manera independiente; otros sistemas están conectados y ustedes tienen sistemas locales y sistemas en la nube, tienen muchos *pay blinders,* muchos procesos.

Entonces, ¿cómo se llevan a cabo estas cosas, cómo cada uno de los usuarios tiene acceso y cuánto acceso tienen a cada usuario a estos sistemas?

Ahora, la filtración de usuarios, seguramente hemos olvidado, a lo mejor decimos: Hoy es un día muy ocupado y resulta que le mando un correo electrónico y envío una documentación de la empresa a un correo personal de un empleado y lo olvidamos. Eso no lo tenemos que hacer y se nos olvida, porque somos seres humanos. Los seres humanos somos el principal problema en las amenazas cibernéticas.

Estos son los retos clave: El trabajar con todos los datos que tenemos y asegurar la privacidad, eso es muy difícil. Asimismo, también acelerar la transformación digital, porque cuanta más tecnología tenemos, más vamos a usarla y hay generativa, la IA generativa, que nos da recomendaciones, nos dice qué tenemos que hacer para un consumidor.

Y, después tenemos también un pico en las actividades de delitos cibernéticos y nuestro entorno cada vez es más complejo, hay muchos puntos de contacto, hay muchas puertas abiertas. De hecho, es un reto muy grande en la actualidad.

Sobre el gasto en Seguridad Cibernética en 2022, se destinaron 172 mil 500 millones de dólares. ¡Esta es una cantidad altísima!

Aquí todos somos gente de negocios, aquí podríamos ganar algo de dinero, podríamos crear algún Seguro Cibernético si supiéramos cómo calcular su precio para minimizar nuestros riesgos. ¡Piénsenlo!

Piensen en cuántas habilidades se requieren ahora, cuántas personas requerimos con habilidades cibernéticas; son muchas cuentas, preguntémonos entonces si tenemos suficiente personal que sepa hacer esto.

Este es el costo global estimado de delitos cibernéticos, el cual asciende a 6.1 trillones de dólares. No los quiero espantar, pero sí les quiero ofrecer opciones y soluciones.

En cuanto a ciberseguridad, ¿cuáles son las oportunidades que tenemos con Datos y la Inteligencia Artificial?

La Tecnología está avanzando y utilizamos todas estas cosas de manera diferente.

¿Entonces qué es lo que podemos hacer?

Podemos utilizar la Inteligencia Artificial y el ML para protegernos y entonces, por supuesto, tenemos que proteger los Datos Personales y ya existe una naturaleza en evolución para proteger los Datos y tenemos que ser capaces de utilizar Inteligencia Artificial para rastrear y monitorear los Datos porque esto siempre va a estar ahí todo el tiempo.

Entonces, cuando haya un cambio en los patrones, cuando haya alguna diferencia que un ser humano no pueda identificar, una máquina sí lo podrá hacer, sí podrá identificarlos.

Las máquinas son persistentes, pueden monitorear 24 horas al día, los 7 días de la semana y los 365 días del año las transacciones, lo cual es muy flexible.

Así, esta Tecnología, la Inteligencia Artificial Generativa, aprende y la podemos utilizar; podemos utilizar esta Tecnología para hacer un mejor trabajo y protegernos de mejor manera.

Entonces, aquí tenemos -por ejemplo- las diferentes cosas que la IA y el aprendizaje por máquinas puede hacer como puede ser la gestión y clasificación de datos para saber cuáles se almacenan y cuáles no, pero también podemos saber cómo filtrar el spam para poder detectar con antelación un hacker, antes de que sea demasiado tarde.

Entonces, estas son las diferentes cosas que podemos hacer y con todo gusto puedo hablar con ustedes, a nivel personal, más adelante.

Por último, me parece que es muy importante que cada empresa valore su propia exposición a las amenazas cibernéticas; deben tener gestión de vulnerabilidades, tienen que conocer cuáles son sus puntos vulnerables y reforzar estas vulnerabilidades para bloquear muy bien esas opciones de delitos cibernéticos y evitar con ello que los hackers entren a sus sistemas, ya sea a través de aplicaciones, de sistemas de capacitación o educación de usuarios.

Para ello tenemos aquí sistemas de detección de malware pues debemos tener comunidades seguras ya que ninguna comunicación puede salir a través de canales que no sean oficiales.

Por supuesto, en torno a esto está la sensibilización a través de una capacitación a usuarios; es decir, necesitamos hacer esto con mucha seriedad porque yo sé que personalmente -yo, por ejemplo- simplemente digo “estoy muy ocupada, estoy demasiado ocupada” y entonces, no tengo tiempo de tomar una capacitación.

En consecuencia, a veces tomo la capacitación mientras estoy haciendo muchas otras cosas al mismo tiempo y hay que prestar mucha atención cuando tomemos una capacitación. Ese es un punto muy importante.

Ahora bien, está el enfoque de seguridad de punto a punto, es algo que tiene que suceder.

Debemos tener una arquitectura cibernética y aplicaciones de negocios, debemos entender cómo es y me parece que muchos de nosotros quizá no sabemos en dónde están nuestros sistemas, no sabemos qué datos están en qué sistemas.

Entonces, tenemos que empezar a hacer un mapeo de esto, para saber en dónde están nuestros sistemas, cuáles son los tipos de datos que tenemos, qué clasificación tienen.

Es decir, tenemos que catalogar estos datos y simplemente hay que colocarlos de manera correcta y en el lugar correcto, para exponer únicamente los datos que vale la pena exponer en la nube.

También debemos tener una gestión de nuestro sistema. Es decir, hay diferentes tipos de aplicaciones que podemos usar para este propósito ya q1ue hay diferentes sistemas de seguridad cibernética y por supuesto, tiene que haber gobierno y control.

Muy a menudo veo que simplemente falta esta pieza y hay gente que cree que con contratar un Seguro Cibernético es suficiente, se da una capacitación y de repente, tenemos un gran proyecto, llega el SISO y nos dice “no, esto no se puede hacer, necesitamos verificaciones”, pero necesitamos una revisión y un control continuo, a nivel de Gobierno Corporativo, porque los delitos, los delincuentes cibernéticos están muy a la vanguardia, están más a la vanguardia que nosotros.

Entonces, por supuesto, necesitamos capacitación continua, monitoreo, mantenimiento, todo lo cual parece ser algo muy sencillo pero no lo es ya que no le estamos dedicando el tiempo a estas actividades.

Muchas veces, simplemente priorizamos el ganar dinero y la seguridad cibernética la ponemos en segundo lugar; bueno, pues yo vengo aquí a decirles que si no protegemos nuestros datos, que si los datos fueran vulnerados, ese daño afectará la relación con nuestro usuario final y eso no lo podremos recuperar, eso es incuantificable.

Entonces, hay dos cosas que les quiero decir en cuanto a los riesgos de seguridad cibernética:

Primero que nada, tienen que tener un Seguro adecuado para seguridad cibernética y esta es un área muy difícil porque tienes que conocer su nivel de exposición, necesitas conocer en qué áreas eres vulnerable y tienes que decidir cuánta inversión vas a poner y en donde, para así cerrar estas brechas. Este es el punto número 1.

Necesitamos un Seguro que sea suficiente -en cuestiones de Seguridad Cibernética- y después requerimos valorar nuestras vulnerabilidades.

En segundo lugar, sobre los que están en las Aseguradoras, piensen en cómo ofrecer un nuevo producto ya que todo mundo lo necesita ahora y es entonces cuando va a haber una demanda en aumento en el mercado. Esto seguramente va a continuar en los siguientes años.

Piensen en cómo podrían beneficiarse de esto pero primero, protejan su propio riesgo, su propia exposición ante los siniestros que se habrán de presentar en un futuro.

Las organizaciones líderes apalancarán sus capacidades internas fuertes y los ecosistemas de sus socios, porque finalmente los riesgos están evolucionando constantemente y es que tienen que revisar quién es quién, quiénes son sus socios, cuáles son los sistemas que utilizan para defender sus datos o ecosistemas.

Pero además, asegúrense de contar con la gente correcta para ayudarles porque internamente no va a ser suficiente; necesitan

tener un ecosistema de colaboración y la velocidad de la evolución hace que esta sea una prioridad estratégica.

Yo sé que están aquí porque saben que esto es importante, por eso les doy las gracias por estar aquí y traten de ver si pueden encontrar una solución para apalancar la Inteligencia Artificial y el aprendizaje por máquinas para que estén protegidos todos los días del año, todas las horas del día, todos los días de la semana.

Por último, quiero decirles que XL es una empresa global, una empresa que alcanzará los mil 700 millones de dólares este año; somos 48 mil empleados en todo el mundo y ahora mismo, en México, estamos contratando ya que tenemos dos posiciones abiertas: Alguien que conozca sobre Seguros y que conozca cómo hacer código, python y SQL.

Nos encantaría hablar con ustedes porque el señor que está sentado por acá, mi compañero de negocios, me acaba de decir que necesitamos invertir ciertos dólares para estar hablando aquí como expertos, con ustedes.

Pero si nosotros logramos reclutar aquí a estas dos personas que necesitamos en México, esta inversión valdrá la pena.

Entonces, si no quieren hablar con EXL sobre Seguridad Cibernética o nada de lo que hacemos, porque hacemos trabajo analítico tenemos 530 clientes en todo el mundo, no tenemos que hablar de eso. Acérquense y soliciten el trabajo.

Muchísimas gracias, espero que hayan disfrutado esta sesión.

¿Quieren hacer alguna pregunta o está todo bien?

(No Hay Preguntas)

Bueno, pues buen día.

Presentador: Bueno, nos hemos ganado un par de minutitos en el reloj, vamos a hacer un receso y nuevamente, si nadie más tiene alguna pregunta, daríamos por concluida esta primera mitad.

Hacemos un receso y regresamos a nuestra tercera reunión que es a las 11:50 en punto, cuando estaremos por acá.

Muchas gracias.

- - -o0o- - -