Infosecurity Mexico finaliza reconociendo la importancia de aplicar leyes de ciberseguridad y fortalecer capital humano especializado

• *Dos días de talleres, exposiciones y conferencias culminaron con 78% en incremento de visitantes en comparación con la edición anterior y más de 150 citas de negocio.*

CDMX, 9 de octubre, 2023.- Infosecurity Mexico 2023 llega al final de su séptima edición con 61 conferencistas, 54 sesiones, 65 marcas expositoras, un crecimiento de 78% en visitantes comparado con la edición 2022 y generando más de 17 millones de dólares en potencial de negocios.

Durante el segundo día de actividades se abordaron temas cruciales relacionados con la ciberseguridad y la seguridad de la información, así como el papel esencial de la regulación y el capital humano experto en este campo. Además, se exploraron las tendencias de digitalización e Inteligencia Artificial en un contexto de amenazas y riesgos que demandan atención tanto por parte de expertos como de la legislación vigente.

En el panel *Regulación Mexicana en Materia de Ciberseguridad*, las expertas Ivonne Muñoz, de IT Lawyers; Erika Mata, ejecutiva y conferencista internacional; y Gabriela Reynaga, CEO de Holistics GRC subrayaron la existencia de regulaciones fragmentadas en materia de ciberseguridad en México. Instaron por la unificación y fortalecimiento de las normativas e hicieron eco de una falta de personal especializado para comprender y aplicar estas regulaciones de manera efectiva. Asimismo, ilustraron la complejidad de la regulación en el sector financiero, donde la Ley Fintech presenta múltiples retos y enfatizaron la importancia de adaptar la regulación a la realidad del país y a los modelos de negocio específicos, así como de involucrar a todas las partes interesadas en el proceso.

Carlos Chalico, líder de Ciberseguridad y Privacidad en EY, compartió tendencias globales en ciberseguridad, destacando que el uso indiscriminado de nuevas tecnologías puede crear vulnerabilidades inadvertidas: “Solamente uno de cada cinco CISOs (Chief Information Security Officer) considera efectiva su función de ciberseguridad. Los ataques van en aumento en volumen y complejidad; el 75% de ellos opina que ha habido un incremento en ataques en los últimos cinco años, y el 76% dice que tardan seis meses o más en detectar y responder a un ataque”.

Se enfatizó la importancia de una estrategia de ciberseguridad que considere la simplificación y se mencionaron tecnologías de alto riesgo, como la nube, el Internet de las cosas y la Inteligencia Artificial.

Chalico también señaló que los principales desafíos en la integración de la ciberseguridad incluyen presupuestos insuficientes, falta de comunicación entre el CISOs y otros líderes de la Alta Dirección, y la falta de seguimiento de las mejores prácticas en áreas fuera de TI. “Las organizaciones requieren trabajar en la adopción de mecanismos de control por diseño, centrándose en la gente y en la facilidad operativa de uso”.

La conferencia final del evento, titulada C*rowdsourcing Government Flight Tracking with Social Media*, fue presentada por el especialista en aviación estadounidense Andrew Logan. En esta

charla, se abordaron los cambios en la seguridad aérea tras los eventos del 11 de septiembre de 2001 y cómo se monitorean las aeronaves en Nueva York.

“Infosecurity Mexico 2023 terminó, pero ya estamos trabajando en la edición del siguiente año donde se anticipa una mayor demanda de soluciones tecnológicas para abordar el desarrollo de la Inteligencia Artificial” concluyó Luis Zúñiga, director del evento.

# # #

Acerca de RX (Reed Exhibitions)
RX está en el negocio de construir negocios para individuos, comunidades y organizaciones. Elevamos el poder de los eventos cara a cara combinando datos y productos digitales para ayudar a los clientes a conocer los mercados, obtener productos y completar transacciones en más de 400 eventos en 22 países, en 42 industrias.
En RX nos apasiona generar un impacto positivo en la sociedad y estamos totalmente comprometidos con la creación de un entorno de trabajo inclusivo para toda nuestra gente. RX es parte de RELX, proveedor global de información basada en análisis y herramientas de decisión para clientes profesionales y de negocios. www.rxglobal.com

Acerca de RELX
RELX es un proveedor global de analítica basada en información y herramientas de decisión para clientes profesionales y de negocio. RELX sirve a clientes en más de 180 países y tiene oficinas en alrededor de 40 países. Emplea a más de 35,000 personas, de las cuales, cerca del 40% se encuentran en Norteamérica. Las acciones de RELX PLC, la empresa matriz, son negociadas en las bolsas de valores de Londres, Ámsterdam y Nueva York Stock Exchanges, utilizando los símbolos: Londres: REL; Ámsterdam: REN; Nueva York: RELX.
*Nota: La actual capitalización de mercado se puede encontrar en: http://www.relx.com/investors

Para mayor información: Jorge Morales García / Agencia Communika
T: +52 55 1795 2790
E: jorgem@communika.com.mx

Infosecurity 2023 abre el mes de la ciberseguridad e IA en el país

- *Además de pensar en riesgos hay que generar valor a través de la ciberseguridad, señalaron expertos durante el encuentro anual más importante en la materia en México*

CDMX, 5 de octubre, 2023.- Infosecurity Mexico abrió sus puertas este miércoles de la mano de expertos, empresarios y asociaciones "El mercado de la ciberseguridad crece en México, ya somos una gran familia que se ocupa de aquello que tiene que ver con vulnerabilidades, costos para las empresas y nuevas tecnologías, entre otros elementos, como la Inteligencia Artificial", señaló Luis Zúñiga, director del evento.

La apertura encabezada por Luis Bellini, Director General de RX México, compañía organizadora del evento, tuvo como invitados especiales a la Embajadora de Israel en México, Einat Kranz Neiger; al inspector en jefe Jorge Jesús Borrego Álvarez, titular de la Dirección Científica de la Guardia Nacional; Ignacio Sotelo, presidente de AMECI; Rubén Quintero, presidente de ISACA Ciudad de México; Jorge Osorio Bretón, presidente de la ISC2 Capítulo CDMX, y Levi Reza, EC Council, cortaron el listón inaugural y dieron la bienvenida a los expositores y visitantes que se estarán dando cita en el Centro Citibanamex.

En su intervención, la diplomática israelí, Einat Kranz, subrayó la cercanía e histórica buena relación entre las dos naciones, e Infosecurity Mexico fue el pretexto para fortalecer esos lazos de amistad entre Israel y México, e intercambiar el conocimiento necesario en temas como la ciberseguridad.

En este espacio, donde se dan a conocer el panorama de la ciberseguridad en México e innovaciones en la materia, también se dieron cita expertos que compartieron soluciones, desarrollos, talleres y buenas prácticas que han contribuido a que las pérdidas que ocasionan los ciberataques cada vez sean menores, que sean controlables y buscan impulsar que las empresas sean resilientes ante la carrera entre vulnerabilidades y la protección de la información. La ciberseguridad debe proponer, además de minimizar los riesgos y la protección per se, crear valor a la empresa, coincidieron en señalar los expertos durante el primer día del Summit 2023.

Por su parte, Óscar Montes, gerente de AdvanceNT México, planteó que la realidad de las organizaciones es considerar que la digitalización y la tecnología habilitan nuevos modelos comerciales y accesos a servicios para lograr la transformación acelerada, aunque también aumenta los riesgos por la realización de consumo masivo de servicios en línea, entornos descentralizados cada vez más complejos y un mayor uso de API's.

Las empresas quieren protegerse, buscan soluciones para cuidar su información y operación, pero no quieren que se interfiera en sus negocios, explicó Montes. Y agregó que la competencia es grande y no se salvan ni los más avanzados, "¿quién pensaría que Microsoft fue atacado?, pues lo ha sido y se le ha dado en su mayor fortaleza, en la disponibilidad de sus servicios. Invaden su tráfico HTTPS capa 7, entran y provocan tráfico evasivo y dinámico en segundos. Ya atacaron así a la monarquía inglesa y a Netflix".

Entre los especialistas que se presentaron en el primer día, figuró Jaime Restrepo Gómez, fundador de DragonJAR SAS, quien explicó y detalló sobre el uso de la inteligencia artificial a

través de ChatGPT. El desarrollador, de origen colombiano, mostró cómo conducir y las limitantes de búsqueda y respuestas de esta popular herramienta de IA.

Restrepo habló sobre la demanda creciente de CISO's (Chief Information Security Officer), quienes se encargan de proteger y mantener la seguridad de los datos ante posibles ciberataques o robo de los mismos. Se trata de expertos que, con herramientas de IA, captan miles de datos a diario y deben proponer la creación de equipos de seguridad de la información, desarrollo e implementación de estrategias, gestión de incidentes de seguridad, así como evaluación y mejora continua, entre otros dominios.

Los asistentes al primer día de Infosecurity Summit 2023 participaron en talleres de desarrollo con las herramientas más innovadoras y utilizadas a escala global, como el impartido por Enrique Herrera, de Cyberimox, quien mostró como se pueden rastrear metadatos descuidados por los usuarios que suben materiales a internet sin borrarlos, o empresas que se encuentran vulnerables en el ciberespacio frente a buscadores que trabajan sobre objetivos claros y puntuales, lo que les permite llegar a sus objetivos a través de caminos directos.

La recomendación fue clara, por parte de Herrera: Todo se puede encontrar si se deja huella, por eso "antes de subir algo a internet o a la nube hay que tomarse el tiempo de eliminar los metadatos", como política de ciberseguridad en toda empresa y de todo usuario.

Infosecurity Mexico abre el mes de la concienciación sobre la ciberseguridad en México, el evento continuará mostrando soluciones y servicios especializados para diseñar estrategias robustas que permitan proteger de mejor manera los activos informáticos de las organizaciones durante este jueves.

# # #

Acerca de RX (Reed Exhibitions)
RX está en el negocio de construir negocios para individuos, comunidades y organizaciones. Elevamos el poder de los eventos cara a cara combinando datos y productos digitales para ayudar a los clientes a conocer los mercados, obtener productos y completar transacciones en más de 400 eventos en 22 países, en 42 industrias.
En RX nos apasiona generar un impacto positivo en la sociedad y estamos totalmente comprometidos con la creación de un entorno de trabajo inclusivo para toda nuestra gente. RX es parte de RELX, proveedor global de información basada en análisis y herramientas de decisión para clientes profesionales y de negocios. www.rxglobal.com

Acerca de RELX
RELX es un proveedor global de analítica basada en información y herramientas de decisión para clientes profesionales y de negocio. RELX sirve a clientes en más de 180 países y tiene oficinas en alrededor de 40 países. Emplea a más de 35,000 personas, de las cuales, cerca del 40% se encuentran en Norteamérica. Las acciones de RELX PLC, la empresa matriz, son negociadas en las bolsas de valores de Londres, Ámsterdam y Nueva York Stock Exchanges, utilizando los símbolos: Londres: REL; Ámsterdam: REN; Nueva York: RELX.
*Nota: La actual capitalización de mercado se puede encontrar en: http://www.relx.com/investors

Para mayor información: Jorge Morales García / Agencia Communika
T: +52 55 1795 2790
E: jorgem@communika.com.mx

Especialistas en ciberseguridad listos para participar en Infosecurity Mexico

- *Llaman a prepararse contra cibercarteles y atender los próximos procesos electorales*

CDMX, a 13 de septiembre de 2023.- Infosecurity México, evento especializado en el sector de la ciberseguridad y seguridad de la información, con acceso a tendencias, conferencias y talleres y demostraciones conducidas por expertos, organizó una conferencia de prensa para presentar los temas y actividades que se llevarán a cabo el 4 y 5 de octubre en el Centro Citibanamex de la CDMX, con el apoyo de representantes de asociaciones especializadas.

Luis Zúñiga, Director de Infosecurity Mexico, explicó que este evento se ha consolidado como el "hub" de soluciones relacionadas con los temas de riesgos, de la seguridad de la información y de la prevención. "Además, contamos con un programa académico muy robusto en el que habrá casi 50 conferencistas que mostrarán innovaciones, tendencias en seguridad de la información, en protección de datos y ciberseguridad".

Igualmente, citó a Kevin Mitnick, ciberdelincuente reformado y convertido en consultor de seguridad informática con reconocimiento mundial, quien decía: "Las empresas pueden invertir cientos de miles de dólares para protegerse, pero los usuarios deben saber que uno de ellos puede ser la entrada para un ataque de ciberseguridad. Todos los entornos pueden ser afectados y hay que hacer conciencia en los empleados para que no se descuiden y estar alertas siempre".

Para entender mejor nuestro entorno, los expertos presentes señalaron que durante el año 2022 se registraron 180,000 millones de intentos de ataques cibernéticos en México, lo que se traduce en más de 3.5 millones de intentos de ataques a la semana. Por citar otro dato de relevancia, la Condusef ha informado que estima daños económicos de entre 14,000 y 17,000 millones de pesos al año por fraudes cibernéticos.

En ese sentido, Roberto Hernández, Presidente de ISACA Capítulo México, anunció que su asociación va a organizar el IV Congreso en Iberoamérica, que se titula "Confianza Digital para Gestionar los riesgos de la IA y tecnologías emergentes", como parte de la programación de Infosecurity Mexico, en donde abordarán temas relacionados con la Inteligencia Artificial enfocada a aspectos de continuidad y privacidad.

"Sabemos que el uso de la IA seguirá creciendo y aplicándose en prácticamente todas las industrias, por lo que en nuestro país tenemos que prepararnos. México está ubicado en la posición 61 de 180 en cuanto a su avance en IA, por detrás de Chile, Brasil y Colombia, y por ello debemos seguir desarrollándonos y entender sus riesgos, como el posible desplazamiento laboral, la manipulación de la información y otros factores que nos pueden afectar como sociedad".

En su turno, Levi Reza, representante de EC Council, adelantó que durante Infosecurity Mexico va a organizar la competencia "Capture the flag, respuesta a incidentes", con el enfoque particular

de mostrar cómo se debe actuar en respuesta a un incidente, y en qué materias se debe capacitar a los encargados de la ciberseguridad en una organización.

“La idea con este concurso es simular un ataque y mostrar la evidencia para que cada participante la analice y confirme que solamente se puede resolver con investigación y análisis. Sabemos que hay un déficit de conocimiento, y que se necesita capacitación, y vamos a aprovechar el foro para contribuir a generarlo”, agregó Reza

Por su parte, Jorge Osorio, Presidente de IsC2 Capítulo México, comentó que durante su participación en el evento seguirán promoviendo certificaciones mundiales de ciberseguridad. “Tenemos un gran reto en materia de ciberseguridad debido en parte al déficit de profesionales en la materia, quienes deben elevar sus conocimientos y madurar, porque incluso el crimen organizado tiene una rama dedicada al hackeo de bancos y cajeros automático; es un cibercartel”.

“También debemos considerar que estamos a un año de las elecciones presidenciales, y tenemos que atender esta situación. Por eso consideramos que Infosecurity es el foro para que entendamos mejor los retos y unirnos como marcas, como profesionales y como asociaciones, reclutando a los nuevos profesionales antes de que los reclute la delincuencia”.

Por último, Enrique Herrera, consultor especializado en ciberseguridad, señaló que siete de cada diez organizaciones mexicanas han sufrido un ataque, “aunque muchos de ellos no se denuncian por temas de reputación, sobre todo porque el 59% de los ciberataques son a través del correo electrónico. México es el segundo país más atacado en Latinoamérica, después de Brasil, por lo que debemos aumentar nuestras defensas y entender que debemos elevar el nivel”.

Como parte de su presentación, Herrera demostró en tiempo real la forma en la que los ciberdelincuentes pueden suplantar la identidad de un correo electrónico, “eso demuestra que hay técnicos que no configuran correctamente un servidor SMTP (protocolo de red básico que permite que los emails viajen a través de internet), lo que provoca una alta vulnerabilidad”.

Infosecurity Mexico se inaugurará el próximo 4 de octubre, y en su piso de exhibición participarán más de 50 empresas que mostrarán soluciones para la prevención y la defensa. Además, facilitará espacios de networking y generará oportunidades de negocio para las compañías patrocinadoras, las expositoras y los visitantes, quienes, además, podrán aprovechar el programa académico en el que participarán especialistas nacionales e internacionales.

# # #

Acerca de RX (Reed Exhibitions)
RX está en el negocio de construir negocios para individuos, comunidades y organizaciones. Elevamos el poder de los eventos cara a cara combinando datos y productos digitales para ayudar a los clientes a conocer los mercados, obtener productos y completar transacciones en más de 400 eventos en 22 países, en 42 industrias.
En RX nos apasiona generar un impacto positivo en la sociedad y estamos totalmente comprometidos con la creación de un entorno de trabajo inclusivo para toda nuestra gente. RX es parte de RELX, proveedor global de información basada en análisis y herramientas de decisión para clientes profesionales y de negocios. www.rxglobal.com

Acerca de RELX
RELX es un proveedor global de analítica basada en información y herramientas de decisión para clientes profesionales y de negocio. RELX sirve a clientes en más de 180 países y tiene oficinas en alrededor de 40 países. Emplea a más de 35,000 personas, de las cuales, cerca del 40% se encuentran en Norteamérica. Las acciones de RELX PLC, la empresa matriz, son negociadas en las bolsas de valores de Londres, Ámsterdam y Nueva York Stock Exchanges, utilizando los símbolos: Londres: REL; Ámsterdam: REN; Nueva York: RELX.
*Nota: La actual capitalización de mercado se puede encontrar en: http://www.relx.com/investors

Para mayor información: Jorge Morales García / Agencia Communika
T: +52 55 1795 2790
E: jorgem@communika.com.mx

Mujeres especialistas en ciberseguridad, avanzan pese a brechas de género

Por staff de redacción Infosecurity Mexico

De acuerdo con un estudio elaborado por LinkedIn en 163 países[1], las mujeres representan el 41.9% de la fuerza laboral general. También se encontró que, en los últimos tres años, solo fue en el 2021 que la proporción de empleos ocupados por mujeres aumento 0.12 puntos porcentuales, en comparación con el 2022 que hubo una caída de 0.03 puntos y un descenso aún mas pronunciado en este 2023 de 0.31 puntos porcentuales.

Por otro lado, se halló que hay industrias en las que la representación de las mujeres ha tenido un aumento considerable desde 2016 (aunque disminuyó a principios de 2023). Estas industrias son el gobierno y sector público (+1,8 puntos porcentuales en 2022 en comparación con 2016), la infraestructura (+ 1,16 puntos porcentuales), servicios profesionales (+0,95 puntos porcentuales), y tecnología, información y medios (+0,94 puntos porcentuales).

Específicamente en el terreno de la tecnología se ha detectado que las mujeres ocuparon el 25% de los trabajos de seguridad cibernética a nivel mundial en 2022, frente al 20% en 2019, y alrededor del 10% en 2013[2]. Con base en tal tendencia, se pronostica que las mujeres representarán el 30% de la fuerza laboral de seguridad cibernética mundial para 2025, y que alcanzará el 35% para 2031.

En este sentido, cuando se habla de ciberseguridad, se debe especificar que las especialidades de referencia son la protección de las redes corporativas, la seguridad de IoT, IIoT e ICS, y ciberseguridad para aplicaciones médicas, automotrices, de aviación y militares, defensa, y otros. El detalle radica en que existe una gran brecha de género cuando se consideran los roles principales en ciberseguridad; por ejemplo, las mujeres ocupan solo el 17% de los puestos de directoras de seguridad de la información (CISO) en las empresas Fortune 500[3].

Sin embargo, hay que considerar que hay una escasez global de talento en ciberseguridad que contribuye a que las redes y los datos sigan en riesgo. Hay más de 3.4 millones de puestos de trabajo abiertos en el mundo, para hombres y mujeres, y el 70% los trabajadores de ciberseguridad sienten que sus organizaciones no tienen personal para defenderse eficazmente contra los ciberataques, según una investigación de (ISC)2 sobre la fuerza laboral de ciberseguridad del 2022[4].

Aunado a ello, se ha encontrado que, al contratar profesionales en ciberseguridad, muchas organizaciones han establecido altos estándares de contratación que impactan en la escasez de talento. A menudo enfatizan en habilidades específicas, o solicitan cinco o más años de experiencia para puestos de nivel inicial, en lugar de buscar personas que demuestren capacidad o habilidades que complementen las necesidades de ciberseguridad. Este es un obstáculo universal en toda la industria.

---

[1] https://n9.cl/7vyk2
[2] https://n9.cl/8i4f6
[3] https://n9.cl/qlui1
[4] https://n9.cl/z18fh

Este panorama está contribuyendo a un desequilibrio de género en la materia. El estudio sobre la fuerza laboral de ciberseguridad citado anteriormente reveló que las mujeres constituían una fracción de la población en ese campo. Las mujeres menores de 30 años representan el 30% de la fuerza laboral, pero esa cifra cae al 24% entre las edades de 30 y 38 años. La brecha es aún mayor entre las personas de 39 años o más.

Sin embargo, a pesar de las batallas libradas para alcanzar sus puestos, el estado general de la industria para las mujeres está mejorando[5]. Las mujeres parecen estar logrando mayores avances en ciberseguridad porque la industria depende de habilidades de colaboración y creación de redes, y estas son habilidades en las que las mujeres tienden a sobresalir.

Además, organizaciones como WiCyS, Executive Women's Forum, Minorities in Cybersecurity y Empow(H)er Cybersecurity buscan ayudar a las mujeres a sobrellevar el proceso de contratación y otras barreras, porque además de ello, se sabe que muchas personas trabajan en ciberseguridad por casualidad y no debido a que hayan estudiado ciencias de la computación o tecnología de la información: en la comunidad de la ciberseguridad siempre hay alguien dispuesto a ayudar a quien quiere aprender.

La próxima cita para las mujeres especialistas en ciberseguridad será en la próxima edición de Infosecurity Mexico, en donde participarán activamente representantes femeninas en talleres y conferencias, y además estarán dispuestas a ayudar e intercambiar conocimiento. Hay que escucharlas.

# # #

Acerca de Infosecurity Mexico
Es el evento más importante del sector de ciberseguridad y seguridad de la información en el que se ofrece acceso a tendencias, conferencias y workshops de la mano de expertos.

Acerca de RX (Reed Exhibitions)

RX está en el negocio de construir negocios para individuos, comunidades y organizaciones. Elevamos el poder de los eventos cara a cara combinando datos y productos digitales para ayudar a los clientes a conocer los mercados, obtener productos y completar transacciones en más de 400 eventos en 22 países, en 42 industrias. En RX nos apasiona generar un impacto positivo en la sociedad y estamos totalmente comprometidos con la creación de un entorno de trabajo inclusivo para toda nuestra gente. RX es parte de RELX, proveedor global de información basada en análisis y herramientas de decisión para clientes profesionales y de negocios. www.rxglobal.com

Acerca de RELX

RELX es un proveedor global de analítica basada en información y herramientas de decisión para clientes profesionales y de negocio. RELX sirve a clientes en más de 180 países y tiene oficinas en alrededor de 40 países. Emplea a más de 35,000 personas, de las cuales, cerca del 40% se encuentran en Norteamérica. Las acciones de RELX PLC, la empresa matriz, son negociadas en las bolsas de

[5] https://n9.cl/z18fh

valores de Londres, Ámsterdam y Nueva York Stock Exchanges, utilizando los símbolos: Londres: REL; Ámsterdam: REN; Nueva York: RELX.

*Nota: La actual capitalización de mercado se puede encontrar en: http://www.relx.com/investors

Para mayor información:
Jorge Morales García
Agencia Communika
T: +52 55 1795 2790
E: jorgem@communika.com.mx

Ciberdelincuencia: un costo anual superior a los diez billones de dólares para la economía mundial

Por staff de redacción Infosecurity Mexico

En el mundo actual, el cibercrimen representa una carga económica que supera los diez millones de dólares anuales, un fenómeno que demanda atención constante y estratégica. EL creciente números de datos almacenados a nivel global, estimado en más de doscientos zettabytes[6]para el 2025, plantea un desafío monumental en términos de seguridad cibernética. Estos datos incluyen información alojada en infraestructuras de TI públicas y privadas, en servicios públicos, centros de datos en la nube, en dispositivos informáticos personales como PC, portátiles, tabletas y teléfonos inteligentes, además de su aplicación en el Internet de las Cosas (IoT).

Actualmente, cerca de 5 mil millones de personas acceden y almacenan datos en dispositivos digitales y en la nube. Se estima que, para el año 2029, el noventa por ciento de la población mundial, es decir, siete mil quinientos millones de personas, estará en línea y generará datos. En 2020, ya había tres mil quinientos millones de usuarios de teléfonos inteligentes que utilizaban internet. Este crecimiento se acelerará con la tecnología 5G, esperando que alcance los dos mil seiscientos millones de suscriptores para el 2025.

Este ascenso vertiginoso en el uso y almacenamiento de datos conlleva riesgos significativos en materia de ciberseguridad. Los ciberataques pueden perturbar, dañar e incluso destruir empresas por ataques a su infraestructura de TI. Simplemente, el costo medio de una filtración de datos es superior a los 4 millones de dólares[7]; el precio incluye descubrir y responder a la infracción, el tiempo de inactividad, la pérdida de ingresos y el daño a la reputación de la empresa y marca.

Una encuesta[8] revela que casi el treinta y uno por ciento de cuatro mil trecientos treinta y dos líderes empresariales a nivel global consideran la ciberseguridad como una de las principales prioridades de inversión para sus organizaciones en el 2023, superando a la gestión de datos, análisis de datos (25%), IA y ML[9] (20%), por citar algunos.

Algunos ciberataques pueden ser aún más costosos. Los ataques de ransomware han exigido rescates de hasta 40 millones de dólares[10], y los ataques al correo electrónico empresarial (BEC) han costado hasta 47 millones de dólares a las víctimas en una sola sesión[11].

Los daños no se limitan a pérdidas financieras, ya que los ataques que comprometen la información de identificación personal (PII) de los clientes pueden resultar en la pérdida de confianza de los clientes, sanciones regulatorias y acciones legales. Se estima[12], que el cibercrimen costará a la economía mundial 10.5 billones de dólares al año desde 2022 hasta 2025.

---

[6] https://n9.cl/abjux
[7] https://n9.cl/cqgw9
[8] https://n9.cl/6940d
[9] Inteligencia Artificial y “Machine Learning”
[10] https://n9.cl/qh5qv
[11] https://n9.cl/ct4it
[12] https://n9.cl/izvnr

Para mitigar estos riesgos, los expertos en seguridad de la información recomiendan las siguientes medidas:

1. Cifrar los datos: cualquier dato que pueda causar daño financiero o a la reputación de una organización, si fuera expuesto o manipulado, debe cifrarse. Esto significa convertir un archivo de texto legible en un texto incomprensible, es decir, cifrado; implica modificar datos legibles de forma aleatoria. Requiere una clave criptográfica y un conjunto de valores matemáticos acordados por el emisor y el destinatario.
2. Realizar una copia de seguridad y recuperación: la mayoría de los ciberintrusos pasan desapercibidos durante lapsos prolongados, por ello las organizaciones deben realizar copias de seguridad de manera que les permitan restaurar los datos a su estado original antes de un ataque, sea que tengan sus datos en la nube, en un centro de datos o en otros dispositivos.
3. Establecer una política transparente: las organizaciones no sólo deben cumplir con leyes como la LFPDPPP o la LGPDPPSO[13], sino que tienen que transmitirlo de manera proactiva a los consumidores y usuarios, que cada vez conocen más acerca de cómo se almacenan y administran sus datos. Por ello las organizaciones deben demostrar abiertamente su compromiso.
4. Contemplar una póliza de seguro: el ransomware podría estar cubierto por pólizas de ciberseguro, que normalmente reembolsan los daños por pérdida de datos, incluso si una organización es (involuntariamente) negligente o imperfecta en sus prácticas de respaldo. Desde luego, cada institución aseguradora solicita requisitos diferentes, y habría que evaluarlos.
5. Contratar expertos: se debe contar con especialistas disponibles contractualmente en todo momento (ya sea que pertenezcan a la propia planta laboral, contratistas o a través de proveedores), con una profunda experiencia en la materia en todos los aspectos de la seguridad de los datos (legal, técnico, operativo y de recuperación ante desastres).

La ciberseguridad es esencial tanto en la nube como en los dispositivos personales, ya que un pequeño descuido puede tener consecuencias graves para una organización. Consultar con expertos, como los que se presentarán en Infosecurity Mexico, es una oportunidad única para conocer las últimas tendencias y mejores prácticas de protección.

# # #

Acerca de Infosecurity Mexico
Es el evento más importante del sector de ciberseguridad y seguridad de la información en el que se ofrece acceso a tendencias, conferencias y workshops de la mano de expertos.

Acerca de RX (Reed Exhibitions)

RX está en el negocio de construir negocios para individuos, comunidades y organizaciones. Elevamos el poder de los eventos cara a cara combinando datos y productos digitales para ayudar a los clientes a conocer los mercados, obtener productos y completar transacciones en más de 400 eventos en 22 países, en 42 industrias. En RX nos apasiona generar un impacto positivo en la sociedad y estamos totalmente comprometidos con la creación de un entorno de trabajo inclusivo para toda nuestra gente. RX es parte de RELX, proveedor global de información basada en análisis y herramientas de decisión para clientes profesionales y de negocios. www.rxglobal.com

[13] https://n9.cl/p7qul

Acerca de RELX

RELX es un proveedor global de analítica basada en información y herramientas de decisión para clientes profesionales y de negocio. RELX sirve a clientes en más de 180 países y tiene oficinas en alrededor de 40 países. Emplea a más de 35,000 personas, de las cuales, cerca del 40% se encuentran en Norteamérica. Las acciones de RELX PLC, la empresa matriz, son negociadas en las bolsas de valores de Londres, Ámsterdam y Nueva York Stock Exchanges, utilizando los símbolos: Londres: REL; Ámsterdam: REN; Nueva York: RELX.

*Nota: La actual capitalización de mercado se puede encontrar en: http://www.relx.com/investors

Para mayor información:
Jorge Morales García
Agencia Communika
T: +52 55 1795 2790
E: jorgem@communika.com.mx

Preocupante la brecha de talento en ciberseguridad, ¿ya se está corrigiendo?

Por staff de redacción Infosecurity Mexico

Generalmente, cuando se habla de ciberseguridad, pensamos en la protección de los activos informáticos contra delitos que afectan a grandes corporativos, empresas de todos los tamaños, instituciones educativas y oficiales y, desde luego, a los usuarios comunes que cada día interactuamos con los dispositivos electrónicos que tenemos a la mano. Por ello, se podría definir la misión de la ciberseguridad como algo que suena muy simple: proteger a la sociedad.

Sin embargo, la magnitud de los daños que pueden causar los ciberdelincuentes que cometen delitos simples, como intentar acceder a nuestros teléfonos celulares para extraer nuestra información, hasta delitos más sofisticados como bloquear servicios públicos o instalaciones críticas, vulnerar sistemas de votación o cometer fraudes bancarios.

Por eso, un país debe diseñar políticas de educación y promoción del talento de profesionales dedicados a la ciberseguridad, ya que son ellos quienes se encargan de mantener en funcionamiento los engranajes con los cuales funciona nuestra sociedad. El problema es que a medida que avanza la tecnología, aumenta el volumen de amenazas, y no hay suficientes profesionales que puedan encargarse de detenerlas. De hecho, según ISC[2] hay una brecha de talento mundial de 3,4 millones de especialistas en la materia[14].

Ante el aumento de los riesgos, hay quien afirma que prácticamente cada puesto de TI, en cualquier especialidad, debe asumir que también está ocupando un lugar como responsable de la seguridad, porque cada trabajador de tecnología debe participar en la protección y defensa de las aplicaciones, datos, dispositivos, infraestructura y hasta de las demás personas.

Según estimaciones de especialistas que coinciden con la cifra estimada por ISC[2], para que nos demos una idea del número de especialistas faltantes, la cantidad es suficiente para llenar poco más de 50 estadios de la NFL. ¿Qué tan alarmante es esta cifra? Bueno, en el 2014 se calculaba el déficit en un millón de vacantes[15].

Viéndolo desde otra perspectiva, la tasa de desempleo de ciberseguridad para trabajadores experimentados del 0%, aunque no para puestos de entrada, y así ha permanecido desde el 2011, pero al ritmo que está creciendo la ciberdelincuencia, el número de puestos vacantes podría crecer.

Por cierto, cabe señalar que existen previsiones de que las mujeres atenderá el 30% de los puestos de ciberseguridad a nivel global para el 2025, y el 35% en el 2031. Recién en el 2022 y 2019 ocuparon el 25 y 20 % respectivamente, y en el 2013 fue del 10%. Por otro lado, solo el 17% de las mujeres son directoras de seguridad de la información.

Ahora bien, cuando se habla de ciberseguridad a estos niveles, no solo se trata de la protección de las redes corporativas, sino que incluye la seguridad del Internet de las Cosas, Internet Industrial de las Cosas y de los Sistemas de Control Industrial, además del resguardo de una

[14] https://n9.cl/o49o4
[15] https://n9.cl/aliu13

amplia gama de aplicaciones, que incluye las médicas, de oficina, automotrices y hasta militares.

De acuerdo con una encuesta a 1,000 profesionales de ciberseguridad de nueve países, que cita el Foro Económico Mundial[16], el 85% de los entrevistados cree que la escasez de mano de obra especializada afecta la capacidad de su organización para proteger sus redes. Igualmente, un centro de investigación[17] descubrió que el costo promedio de una violación de datos en 2022 fue de $4,35 millones USD. La demanda de talento en ciberseguridad, capaz de reducir las infracciones y sus costos, enfrenta una crisis global que afecta a los sectores público y privado.

El reto no es menor, pero se puede atender. Hay iniciativas que promueven que la ciberseguridad debe integrarse en los planes de educación primaria y a partir de ahí, estimular el estudio en niveles medios y superiores, incluso con becas. Igualmente, estimular a los alumnos de estudios superiores a integrarse al mundo corporativo aun en su etapa académica, y ya en el campo de trabajo diseñar estrategias que posibiliten la actualización y la retención de talento.

Por eso, vale la pena participar en foros como Infosecurity Mexico, en donde se presentan este tipo de temas y se proponen soluciones, además de que se comparten experiencias y buenas prácticas. Hay que considerarlo.

# # #

Acerca de Infosecurity Mexico
Es el evento más importante del sector de ciberseguridad y seguridad de la información en el que se ofrece acceso a tendencias, conferencias y workshops de la mano de expertos.

Acerca de RX (Reed Exhibitions)
RX está en el negocio de construir negocios para individuos, comunidades y organizaciones. Elevamos el poder de los eventos cara a cara combinando datos y productos digitales para ayudar a los clientes a conocer los mercados, obtener productos y completar transacciones en más de 400 eventos en 22 países, en 42 industrias.
En RX nos apasiona generar un impacto positivo en la sociedad y estamos totalmente comprometidos con la creación de un entorno de trabajo inclusivo para toda nuestra gente. RX es parte de RELX, proveedor global de información basada en análisis y herramientas de decisión para clientes profesionales y de negocios. www.rxglobal.com

Acerca de RELX
RELX es un proveedor global de analítica basada en información y herramientas de decisión para clientes profesionales y de negocio. RELX sirve a clientes en más de 180 países y tiene oficinas en alrededor de 40 países. Emplea a más de 35,000 personas, de las cuales, cerca del 40% se encuentran en Norteamérica. Las acciones de RELX PLC, la empresa matriz, son negociadas en las bolsas de valores de Londres, Ámsterdam y Nueva York Stock Exchanges, utilizando los símbolos: Londres: REL; Ámsterdam: REN; Nueva York: RELX. La capitalización de mercado es de aproximadamente £ 33 mil millones, € 39 mil millones, $ 47 mil millones*.
*Nota: La actual capitalización de mercado se puede encontrar en: http://www.relx.com/investors

Para mayor información:
Jorge Morales García
Agencia Communika
T: +52 55 1795 2790
E: jorgem@communika.com.mx

[16] https://n9.cl/o49o4
[17] https://n9.cl/owr09

Daños por más de 10 billones de dólares impulsan al mercado global de ciberseguridad

Por staff de redacción Infosecurity Mexico

De acuerdo con reportes de especialistas[18], 5,190 millones de usuarios utilizaban Internet a principios del tercer trimestre de 2023 alrededor del mundo; es decir, el 64.5 % de la población global. Tal cantidad continúa aumentando, y los datos más recientes indican que la población conectada creció en más de 100 millones desde julio del 2022 hasta el mismo mes de este año.

Se calcula que los daños causados por los ciberdelincuentes alcanzarán los 10.5 billones de dólares por año, desde lo que resta del 2023, hasta el 2025[19]. Tan solo para el 2023 se estima que los delitos cibernéticos ocasionen daños globales por 8 billones de dólares. Tal cifra equivale a lo que sería la tercera economía más grande del mundo, después de EE. UU. y China.

Probablemente los costos globales del cibercrimen crecerán 15% por año durante los próximos tres, y alcanzarán la cifra citada para el 2025, frente a los 3 billones de dólares que se registraron en el 2015. Esta sería la mayor transferencia de riqueza económica en la historia, y como consecuencia, arriesga los incentivos para innovar e invertir. Los impactos resultantes son superiores a los causados por los desastres naturales en un año y serán más rentables que el comercio global de las principales drogas ilegales combinadas.

¿Por qué los costos de los delitos cibernéticos son tan grandes y cuáles son las afectaciones? Porque se incluyen daños y destrucción de datos, extracción de dinero, pérdida de productividad, daños a la propiedad intelectual, robo de datos personales y financieros, malversación, fraudes, crisis en el negocio después del ataque, desvío de recursos para la investigación forense, la restauración y eliminación de datos pirateados, y daños a los sistemas e incluso a la reputación.

Es por eso que, a medida que las filtraciones de datos, la piratería y los delitos cibernéticos se incrementan, las organizaciones deben incrementar su confianza en los profesionales en seguridad cibernética para identificar amenazas potenciales y proteger su información. Por lo tanto, se espera que el mercado de la seguridad cibernética crecerá de $217,000 millones en 2021 a $345,000 millones para 2026, con una tasa de crecimiento anual compuesto del 9.7% en el mismo lapso[20].

Cabe señalar que un delito cibernético comprende cualquier actividad no autorizada que involucre una computadora, dispositivo o red. Hay tres clasificaciones reconocidas de tales delitos: los asistidos por computadora, los delitos en los que la computadora misma es un objetivo y aquellos en los que la computadora es incidental al delito y no se relaciona directamente.

A continuación citamos las amenazas cibernéticas más comunes:

- Ciberterrorismo: es un ataque a las computadoras y a las TI en general con motivos políticos; buscan causar daño y generalizar una perturbación social.
-

[18] https://n9.cl/5j5kn

[19] https://n9.cl/aliu13

[20] https://n9.cl/czhqz

- Malware: abarca el ransomware, spyware, virus y gusanos. Puede instalar software dañino, bloquear el acceso a los recursos de la computadora, interrumpir el sistema o transmitir información desde el centro de almacenamiento de datos de forma encubierta.
- Botnets: son ataques cibernéticos, remotos y a gran escala, realizados por dispositivos infectados por malware. Es como si formaran una cadena de computadoras coordinada por un ciberdelincuente y como consecuencia las computadoras comprometidas se vuelven parte del sistema botnet.
- Adware: es una forma de malware. A menudo se le llama software con publicidad; se trata de un programa potencialmente no deseado (PUP) que se instala sin permiso y genera anuncios en línea no deseados.
- Phishing: los piratas informáticos utilizan comunicaciones falsas, especialmente el correo electrónico, para engañar al destinatario para que lo abra y siga instrucciones que normalmente solicitan información personal. Algunos ataques de este tipo también instalan malware.
- Ataque “Man-in-the-middle”: involucran a los piratas informáticos que se insertan en una transacción en línea de dos personas. Una vez dentro, los piratas informáticos pueden filtrar y robar los datos deseados. A menudo ocurren en redes wifi públicas no seguras.
- Denegación de servicio: DoS es un ataque que inunda una red o computadora con una cantidad abrumadora de procesos de "apretón de manos", sobrecargando efectivamente el sistema y haciéndolo incapaz de responder a las solicitudes de los usuarios.

Para conocer más, Infosecurity Mexico espera a los profesionales de la ciberseguridad para que compartan experiencias, conozcan tendencias y las mejores soluciones para prevenir ataques y recuperarse de los ciberdelitos. La cita está hecha.

# # #

Acerca de Infosecurity Mexico
Es el evento más importante del sector de ciberseguridad y seguridad de la información en el que se ofrece acceso a tendencias, conferencias y workshops de la mano de expertos.

Acerca de RX (Reed Exhibitions)

RX está en el negocio de construir negocios para individuos, comunidades y organizaciones. Elevamos el poder de los eventos cara a cara combinando datos y productos digitales para ayudar a los clientes a conocer los mercados, obtener productos y completar transacciones en más de 400 eventos en 22 países, en 42 industrias.

En RX nos apasiona generar un impacto positivo en la sociedad y estamos totalmente comprometidos con la creación de un entorno de trabajo inclusivo para toda nuestra gente. RX es parte de RELX, proveedor global de información basada en análisis y herramientas de decisión para clientes profesionales y de negocios. www.rxglobal.com

Acerca de RELX

RELX es un proveedor global de analítica basada en información y herramientas de decisión para clientes profesionales y de negocio. RELX sirve a clientes en más de 180 países y tiene oficinas en alrededor de 40 países. Emplea a más de 35,000 personas, de las cuales, cerca del 40% se encuentran en Norteamérica. Las acciones de RELX PLC, la empresa matriz, son negociadas en las bolsas de valores de Londres, Ámsterdam y Nueva York Stock Exchanges, utilizando los símbolos: Londres: REL; Ámsterdam: REN; Nueva York: RELX.
*Nota: La actual capitalización de mercado se puede encontrar en: http://www.relx.com/investors

Para mayor información:
Jorge Morales García
Agencia Communika
T: +52 55 1795 2790
E: jorgem@communika.com.mx

Crece gasto global en ciberseguridad, pero el ransomware no se detiene

Por staff de redacción Infosecurity Mexico

Aunque no es un fenómeno nuevo, hablar de cibercrímenes resulta un tema recurrente en la actualidad, ya que a diario se escucha de algún acontecimiento en el mundo relacionado con afección de datos y sistemas. Se tiene el registro de que el primer delito considerado como cibercrimen se llevó a cabo en Francia[21], en 1834, cuando dos ladrones robaron información del mercado financiero pirateando el sistema telegráfico francés.

Desde entonces, el mundo empresarial ha experimentado varias transformaciones y avances tecnológicos que, al tiempo de generar beneficios, han provocado riesgos potenciales y reales, sobre todo en lo relacionado al uso de las TI. En ese sentido, uno de los hitos que cambiaron el quehacer empresarial fue el surgimiento de Internet, cuyo inicio se registra alrededor del año 1960[22], aunque la fecha puede variar dependiendo la fuente.

Hoy en día, uno de los temas de los que más se habla es el de la digitalización, que se refiere al uso de tecnologías digitales para cambiar un modelo de negocio y proporcionar nuevos ingresos y oportunidades de producción de valor[23]. Conduce a grandes cambios en los procesos y también puede influir significativamente en la satisfacción del cliente y la calidad del producto.

Algunos ejemplos de tecnologías digitales son los sitios web, los teléfonos celulares, sistemas de geolocalización, cajeros automáticos, blogs, computadoras y otras herramientas que, por otro lado, son afectadas por los cibercriminales a través de una gama múltiple de formas de ataque que provocan grandes daños.

El problema es de tal dimensión que se calcula que el gasto global en ciberseguridad alcanzará la cifra de más de 1.75 billones de dólares, de forma acumulativa, en el 2025, iniciando el cálculo desde el 2021. Esto se debe al imperativo de proteger a las empresas, precisamente cada vez más digitalizadas[24], los dispositivos de Internet de las cosas (IoT), y a los propios usuarios.

Solo como referencia, en 2004, el mercado mundial de ciberseguridad valía solo 3,500 millones de dólares[25], y ahora es uno de los sectores más grandes y de más rápido crecimiento en la economía de la información, por eso se esperaba que el mercado de la ciberseguridad creciera un 15 %, año tras año, entre 2021 y 2025.

Las empresas requieren invertir en ciberseguridad porque las ciberamenazas son múltiples, y quizá una de las más recurrentes es el ransomware, que impide a los usuarios acceder a su sistema o a sus archivos personales, y exige el pago de un rescate para poder recuperar el acceso.

---

[21] https://n9.cl/96q3p
[22] https://n9.cl/46p0tx
[23] https://n9.cl/4yyew
[24] https://n9.cl/aliu13
[25] https://n9.cl/2dyxs

Este delito causó daños por 20,000 millones de dólares en el 2021, y se calcula que la cifra alcanzará los 265,000 millones para el 2031[26]. El problema radica en que, de todas las víctimas, el 32% paga el rescate, pero solo recuperan el 65 % de sus datos, en tanto que solo el 57 % de las empresas recupera su información gracias a que cuentan con una copia de seguridad. La amenaza es mayor, porque la frecuencia de los ataques de ransomware a gobiernos, empresas, consumidores y dispositivos seguirá aumentando durante los próximos ocho años, llegando a realizarse un nuevo ataque cada dos segundos para el 2031.

Tampoco se puede ignorar la variante del ransomware dirigido, especialmente orientado a las industrias que dependen en gran medida de softwares específicos para ejecutar sus actividades diarias. Un ejemplo de tal modalidad de ransomware es el ataque Wanna Cry[27] en los hospitales del Servicio Nacional de Salud en Inglaterra, Escocia, que corrompió más de 70,000 dispositivos médicos.

Desde luego, existen más amenazas, y por eso es que vale considerar a Infosecurity Mexico como un foro en el que se presentan los profesionales de la ciberseguridad, quienes compartirán las mejores prácticas y mostrarán la tecnología más avanzada para prevenir ataques y solucionar problemas causados por ciberataques. La cita es cada vez más cercana.

# # #

Acerca de Infosecurity Mexico
Es el evento más importante del sector de ciberseguridad y seguridad de la información en el que se ofrece acceso a tendencias, conferencias y workshops de la mano de expertos.

Acerca de RX (Reed Exhibitions)
RX está en el negocio de construir negocios para individuos, comunidades y organizaciones. Elevamos el poder de los eventos cara a cara combinando datos y productos digitales para ayudar a los clientes a conocer los mercados, obtener productos y completar transacciones en más de 400 eventos en 22 países, en 42 industrias.
En RX nos apasiona generar un impacto positivo en la sociedad y estamos totalmente comprometidos con la creación de un entorno de trabajo inclusivo para toda nuestra gente. RX es parte de RELX, proveedor global de información basada en análisis y herramientas de decisión para clientes profesionales y de negocios. www.rxglobal.com

Acerca de RELX
RELX es un proveedor global de analítica basada en información y herramientas de decisión para clientes profesionales y de negocio. RELX sirve a clientes en más de 180 países y tiene oficinas en alrededor de 40 países. Emplea a más de 35,000 personas, de las cuales, cerca del 40% se encuentran en Norteamérica. Las acciones de RELX PLC, la empresa matriz, son negociadas en las bolsas de valores de Londres, Ámsterdam y Nueva York Stock Exchanges, utilizando los símbolos: Londres: REL; Ámsterdam: REN; Nueva York: RELX.
*Nota: La actual capitalización de mercado se puede encontrar en: http://www.relx.com/investors

Para mayor información:
Jorge Morales García
Agencia Communika
T: +52 55 1795 2790
E: jorgem@communika.com.mx

[26] https://n9.cl/fyr6b
[27] https://n9.cl/fxmdq

¿Qué es el BEC, cuáles sus efectos y cómo protegernos?

Por staff de redacción Infosecurity Mexico

Ya hace casi una década que el FBI encontró las primeras pistas de lo que bautizó como "Business Email Compromise" (e-mail de negocio comprometido), o "BEC", que consiste en un ciberataque de estafa que involucra piratería, falsificación o suplantación de una dirección de correo de un negocio, y desde entonces, la amenaza sigue creciendo.

En este tipo de ataques, la víctima recibe un correo que parece provenir de una empresa de confianza, simula ser genuino, pero normalmente tiene un enlace de phishing, un archivo adjunto de carácter maligno, o bien, una solicitud de transferencia de dinero a una cuenta que termina siendo la del atacante.

Relacionadas con los BEC, figuran las cuentas de correo comprometidas (EAC), cuya vulnerabilidad resulta a partir de que el usuario accede a una página que contiene una brecha de seguridad que expone sus datos para aprovecharlos con fines maliciosos. Este tipo de cuentas están creciendo en esta era de infraestructura basada en la nube.

Sin embargo, el mayor riesgo es que las cuentas comprometidas se utilizan cada vez más para fraudes de BEC, los cuales son difíciles de detectar, especialmente con herramientas tradicionales y defensas nativas de plataformas de nube.

Para realizar estafas de BEC los cibercriminales pueden suplantar una cuenta de correo o sitio web para engañar a las víctimas que piensan que las cuentas son auténticas; ya decíamos del envío de correos con phishing que parecen provenir de un remitente seguro para que las víctimas entreguen información confidencial, pero además figura el uso de malware que se infiltra a la red de la empresa para obtener acceso legítimo a correos para buscar información de pagos y facturas, así como datos de la víctima como contraseñas y números de cuentas financieras.

De acuerdo con el Reporte de Investigación de Brechas de Datos[28], la mayoría de los ciberataques de BEC están motivados por dinero. Un correo fraudulento puede tener un enlace de phishing que lleve a una página de inicio falsa para obtener credenciales. Los atacantes pueden persuadir a su víctima de comprar certificados de regalo, más que de hacer una transferencia de dinero.

El BEC se considera un método de ciberataque común, pero dado que los ataques pasan desapercibidos es difícil saber cuántos negocios han sido afectados y en qué grado. La mejor fuente de estadísticas del cibercrimen es el Centro de Quejas de Crimen de Internet del FBI que reporta lo siguiente:

- Entre 2016 y 2020 se registraron 185,718 incidentes BEC en el mundo que resultaron en $28,000 millones de dólares en pérdidas[29].
- Las pérdidas por BEC en 2020 superaron los $1,800 millones de dólares.
- El número de incidentes BEC creció 61% entre 2016 y 2020.

[28] https://n9.cl/k018o
[29] https://n9.cl/zqfo7

Cómo protegerse de un fraude de BEC

1. Cuide la información que comparte en línea o redes sociales, como nombres de mascotas, escuelas, cumpleaños, ligas a miembros de la familia; los cibercriminales obtienen información para adivinar contraseñas o responder preguntas de seguridad.
2. No abra correos o mensajes de texto no solicitados en donde le soliciten que actualice o verifique información de cuentas; llame de inmediato a la empresa o banco que supuestamente hace la solicitud para verificar e informarles.
3. Examine con cuidado las direcciones de correo, URLs y deletreo usado en los correos; los estafadores usan pequeñas diferencias para engañar la vista y ganarse su confianza.
4. Cuidado con lo que descarga: nunca abra un archivo adjunto de alguien que desconozca y tenga cuidado con los archivos adjuntos reenviados a usted.
5. Establezca autenticaciones de dos o más pasos en cualquier cuenta que lo permita y no las deshabilite.
6. Si es posible verifique las solicitudes de compra y pagos presenciales llamando al a persona para verificar su legitimidad. Debe verificar cualquier cambio de número de cuenta o procedimientos de pago con quien hace la solicitud.
7. Sea especialmente cauteloso si el solicitante lo presiona a actuar con rapidez.

Infosecurity Mexico recomienda que los usuarios estén muy atentos a los correos electrónicos que reciben, ya que siguen siendo una herramienta de comunicación y negocios, así que debemos seguir administrándolos adecuadamente… por mucho tiempo.

# # #

Acerca de Infosecurity Mexico
Es el evento más importante del sector de ciberseguridad y seguridad de la información en el que se ofrece acceso a tendencias, conferencias y workshops de la mano de expertos.

Acerca de RX (Reed Exhibitions)
RX está en el negocio de construir negocios para individuos, comunidades y organizaciones. Elevamos el poder de los eventos cara a cara combinando datos y productos digitales para ayudar a los clientes a conocer los mercados, obtener productos y completar transacciones en más de 400 eventos en 22 países, en 42 industrias.
En RX nos apasiona generar un impacto positivo en la sociedad y estamos totalmente comprometidos con la creación de un entorno de trabajo inclusivo para toda nuestra gente. RX es parte de RELX, proveedor global de información basada en análisis y herramientas de decisión para clientes profesionales y de negocios. www.rxglobal.com

Acerca de RELX
RELX es un proveedor global de analítica basada en información y herramientas de decisión para clientes profesionales y de negocio. RELX sirve a clientes en más de 180 países y tiene oficinas en alrededor de 40 países. Emplea a más de 35,000 personas, de las cuales, cerca del 40% se encuentran en Norteamérica. Las acciones de RELX PLC, la empresa matriz, son negociadas en las bolsas de valores de Londres, Ámsterdam y Nueva York Stock Exchanges, utilizando los símbolos: Londres: REL; Ámsterdam: REN; Nueva York: RELX. La capitalización de mercado es de aproximadamente £ 33 mil millones, € 39 mil millones, $ 47 mil millones*.
*Nota: La actual capitalización de mercado se puede encontrar en: http://www.relx.com/investors

Para mayor información:
Jorge Morales García
Agencia Communika
T: +52 55 1795 2790
E: jorgem@communika.com.mx

Considera Infosecurity Mexico vital el “compliance” o cumplimiento para evaluar riesgos

Por staff de redacción Infosecurity Mexico

A pesar de que en el año 2022 México se situaba en el puesto 87 de 163 países que clasifica el National Cyber Security Index, organismo que configura una muestra mundial en materia de seguridad informática, para el presente año descendió y ubicándose hoy en el lugar 90 del mismo registro[30].

Por ello es que, conforme crece el número de ciberataques, las organizaciones de todas las industrias deben reforzar su seguridad al tiempo que crean regulaciones más restrictivas con nuevos requerimientos. Bajo tales condiciones, el cumplimiento de la ciberseguridad se ha vuelto la fuerza impulsora del éxito, por lo que las entidades deben combinar una estrategia eficiente de seguridad al mismo tiempo que adelantarse a los requisitos legales y corporativos.

Debido a que todas las organizaciones trabajan con información y están conectadas a Internet, por eso deben pensar seriamente en la ciberseguridad. Acceder a los datos y moverlos de un lugar a otro expone a las organizaciones y las hace vulnerables a potenciales ciberataques. Por esta razón vale la pena considerar el cumplir con los lineamientos de ciberseguridad para adherirse a los estándares y requisitos reglamentarios establecidos por una agencia, ley o autoridad.

Las organizaciones deben lograr este cumplimiento estableciendo controles basados en riesgos para proteger la confidencialidad, integridad y disponibilidad de la información, la cual debe estar protegida mientras está almacenada, procesada, integrada o es transferida. El cumplimiento es un reto importante para las organizaciones porque los estándares y requerimientos pueden traslaparse, llevando a confusión y más trabajo.

Sin embargo, el cumplimiento (compliance) en la ciberseguridad es imperante para las empresas, porque ninguna está inmune a los ciberataques. Cumplir con los estándares y regulaciones es un principio de administración, de hecho, es un factor determinante en la capacidad de la organización para alcanzar el éxito, tener operaciones fluidas y mantener prácticas de seguridad.

El problema es que las empresas pequeñas y medianas tienden a estar en mayor riesgo, ya que no priorizan la ciberseguridad, facilitando el camino para que los delincuentes aprovechen sus vulnerabilidades y recibiendo ataques que causan daños costosos. Según el Cyber Readiness Institute, solo el 40% de estas empresas han implementado políticas de ciberseguridad.

Crear un programa de cumplimiento de ciberseguridad podría parecer una tarea enorme, porque no hay una estrategia única, pero siguiendo los siguientes pasos se puede desarrollar un programa propio para cumplir con los requisitos de cumplimiento de regulaciones:
1. Crear un equipo de cumplimiento: el equipo de TI es el primer involucrado en la ciberseguridad, pero las demás áreas de la empresa deben trabajar en equipo para mantener una buena postura ante las medidas de cumplimiento.
2. Establecer un proceso de análisis de riesgo: hay 4 pasos básicos en un proceso de análisis; **identificar** los sistemas, activos y redes que pueden acceder a la información; **evaluar**

[30] bit.ly/3PSObMO

el nivel de riesgo; **analizar la probabilidad** del riesgo y su costo; **establecer tolerancias** para mitigar, transferir, rechazar o aceptar una determinada contingencia.
3. Establecer controles para mitigar riesgos: el siguiente paso es establecer controles de ciberseguridad que mitiguen los riesgos. Un control detecta, previene y disminuye amenazas, y puede ser de tipo técnico como contraseñas y controles de acceso, o de tipo físico como cámaras de vigilancia. Igual pueden ser encriptaciones, firewalls, seguros, capacitación, plan de respuesta a incidentes, control de accesos y programación, y gestión de parches.
4. Crear políticas: se deben documentar las políticas y guías de los controles que los equipos de TI, empleados y otros deben cumplir.
5. Monitoreo y rápida respuesta: es crucial monitorear constantemente el programa de cumplimiento conforme surgen regulaciones o se actualizan las políticas. La meta del programa de cumplimiento es identificar y gestionar los riesgos y detener a las amenazas antes de que se conviertan en una brecha de datos.

Vale la pena que los encargados de ciberseguridad consideren todos los elementos que inciden en el cumplimiento, y una de las mejores formas de hacerlo es actualizarse en foros como Infosecurity Mexico, en donde se dan cita los profesionales de la ciberseguridad para intercambiar conocimientos y actualizarse en su especialidad. Ya está la cita programada.

# # #

Acerca de Infosecurity Mexico
Es el evento más importante del sector de ciberseguridad y seguridad de la información en el que se ofrece acceso a tendencias, conferencias y workshops de la mano de expertos.

Acerca de RX (Reed Exhibitions)
RX está en el negocio de construir negocios para individuos, comunidades y organizaciones. Elevamos el poder de los eventos cara a cara combinando datos y productos digitales para ayudar a los clientes a conocer los mercados, obtener productos y completar transacciones en más de 400 eventos en 22 países, en 42 industrias.
En RX nos apasiona generar un impacto positivo en la sociedad y estamos totalmente comprometidos con la creación de un entorno de trabajo inclusivo para toda nuestra gente. RX es parte de RELX, proveedor global de información basada en análisis y herramientas de decisión para clientes profesionales y de negocios. www.rxglobal.com

Acerca de RELX
RELX es un proveedor global de analítica basada en información y herramientas de decisión para clientes profesionales y de negocio. RELX sirve a clientes en más de 180 países y tiene oficinas en alrededor de 40 países. Emplea a más de 35,000 personas, de las cuales, cerca del 40% se encuentran en Norteamérica. Las acciones de RELX PLC, la empresa matriz, son negociadas en las bolsas de valores de Londres, Ámsterdam y Nueva York, utilizando los símbolos: Londres: REL; Ámsterdam: REN; Nueva York Stock Exchanges. La capitalización de mercado es de aproximadamente £ 33 mil millones, € 39 mil millones, $ 47 mil millones*.
*Nota: La actual capitalización de mercado se puede encontrar en: http://www.relx.com/investors

Para mayor información:
Jorge Morales García
Agencia Communika
T: +52 55 1795 2790
E: jorgem@communika.com.mx

Anuncia Infosecurity Mexico su programa de conferencias especializadas

- También habrá un panel en el que se abordará el tema de la legislación en ciberseguridad

CDMX, a __ de julio de 2023.- Infosecurity Mexico dio a conocer los detalles de los horarios y temas de las conferencias especializadas y paneles que conforman su programa educativo, el cual estará a cargo de ponentes nacionales e internacionales que actualizarán a los profesionales de la ciberseguridad que se darán cita el 4 y 5 de octubre en el Centro Citibanamex de la Ciudad de México.

La primera plática, con el tema “Estándares y marcos de referencia – nivel expert”, se llevará a cabo el miércoles 4 en el área de Tech Lab, a cargo de Gabriela Reynaga, Directora de consultoría en Holistics GRC, con un horario de 09:00 h a 11:00 h. Esta misma plática se repetirá de 15:00 h a 17:00 h. Posteriormente, de 12:30 h a 13:10 h, en la Smart Defense Arena, estará Mike Nelson, VP de DigiCert, con la plática “Creating Digital Trust in 2023 and beyond”.

De 13:00 h a 14:00 h en el Summit, estará Roger A. Grimes, Data-driven Defense Evangelist, con el tema “Ransomware: prevención y respuesta paso a paso”. De 15:00 h a 15:30 h en el Coffee se presentará Marlon Palma, LATAM Director Next Group, con “Resiliencia sin dolor”; y de 16:00 h a 16:40 h en la Smart Defense Arena se encontrará Juan Alejandro Aguirre, Director de ingeniería para Sophos Latam, hablando de “Telemetría de terceros, Pipeline de detección y creación de casos”.

Ese mismo día, de 16:00 h a 17:00 h en el Summit intervendrá Carlos Chalico, Líder de ciberseguridad y privacidad en EY, con el tema “Tendencias globales de ciberseguridad y privacidad”. El cierre del miércoles 4 se realizará en el mismo sitio y estará a cargo de Deepak Daswuani, experto en ciberseguridad y autor del libro “La amenaza hacker”, quien presentará una conferencia única de 17:20 h a 18:20 h.

El ciclo de conferencias del jueves 5 iniciará a las 09:00 h con el panel “Regulación mexicana en materia de ciberseguridad”, en el área del Summit, en el que participarán Gabriela Reynaga, Directora de consultoría en Holistics GRC; Erika Mata, Catedrática y Conferencista internacional; Ivonne Muñoz, experta en comercio electrónico y Auditora líder; y Jorge Osorio Bretón, Director en CSI Consultores en Seguridad de la Información.

El programa continuará de 11:30 h a 12:10 h en la Smart Defense Arena, en donde se presentará Weimar Gutiérrez, Technical Account Manager, con el tema “CIEM, obteniendo visibilidad y control en la nube”. Acto seguido, de 12:30 h a 13:30 h, en el Summit, tendrá turno Omar Herrera, CISO, con el tema “Ciberseguridad costo-efectiva en la nube”.

De 12:30 h a 13:10 h, en la Smart Defense Arena, estará nuevamente Juan Alejandro Aguirre, Director de ingeniería para Sophos Latam, ahora con la plática “Síndrome de la rana hervida – lecciones de la remediación de ransomware”. De 15:10 h a 16:10 h se presentará una vez más Weimar Gutiérrez, Technical Account Manager, con el tema “Puntos débiles de ciberseguridad que deben abordarse antes de adoptar el ataque”.

Las dos últimas conferencias del día, ambas en el Summit, serán “Los desarrolladores: culpables o inocentes de la inseguridad en los sistemas”, de 16:00 h a 17:00 h, a cargo de Mario Farías Elinos, Cyber Security Researcher and Expert, y “Crowdsourcing government flight tracking with

social media", de 17:20 h a 18:20 h, por parte de Andrew Logan, Tracking Military Ghost Helicopters.
Se recomienda que para conocer los costos y condiciones de acceso a las conferencias se consulte el sitio www.infosecuritymexico.com y obtener información sobre el registro y más datos sobre los conferencistas y los temas que van a desarrollar.

# # #

Acerca de Infosecurity Mexico
Es el evento más importante del sector de ciberseguridad y seguridad de la información en el que se ofrece acceso a tendencias, conferencias y workshops de la mano de expertos.

Acerca de RX (Reed Exhibitions)
RX está en el negocio de construir negocios para individuos, comunidades y organizaciones. Elevamos el poder de los eventos cara a cara combinando datos y productos digitales para ayudar a los clientes a conocer los mercados, obtener productos y completar transacciones en más de 400 eventos en 22 países, en 42 industrias.
En RX nos apasiona generar un impacto positivo en la sociedad y estamos totalmente comprometidos con la creación de un entorno de trabajo inclusivo para toda nuestra gente. RX es parte de RELX, proveedor global de información basada en análisis y herramientas de decisión para clientes profesionales y de negocios. www.rxglobal.com

Acerca de RELX
RELX es un proveedor global de analítica basada en información y herramientas de decisión para clientes profesionales y de negocio. RELX sirve a clientes en más de 180 países y tiene oficinas en alrededor de 40 países. Emplea a más de 35,000 personas, de las cuales, cerca del 40 % se encuentran en Norteamérica. Las acciones de RELX PLC, la empresa matriz, son negociadas en las bolsas de valores de Londres, Ámsterdam y Nueva York, utilizando los símbolos: Londres: REL; Ámsterdam: REN; Nueva York: Stock Exchanges. La capitalización de mercado es de aproximadamente £ 33 mil millones, € 39 mil millones, $ 47 mil millones*.
*Nota: La actual capitalización de mercado se puede encontrar en: http://www.relx.com/investors

Para mayor información:
Jorge Morales García
Agencia Communika
T: +52 55 1795 2790
E: jorgem@communika.com.mx

Esperan los talleres de Infosecurity Mexico a los profesionales en ciberseguridad

- Incluso habrá una competencia en la que los participantes podrán mostrar sus conocimientos

CDMX, julio de 2023.- Infosecurity México anunció el calendario de talleres que tendrán lugar el 4 y 5 de octubre, en el que expertos en seguridad en internet y en sistemas, llevarán a cabo conferencias, talleres y demostraciones, e invitarán a practicar a los asistentes interesados en actualizarse y conocer nuevas modalidades de ataques y cómo defenderse ante ellos.

El primero de ellos, con el título "Taller Red Team – Penetration Testing, nivel expert", tendrá lugar el miércoles 4 de 09:00 a 11:00 h, y será impartido por Enrique Herrera, de la firma de ciberseguridad *Cyberimox*, quien cuenta con más de una década de experiencia en los sectores público y privado. Ese mismo día habrá un taller a cargo de la firma Kaspersky de 13:00 a 14:00 h.

Más tarde, de 15:00 a 17:00 h, se llevará a cabo el taller "OSINT ciber inteligencia – nivel en formación", que igualmente estará a cargo de Enrique Herrera, quien se presentará nuevamente el jueves 5 de 09:00 h a 11:00 h con el taller "Mittre Attack – nivel en formación". Posteriormente, de 15:00 h a 17:00 h, él dirigirá el taller de "Informática forense – nivel expert".

Entre las novedades que se presentarán en la próxima edición de Infosecurity Mexico figura la competencia "Capture the flag – respuesta a incidentes", que estará a cargo de Levi Sinuhe Reza, Conferencista internacional especializado en temas de ciberseguridad e Instructor de EC-Council y CompTIA.

De acuerdo con el Comité Organizador, la convocatoria a esta competición se dirige a profesionales de la ciberseguridad que posean conocimientos básicos e intermedios en seguridad ofensiva e IR, o bien, que se desempeñen en SOC´S y conozcan de monitoreo, incident response o forense.

En el lugar, los participantes del concurso recibirán máquinas virtuales tools con evidencias de equipos comprometidos para poder ejecutar un plan de respuesta a incidentes, obteniendo Artifacts para obtener IoCs, TTPs, mapeo a Mitre ATT&ACK, y búsqueda de evidencias con reglas Yara y Sigma, todo con el propósito de contener el incidente de ciberseguridad.

Para los ganadores, se entregarán los siguientes premios: El primer lugar recibirá unos audífonos Apple Air Pods Max, al segundo se le entregará un reloj Apple Watch, y el tercer lugar será acreedor de una bocina de alta fidelidad Apple Home Pod. La competencia se llevará a cabo el jueves 5 de 09:00 h a 11:00 h, y se repetirá de 15:00 h a 17:00 h.

En todos los casos, para conocer los costos y condiciones de acceso a los talleres que se llevarán a cabo en los espacios designados, Tech Lab 1 y Tech Lab 2, así como los detalles de la competencia, se invita a los interesados a visitar el sitio www.infosecuritymexico.com

# # #

Acerca de Infosecurity Mexico
Es el evento más importante del sector de ciberseguridad y seguridad de la información en el que se ofrece acceso a tendencias, conferencias y workshops de la mano de expertos.

Acerca de RX (Reed Exhibitions)
RX está en el negocio de construir negocios para individuos, comunidades y organizaciones. Elevamos el poder de los eventos cara a cara combinando datos y productos digitales para ayudar a los clientes a conocer los mercados, obtener productos y completar transacciones en más de 400 eventos en 22 países, en 42 industrias.
En RX nos apasiona generar un impacto positivo en la sociedad y estamos totalmente comprometidos con la creación de un entorno de trabajo inclusivo para toda nuestra gente. RX es parte de RELX, proveedor global de información basada en análisis y herramientas de decisión para clientes profesionales y de negocios. www.rxglobal.com

Acerca de RELX
RELX es un proveedor global de analítica basada en información y herramientas de decisión para clientes profesionales y de negocio. RELX sirve a clientes en más de 180 países y tiene oficinas en alrededor de 40 países. Emplea a más de 35,000 personas, de las cuales, cerca del 40% se encuentran en Norteamérica. Las acciones de RELX PLC, la empresa matriz, son negociadas en las bolsas de valores de Londres, Ámsterdam y Nueva York Stock Exchanges, utilizando los símbolos: Londres: REL; Ámsterdam: REN; Nueva York: RELX. La capitalización de mercado es de aproximadamente £ 33 mil millones, € 39 mil millones, $ 47 mil millones*.
*Nota: La actual capitalización de mercado se puede encontrar en: http://www.relx.com/investors

Para mayor información:
Jorge Morales García
Agencia Communika
T: +52 55 1795 2790
E: jorgem@communika.com.mx

Los bancos preocupados por el robo de identidad; el usuario debe cooperar

Por staff de redacción Infosecurity Mexico

Hay cifras que nos hacen reflexionar cuando hablamos del robo de identidad, un delito que, si llega a sucedernos, nos puede afectar de gran manera. Solo para dimensionar este fenómeno, vale la pena considerar que los costos que genera tal fraude a las instituciones que otorgan créditos a través de canales digitales en el país[31], equivalen al 2.42% de sus ingresos anuales.

Por cierto, los avances tecnológicos que ayudan a crear nuevos productos y brindar opciones de crédito para la población no bancarizada también posibilitan los intentos de fraude bancario en distintas modalidades que generan pérdidas millonarias a las instituciones financieras dedicadas a promover créditos, pero al mismo tiempo deben cuidarse de no ser afectadas por tal crimen.

Se debe considerar que, por lo menos, hay dos esquemas de fraude: el robo de identidad y la creación de identidades sintéticas, ambos se usan para solicitar algún tipo de crédito o tarjeta bancaria, y su daño es tal que, por cada dólar involucrado en un caso de fraude de identidad, las instituciones crediticias pierden hasta cuatro veces el valor nominal en cada operación financiera.

La diferencia entre ambos tipos es que el robo de identidad se configura cuando el delincuente obtiene datos financieros y de identificación de alguna persona, con lo cual pueden usurpar la identidad de alguien y solicitar algún tipo de crédito o producto financiero, abrir cuentas bancarias o tener acceso a una cuenta de un tercero. ¿Quién paga los daños? El afectado por el robo.

En cuanto a las identidades sintéticas, se elaboran mediante la combinación de información real de uno o varios individuos, con datos de empleo, residencia, estados financieros, junto con datos falsos para buscar obtener algún bien, un crédito o un servicio que no podría obtener de manera legal o normal. Se trata de identidades falsas, nuevas.

En cualquier caso, el daño es significativo. A nivel global, un estudio[32] arrojó que el 26% de los bancos encuestados y 17 % de fintech reportaron más de cien incidentes de fraude de identidad en el 2022, de acuerdo con expertos en delitos en servicios financieros de Australia, Francia, Alemania, Reino unido, Estados Unidos y México, entre otros países.

En todos los casos, la falsificación de documentos configuró el tipo de fraude de identidad más común. El 54% de los encuestados declararon haber lidiado con incidentes relacionados con documentación modificada, y es que la creatividad y habilidad de los delincuentes pareciera que no tienen límite.

Este tipo de delito representa un motivo de alarma para las instituciones financieras, pero también el usuario debe poner de su parte, sobre todo en el caso del robo de identidad. En ese sentido, la CONDUSEF[33] recomienda que no se proporcione información de las cuentas bancarias personales por vía telefónica, mensaje de texto, WhatsApp, correo electrónico, o redes sociales.

Como complemento, se deben cambiar las contraseñas con frecuencia, revisar regularmente los

[31] https://t.ly/Ji1c3
[32] https://t.ly/-o3YW
[33] https://t.ly/yx_S

estados de cuenta bancaria, no acceder a enlaces recibidos por correo, supuestamente provenientes del banco personal, y no descargar aplicaciones si no hay seguridad de que es el banco el que lo solicita.

Y si hay un robo de tarjetas se debe avisar de inmediato al banco y cancelarlas. Si hay robo de identificaciones, se debe acudir al Ministerio Público y solicitar reposiciones en las instituciones correspondientes.

No hay opción: debemos cuidar nuestros documentos y estar atentos a la información que recibimos en algún dispositivo. Es mejor exagerar en las prevenciones a despertar un día y decir "me hackearon". Para aprender más sobre estos delitos, vale la pena visitar Infosecurity Mexico. Ya estamos cerca.

# # #

Acerca de Infosecurity Mexico
Es el evento más importante del sector de ciberseguridad y seguridad de la información en el que se ofrece acceso a tendencias, conferencias y workshops de la mano de expertos.

Acerca de RX (Reed Exhibitions)
RX está en el negocio de construir negocios para individuos, comunidades y organizaciones. Elevamos el poder de los eventos cara a cara combinando datos y productos digitales para ayudar a los clientes a conocer los mercados, obtener productos y completar transacciones en más de 400 eventos en 22 países, en 42 industrias.
En RX nos apasiona generar un impacto positivo en la sociedad y estamos totalmente comprometidos con la creación de un entorno de trabajo inclusivo para toda nuestra gente. RX es parte de RELX, proveedor global de información basada en análisis y herramientas de decisión para clientes profesionales y de negocios. www.rxglobal.com

Acerca de RELX
RELX es un proveedor global de analítica basada en información y herramientas de decisión para clientes profesionales y de negocio. El Grupo sirve a clientes en más de 180 países y tiene oficinas en alrededor de 40 países. Emplea a más de 33,000 personas, de las cuales, cerca de la mitad se encuentran en Norteamérica. Las acciones de RELX PLC, la empresa matriz, son negociadas en las bolsas de valores de Londres, Ámsterdam y Nueva York, utilizando los símbolos: Londres: REL; Ámsterdam: REN; Nueva York: RELX. La capitalización de mercado es de aproximadamente £ 33 mil millones, € 39 mil millones, $ 47 mil millones*.
*Nota: La actual capitalización de mercado se puede encontrar en: http://www.relx.com/investors

Para mayor información:
Jorge Morales García
Agencia Communika
T: +52 55 1795 2790
E: jorgem@communika.com.mx

El ciber espionaje no es solo de película, también afecta tu dispositivo

Por staff de redacción Infosecurity Mexico

¿Qué es el ciber espionaje? Bueno, es el tipo de ciberataque en el que un usuario no autorizado intenta acceder a información sensible o clasificada, o propiedad intelectual de un tercero, para buscar un beneficio económico, ventaja competitiva, o motivado por razones políticas, aunque en algunos casos busca tan solo ocasionar un daño a la víctima exponiendo su información privada, o bien, dar a conocer prácticas de negocios cuestionables.

Aunque la mayoría de los ataques de ciber espionaje están motivados por ganancias monetarias, incluso también pueden ser desplegados en conjunto con operaciones militares o como actos de ciber terrorismo o ciber guerra. En este caso, su impacto, sobre todo cuando es parte de una campaña militar o política mayor, puede llevar a la disrupción de servicios públicos, infraestructura, así como a pérdida de vidas.

Los objetivos más comunes de los ataques de ciber espionaje son las grandes corporaciones, agencias de gobierno, instituciones académicas, institutos de investigación y otras organizaciones como las ONGs, que tienen valiosa propiedad intelectual o información técnica que puede darle una ventaja competitiva a otra organización o gobierno. Por otro lado, algunas veces las campañas pueden ser en contra de individuos, como prominentes líderes políticos, funcionarios de gobierno, ejecutivos corporativos y hasta celebridades.

Tácticas de ciber espionaje: La mayor parte de los ataques de ciber espionaje configuran una amenaza persistente avanzada (APT) en la que el intruso establece una presencia no detectada en la red para robar información sensible en cierto lapso. Este tipo de ataque requiere una cuidadosa planeación y diseño para infiltrar a una organización y evadir los sistemas de seguridad por largos periodos; exige un alto grado de sofisticación y los realizan equipos experimentados de cibercriminales, bien fondeados, cuyos objetivos son las organizaciones de alto valor. Además, invierten grandes cantidades de tiempo y recursos para investigar e identificar vulnerabilidades.

La mayoría de los ataques también se basan en la llamada ingeniería social para reunir la información necesaria del objetivo para realizar la intrusión. Estos métodos explotan emociones humanas como excitación, curiosidad, empatía o miedo para que las “víctimas” actúen rápido y, al hacerlo, los cibercriminales los engañan para obtener información personal dando clic en enlaces maliciosos, con lo que descargan malware o se les fuerza a pagar un rescate.

Otras técnicas de ataque incluyen el **watering-hole**, en el que los actores maliciosos infectan sitios legítimos que comúnmente usa la víctima o gente cercana para comprometer al usuario; el **spear-phishing**, en donde el agresor ataca a sus víctimas con correos, textos y llamadas fraudulentas para robar credenciales o información sensible; el **Zero-day exploits**, mediante el que los cibercriminales aprovechan alguna vulnerabilidad de seguridad o falla del software antes de que sea “parchada”; y las **amenazas internas**, en las que se convence a algún empleado o proveedor a compartir o vender información o acceso al sistema a usuarios no autorizados.

Cómo prevenir el ciber espionaje: Detectar a los ciber espías es uno de los retos más grandes para los equipos de seguridad de cualquier organización, ya que sus ataques son muy sofisticados y silenciosos en la red. Por ejemplo, el Reporte de Ciber Espionaje de Verizon encontró muchos ejemplos que comprometieron a sus usuarios en minutos, o incluso segundos, mientras que las organizaciones tardaron meses o años en descubrir el ataque.

Pero ante tales prácticas, existen algunas prácticas generales de ciber higiene que ayudan a protegerse; la principal es mantener el software actualizado, pero hay algunas consideraciones especiales que pueden ayudar a mitigar el riesgo del ciber espionaje:

Observar el comportamiento, acciones y anomalías: Los ciber espías pueden ser tan sofisticados que es difícil detectarlos con productos de seguridad, por lo que es mejor buscar anomalías en el comportamiento de usuarios y entidades a través de analíticos para detectar signos de ataques y robo de datos, ya que no se consideran registros de ataques anteriores; más bien usan modelos de comportamientos que aprenden lo que es "normal" de cada usuario y dispositivo, y detectan amenazas potenciales por actividad inusual.

Utilizar contraseñas fuertes y autenticación multifactor: El robo de credenciales es redituable para los ciber espías porque no disparan alarmas. Por ello, las organizaciones con información confidencial o sensible deben tener políticas de bloqueo de contraseñas y monitoreo de cuentas para así detectar ataques, exitosos o no, y pueden ser críticos para conocer los movimientos del atacante luego de su intento inicial.

Control de acceso y principio de menores privilegios: Este principio puede ser muy efectivo contra las campañas de espionaje y robo de datos, y se basa en que los usuarios deben tener los menores privilegios posibles de acceso para realizar su trabajo dentro de la organización, tanto para que no pueda entrometerse en otras áreas como para que, si sus credenciales son robadas, no puedan tener acceso irrestricto a los sistemas de la empresa.

Educar a los empleados y construir cultura de seguridad: Los programas de ciberseguridad completos deben incluir el elemento humano para ser efectivos. El entrenamiento de consciencia de seguridad es la mejor defensa contra los ataques de ingeniería social, por lo que es esencial enseñar a los empleados a identificar signos de phishing, pretexting y carfishing para que los espías no puedan meter un pie en el sistema.

Implementar cero confianza: En este modelo todos los dispositivos y usuarios en una organización se consideran potencialmente comprometidos por los adversarios hasta que prueben lo contrario.

Hay que tener en cuenta que aún cuando muchos países han acusado a terceros por actividades de ciber espionaje, en la mayoría de los casos los atacantes se encuentran en otros países en donde no son sujetos a extradición, por lo que las agencias de hacer cumplir la ley no tienen poder para perseguirlos. Por esto, lo más conveniente es la prevención para evitar lo más posible ser víctima de estos delincuentes.

La invitación es a que usuarios y encargados de seguridad se protejan con herramientas e inteligencia, bajo el entendido de que los cibercriminales generalmente buscan ir uno o dos pasos delante de nosotros. Por eso vale la pena darse una vuelta a foros como Infosecurity Mexico para conocer la última tecnología en ciberseguridad y las prácticas más actualizadas.

# # #

Acerca de Infosecurity Mexico
Es el evento más importante del sector de ciberseguridad y seguridad de la información en el que se ofrece acceso a tendencias, conferencias y workshops de la mano de expertos.
https://www.infosecuritymexico.com/es.html

Acerca de RX
RX está en el negocio de construir negocios para individuos, comunidades y organizaciones. Elevamos el poder de los eventos cara a cara combinando datos y productos digitales para ayudar a los clientes a conocer los mercados, obtener productos y completar transacciones en más de 400 eventos en 22 países, en 43 industrias.
En RX nos apasiona generar un impacto positivo en la sociedad y estamos totalmente comprometidos con la creación de un entorno de trabajo inclusivo para toda nuestra gente. RX es parte de RELX Group, proveedor global de información basada en análisis y herramientas de decisión para clientes profesionales y de negocios. www.rxglobal.com

Acerca de RELX
RELX es un proveedor global de analítica basada en información y herramientas de decisión para clientes profesionales y de negocio. El Grupo sirve a clientes en más de 180 países y tiene oficinas en alrededor de 40 países. Emplea a más de 33,000 personas, de las cuales, cerca de la mitad se encuentran en Norteamérica. Las acciones de RELX PLC, la empresa matriz, son negociadas en las bolsas de valores de Londres, Ámsterdam y Nueva York, utilizando los símbolos: Londres: REL; Ámsterdam: REN; Nueva York: RELX. La capitalización de mercado es de aproximadamente £ 33 mil millones, € 39 mil millones, $ 47 mil millones*.
*Nota: La actual capitalización de mercado se puede encontrar en: http://www.relx.com/investors

Para mayor información:
Jorge Morales García
Agencia Communika
T: +52 55 1795 2790
E: jorgem@communika.com.mx

Tiempo de votaciones, ¿son confiables las urnas electrónicas?

➢ *Por staff de redacción Infosecurity Mexico.*

El mundo gira en torno a los cada vez más sofisticados dispositivos electrónicos personales, el acceso a internet en cualquier lugar y a la inmediatez para conseguir información, comunicarse y comprar. Se calcula que existen alrededor de 15,140 millones de dispositivos *IoT* conectados globalmente, y se piensa que se duplicarán para el año 2030[34]. En enero de 2023 México tenía una población en línea de aproximadamente 100.6 millones de usuarios y más de 96.47 millones de usuarios de internet móvil[35].

Sin embargo, uno de los procesos que en muchos países no ha logrado establecerse completamente de manera electrónica son las votaciones para elecciones gubernamentales, aunque la tendencia es cada vez mayor en adoptar nuevas tecnologías y sistemas electrónicos para realizarlas. En América, tanto Brasil como EE. UU[36]. han implementado este sistema, no obstante, la implementación ha sido desigual.

Puede parecer increíble que, mientras la tecnología influye cada vez más en nuestra vida y actividades diarias, el uso de medios electrónicos para elecciones o consultas aún no se ha difundido de forma masiva. Lo cierto es que en México se irá utilizar parcialmente, o de manera paralela, en las próximas elecciones del Estado de México, el próximo cuatro de junio[37].

De acuerdo con expertos, el escaso uso de esta modalidad se debe principalmente a la desconfianza que genera en muchas personas la duda de que los votos sean realmente libres, confiables, secretos y seguros, ya que consideran que es fácil que un sistema computarizado pueda ser vulnerado y altere el voto personal o el resultado final[38].

Sin embargo, cabe señalar algunas ventajas que ofrecen los sistemas electrónicos para votar:

- Celeridad en el proceso.
- Ahorro de recursos en logística y material desechable.
- Menor carga de trabajo para funcionarios electorales.
- Posibilidad de votar desde cualquier lugar y no en una casilla específica.
- Rápida obtención y difusión de resultados.

Aunque, desde luego, también hay desventajas en un proceso electrónico:

- Altos costos de los equipos que deben instalarse en las casillas para el proceso.
- Probabilidad de manipulación si no se toman medidas de seguridad adecuadas.
- Escasa confianza de los electores y partidos políticos.

Este último es precisamente el principal escollo para implantar este tipo de sistemas, pues en una elección tradicional se cuentan los votos físicos para verificar los resultados, mientras que en un sistema electrónico hay temor de que se alteren los resultados por parte de los organizadores, el gobierno o los piratas cibernéticos que pudieran afectar el proceso.

---

[34] https://bit.ly/3IkZpFh
[35] https://bit.ly/2nRzrQk
[36] https://bit.ly/3MzTGgb
[37] https://bit.ly/3MBmMgd
[38] https://bit.ly/3pFCxcT

Es decir, aun con tecnología de punta, existe la posibilidad de algún imprevisto por los riesgos del sistema o por el uso de los dispositivos electrónicos, por lo que se debe contar con un plan de respuesta que contemple un mapa de riesgos con soluciones inmediatas para no impactar el proceso, además del apoyo de sistemas y especialistas forenses tecnológicos que puedan aclarar los hechos ante la opinión pública, junto con las autoridades electorales.

Desde luego, para su implementación es indispensable que el sistema realice la autenticación de los votantes para confirmar que quien se presenta a votar sea quien dice ser, a través de biometría dactilar, facial y prueba de vida; así como protocolos criptográficos que aseguren la separación de los datos del votante y del voto emitido, ya que se debe mantener la secrecía del voto, el cual no debe quedar relacionado con los datos de quien lo emitió.

Ya que se debe asegurar la precisión del proceso, se tiene que cifrar la transacción para evitar que pueda ser alterada y para contribuir a la transparencia en el conteo y los resultados de la votación[39], aunque existen plataformas desarrolladas para llevar a cabo este tipo de procesos que cumplen con las garantías electorales de mantener la privacidad y el anonimato.

Cabe destacar que la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE.UU., país que en 2016 posibilitó que 80 millones de personas votaran electrónicamente, realizó en 2020 un estudio para evaluar el riesgo cibernético de la infraestructura electoral, encontraron varios problemas con el sistema de votación electrónica de ese país que deben tenerse en cuenta.

Concluyeron que, si bien sus sistemas electorales integran infraestructuras y controles de seguridad, todos son potencialmente vulnerables a los ataques cibernéticos sofisticados, y aunque el riesgo es bajo, se deben tener planes de control y respuesta a incidentes porque las campañas de desinformación, en conjunto con los ataques cibernéticos, pueden entorpecer los procesos electorales y debilitar la confianza del público en los resultados de las elecciones[40].

Como se mencionó con anterioridad, en México se están implementado sistemas para votaciones electrónicas, por lo que se está a tiempo de aprender de las experiencias de otros países para ofrecer a los ciudadanos confiabilidad y certeza en la utilización de herramientas digitales para la votación, asegurando que el voto sea libre, secreto, individual, personal e intransferible[41].

Para ello, es imprescindible prevenir todo tipo de vulnerabilidades, tanto en el proceso como en los equipos de las casillas en donde se lleva a cabo la votación adoptando las mejores prácticas, implementación de controles, planes de contingencia, y auditorías previas a los sistemas para verificar su buen funcionamiento. Cabe mencionar que estas herramientas existen y se pueden conocer en foros como Infosecurity Mexico. Vale la pena actualizarse.

# # #

Acerca de Infosecurity Mexico
Es el evento más importante del sector de ciberseguridad y seguridad de la información en el que se ofrece acceso a tendencias, conferencias y workshops de la mano de expertos.

Acerca de RX
RX está en el negocio de construir negocios para individuos, comunidades y organizaciones. Elevamos el poder de

[39] https://bit.ly/42YAuiM
[40] https://bit.ly/42Nuzxd
[41] https://bit.ly/2F8kNdk

los eventos cara a cara combinando datos y productos digitales para ayudar a los clientes a conocer los mercados, obtener productos y completar transacciones en más de 400 eventos en 22 países, en 43 industrias.
En RX nos apasiona generar un impacto positivo en la sociedad y estamos totalmente comprometidos con la creación de un entorno de trabajo inclusivo para toda nuestra gente. RX es parte de RELX Group, proveedor global de información basada en análisis y herramientas de decisión para clientes profesionales y de negocios. www.rxglobal.com

Acerca de RELX
RELX es un proveedor global de analítica basada en información y herramientas de decisión para clientes profesionales y de negocio. El Grupo sirve a clientes en más de 180 países y tiene oficinas en alrededor de 40 países. Emplea a más de 33,000 personas, de las cuales, cerca de la mitad se encuentran en Norteamérica. Las acciones de RELX PLC, la empresa matriz, son negociadas en las bolsas de valores de Londres, Ámsterdam y Nueva York, utilizando los símbolos: Londres: REL; Ámsterdam: REN; Nueva York: RELX. La capitalización de mercado es de aproximadamente £ 33 mil millones, € 39 mil millones, $ 47 mil millones*.
*Nota: La actual capitalización de mercado se puede encontrar en: http://www.relx.com/investors

Para mayor información:
Jorge Morales García
Agencia Communika
T: +52 55 1795 2790
E: jorgem@communika.com.mx

Infosecurity Mexico confirma las fechas de su próxima edición en octubre

- Se trata de la exhibición de tecnología, talleres y conferencias relacionadas con la ciberseguridad

CDMX, mayo, 2023.- Infosecurity Mexico, el evento que reúne a la comunidad de profesionales de la ciberseguridad y de la seguridad de la información, confirmó la fecha de su edición 2023, que será el 4 y 5 de octubre en su tradicional sede del Centro Citibanamex, de la Ciudad de México.

"En un mundo digital cada vez más conectado, la ciberseguridad es crítica para la protección de datos y la continuidad del negocio. Infosecurity México se mantendrá como el evento líder que muestra todas las herramientas para la prevención y protección de los entornos tecnológicos. Igualmente, la educación y el contenido académico que presentaremos seguirán siendo parte de la mejor defensa contra las amenazas cibernéticas", explicó Luis Zúñiga, director del evento.

Como referencia, Infosecurity Mexico, organizado por RX, recibió en su última edición a más de mil 500 asistentes, quienes empezaron a regresar a los eventos presenciales. Igualmente, se presentaron casi 50 proveedores, se programaron más de 120 citas de negocios, y hubo más de 40 conferencias que conformaron su programa académico.

A decir de Luis Zúñiga, el comité organizador espera recibir treinta por ciento más de asistentes, con relación al año pasado, de diversas especialidades relacionadas con la ciberseguridad, dentro de los que se incluye a profesionales de las tecnologías de la información, del sector oficial, de la seguridad de la información, de las telecomunicaciones, consultores y auditores, y del sector educativo.

Para la próxima edición, Infosecurity México ha reunido a un grupo de expertos en ciberseguridad, activos profesionalmente, que participarán en el programa de conferencias y contribuirán en su diseño para asegurar que el conocimiento que se imparta sea de actualidad y de utilidad a los asistentes. Entre ellos se encuentran Ivonne Muñoz, directora de IT Lawyers; Enrique Herrera, CEO de Cyberimox, y Erika Mata, CISO México de Bank of America.

Al grupo de especialistas lo complementan Jorge Osorio, presidente de ISC2; Rhett Nieto, gerente de Estrategia y Riesgos Digitales, de FEMSA; Gabriela Reynaga, directora de Holistics; y Arturo García, IT Security Manager del Banco de México. "Todos conforman un grupo que ya ha colaborado con nosotros en ediciones anteriores, y su próxima participación nos permite garantizar contenido de alto valor para los asistentes", agregó Zúñiga.

A partir de este mes, los visitantes pueden registrarse en www.infosecuritymexico.com para asistir y consultar la información del programa académico, del cual hasta hoy se han confirmado la conferencia "Metodologías y marcos de referencia - Nivel Expert", y los talleres "Ataques de ingeniería social - Nivel en formación", "Mittre Attack - Nivel en formación", "Informática forense - Nivel Expert", "Red team - Penetration testing Nivel Expert", y "Metodologías y marcos de referencia - Nivel Expert".

Igualmente, Infosecurity Mexico ya dio a conocer la información de los pases de entrada. El primero de ellos "Free Pass", incluye acceso al piso de exhibición, a las zonas Infosecurity Coffee y Smart Defense Arena, y permite participar en dos talleres. El segundo pase, "Summit Pass 2 Day", incluye

acceso al piso de exhibición, a las zonas Infosecurity Coffee, Smart Defense Arena, Infosecurity Summit y One 2 One Zone, además de dos talleres, derecho a asistir a la comida de networking, y a recibir un kit de bienvenida, que incluye playera y termo.

“Nuestro tercer pase es el de Summit Pass + Tech Lab, que incluye acceso al piso de exhibición, a las zonas Infosecurity Coffee, Smart Defense Arena, Infosecurity Summit y One 2 One Zone, además de dos talleres exclusivos a elegir, derecho a asistir a la comida de networking, y a recibir un kit de bienvenida, que incluye playera, termo y un USB con herramientas de hacking. En cualquier caso, la información completa estará disponible a partir del 15 de mayo, cuando inicia la preventa. Ya los estamos esperando”, finalizó Zúñiga.

# # #

Acerca de Infosecurity Mexico
Es el evento más importante del sector de ciberseguridad y seguridad de la información, en el que se ofrece acceso a tendencias, conferencias y workshops, de la mano de expertos.

Acerca de RX
RX está en el negocio de construir negocios para individuos, comunidades y organizaciones. Elevamos el poder de los eventos cara a cara combinando datos y productos digitales para ayudar a los clientes a conocer los mercados, obtener productos y completar transacciones en más de 400 eventos en 22 países, en 43 industrias.
En RX nos apasiona generar un impacto positivo en la sociedad y estamos totalmente comprometidos con la creación de un entorno de trabajo inclusivo para toda nuestra gente. RX es parte de RELX Group, proveedor global de información basada en análisis y herramientas de decisión para clientes profesionales y de negocios. www.rxglobal.com

Acerca de RELX
RELX es un proveedor global de analítica basada en información y herramientas de decisión para clientes profesionales y de negocio. El Grupo sirve a clientes en más de 180 países y tiene oficinas en alrededor de 40 países. Emplea a más de 33,000 personas, de las cuales, cerca de la mitad se encuentran en Norteamérica. Las acciones de RELX PLC, la empresa matriz, son negociadas en las bolsas de valores de Londres, Ámsterdam y Nueva York, utilizando los símbolos: Londres: REL; Ámsterdam: REN; Nueva York: RELX. La capitalización de mercado es de aproximadamente £ 33 mil millones, € 39 mil millones, $ 47 mil millones*.
*Nota: La actual capitalización de mercado se puede encontrar en: http://www.relx.com/investors

Para mayor información:
Jorge Morales García
Agencia Communika
T: +52 55 1795 2790
E: jorgem@communika.com.mx