10 tendencias a considerar en el 2022 sobre Riesgos & Seguridad Cibernética

Mayo 2022

Este documento es una traducción, para leer el artículo original da clic aquí. https://lnkd.in/e_9mgAsa

LOCKTON®

A lo largo del 2021, los organismos públicos y privados siguieron sintiendo el enorme impacto de un panorama siempre cambiante de amenazas cibernéticas, mientras que seguían bajo la inmensa presión de la incesante pandemia. En el arranque del 2022 van a continuar algunos de los mismos temas que en el 2021, pero ahora están saliendo a la luz nuevos retos en cuanto a riesgos cibernéticos y de seguridad que seguramente se van a materializar.

A continuación, algunas de las principales tendencias que estaremos monitoreando en lo que resta del año.

1 NO CESAN LOS CASOS DE SECUESTRO DE DATOS

El secuestro de datos dominó el panorama de amenazas durante el 2021. El ataque, enfocado asociado a una creciente sofisticación por parte de los autores de amenazas, resultó en grandes pérdidas para las aseguradoras y organizaciones alrededor del mundo.

Durante los primeros seis meses del 2021, la Red contra Crímenes Financieros del Departamento de Tesorería de los Estados Unidos reportó $590 millones de dólares en actividad sospechosa relacionada con el secuestro de datos. Al mismo tiempo, el Centro Nacional de Seguridad Cibernética (NCSC por sus siglas en inglés), en el Reino Unido, reportó que tan sólo en los primeros cuatro meses del 2021 manejó el mismo número de incidentes de secuestro de datos registrados en el 2020, que es tres veces el número de casos que enfrentó la NCSC durante 2019.

Los autores de amenazas han mostrado que continuamente están perfeccionando sus habilidades y no hay ninguna indicación de que esto vaya a disminuir en 2022. La creciente sofisticación de los autores de amenazas puede llegar a infringir un daño tan grande que el potencial de hacer dinero disminuye. Por lo tanto, los infractores por lo general van a buscar un equilibrio entre infringir el daño y asegurar grandes recompensas.

El grupo de infractores también va a crecer con el concepto de “secuestro-como-servicio”, expandiendo así su campo de acción y alcance. Al principio, el autor de amenazas de menor importancia empieza a una escala muy pequeña, pero a lo largo del tiempo va mejorando sus habilidades como extorsionador y creciendo su actividad criminal.

La encriptación y exfiltración de datos han resultado ser rentables en años recientes. Algunos infractores están buscando cómo incrementar su apuesta. Y es que organizaciones que de otra forma podrían recuperar sus datos a través de un respaldo y permanecer indiferentes a la divulgación de datos exfiltrados, ahora deben ponerse a pensar cómo responder cuando los autores de amenazas buscan extorsionar a sus clientes, proveedores y asociados y/o lanzar ataques distribuidos de negación-de-servicio (DDoS por sus siglas en inglés) que ocasionan un caos en las redes al inundarlas con tráfico en internet.

El secuestro de datos enfocado a la industria de la salud no es nada nuevo y no podemos negar su capacidad para impactar el cuidado del paciente. Sin embargo, en el otoño del 2021 se reportó que habían interpuesto una demanda alegando la muerte de un bebé debido a un ataque de secuestro de datos. Estos continuos ataques en la industria de la salud pueden resultar en el incremento de reclamaciones por pérdidas, alegando un cuidado impropio e insuficiente debido a incidentes de ciberseguridad.

El riesgo y la exposición a ataques de secuestro de datos va a seguir desarrollándose, se hará más sofisticado y causará un daño substancial en el sector público y privado. Las organizaciones necesitan permanecer vigilantes en el 2022 y más allá.

2 ACELERAR LA ACTIVIDAD REGULATORIA

Cuando la Unión Europea adoptó en 2016 la Regulación General para Protección de Datos fue un hecho revolucionario, se trataba de una ley de protección a la privacidad, la primera en su tipo. Todavía hoy en día los Estados Unidos no tienen una ley de protección a la privacidad a nivel nacional, aunque algunos Estados – incluyendo California, Colorado y Virginia – han promulgado leyes muy completas de protección a la privacidad. La presión por parte de miembros del público, la comunidad empresarial y agencias gubernamentales para que los legisladores se enfoquen a riesgos y seguridad cibernética los va a mantener ocupados durante el 2022.

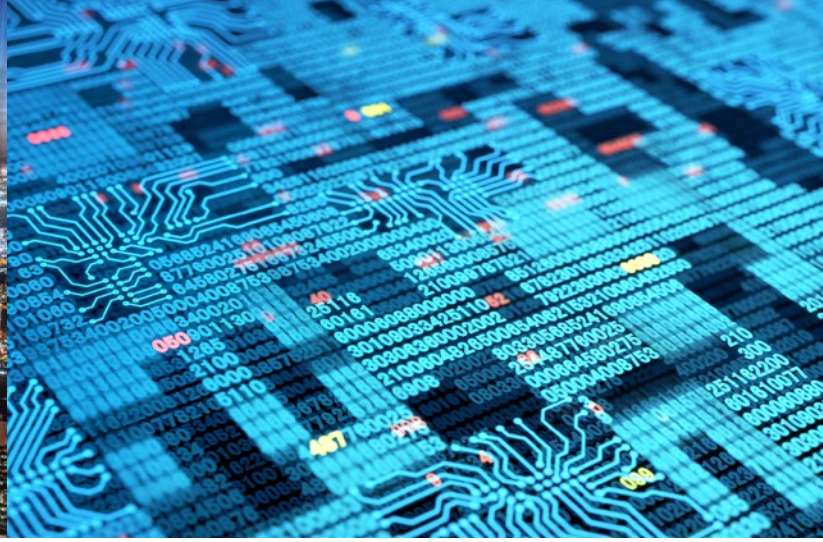
A nivel federal, la Ley de Reporte de Incidentes Cibernéticos, introducida en el 2021, propone establecer una Oficina de Revisión de Incidentes Cibernéticos dentro de la Agencia de Seguridad Cibernética e Infraestructura (CISA por sus siglas en inglés) para recibir, acumular y analizar reportes de incidentes cubiertos. Los incidentes cubiertos deben ser reportados dentro de las siguientes 72 horas de que una entidad cubierta crea razonablemente que ha ocurrido un incidente cubierto. Este proyecto de ley también impondría otros requerimientos de reporte inmediato.

A nivel internacional, el 2021 pudo ver la entrada en vigor de una Ley de Protección a Información Personal en China, las penalizaciones que impone Le Geral de Protecao de Dados Pessoais en Brazil y la decisión final de los Estados Unidos de implementar las cláusulas contractuales estándar. A finales del 2021 el Parlamento y Consejo Europeo acordaron un borrador de la Ley de Gobernabilidad de Datos (DGA por sus siglas en inglés) la cual "busca incrementar la confianza en compartir datos, crear nuevas reglas para la Unión Europea sobre la neutralidad de mercados de datos y facilitar la reutilización de ciertos datos que están en manos del sector público". Es probable que en el 2022 se adopte la DGA.

El tamaño y alcance de la actividad regulatoria probablemente continue creciendo en el 2022, quizá veamos la introducción de nuevas regulaciones, así como enmiendas, regulaciones de apoyo, ajustes y asesorías relacionadas con muchas de estas leyes que recientemente se promulgaron. Conforme estas nuevas leyes e iniciativas entren en vigor, se incrementará su aplicación, así como los litigios relacionados con las leyes de protección a la privacidad y el acudir a las cortes para la interpretación del significado y la forma en que estas leyes se están aplicando.

ALGUNAS INICIATIVAS FEDERALES EN ESTADOS UNIDOS DURANTE EL 2021 INCLUYEN:

- Orden Ejecutiva 14028. Mejorar la Ciberseguridad de la Nación requiere entre otras cosas que los proveedores de servicio compartan información acerca de amenazas cibernéticas que pudieran afectar las redes del gobierno.
- Una asesoría actualizada por parte de la Oficina de Control de Activos Foráneos del Departamento de Tesorería acerca de sanciones que potencialmente pudieran ser impuestas por facilitar el pago por secuestro de datos.
- Nuevos manuales de respuesta a incidentes y vulnerabilidad lanzados por CISA.
- La Iniciativa Civil de Fraude Cibernético del Departamento de Justicia, que se enfocará al fraude relacionado con la ciberseguridad por contratistas del gobierno y becarios.



3 RETOS PERSISTENTES DEL SERVICIO EN LA NUBE

Conforme un mayor número de organizaciones transitan hacia soluciones basadas en la nube para apoyar sus operaciones e infraestructura de redes, los autores de amenazas van a buscar la forma de explotar e infiltrar ese tipo de soluciones. Y en 2022 no serán pocos los retos a la ciberseguridad asociados con la nube.

Una simple falla en la configuración o permisos inadecuados dejan a los sistemas basados en la nube vulnerables a ataques por parte de autores de amenazas. El dejar abierto los puertos o almacenar credenciales de administración y claves de encriptación en un ambiente inseguro en la nube es la oportunidad perfecta para que los autores de amenazas tengan acceso a datos y activos críticos de la organización.

El uso de ambientes en múltiples nubes también puede crear oportunidades para que se haga uso de datos e información. Los ambientes en múltiples nubes requieren que los responsables de información tecnológica y funciones de seguridad entiendan lo complejo de un ambiente en más de una nube y se aseguren de que existe un programa de seguridad dirigido a los distintos ambientes.

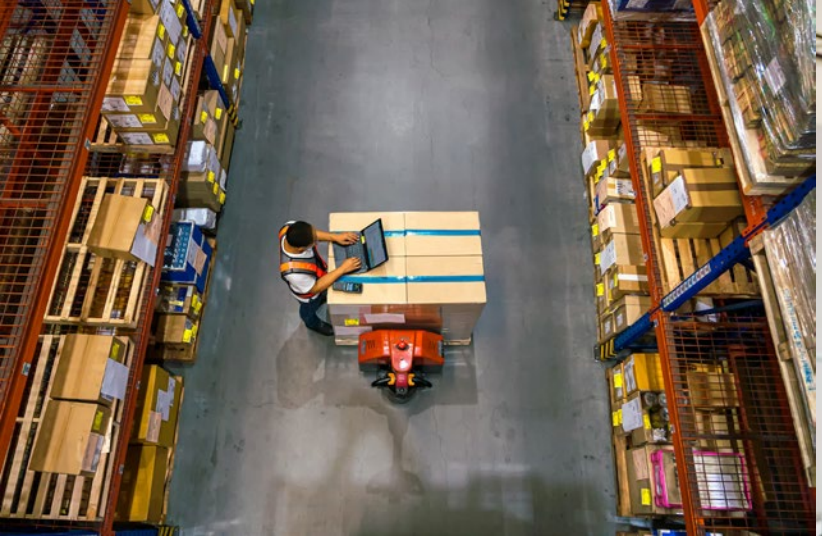
Algunas organizaciones ven que moverse a una solución basada en la nube es una forma de liberarse y no tener que involucrarse en la seguridad. “El proveedor de la nube se encargará de eso, ¿correcto?”. Es una forma de pensar equivocada. Mientras que el proveedor de la nube ofrece determinada seguridad, el asegurar que se implementen medidas adicionales de seguridad para proteger su patrimonio sigue siendo responsabilidad de la organización que está utilizando la solución en la nube.

4 CRECIENTES AMENAZAS EN TECNOLOGÍA OPERACIONAL

Con la transformación digital llegó el punto de convergencia de la tecnología operacional (TO) con la tecnología de la información (TI). Antes de la era digital, las personas monitoreaban las máquinas y los sistemas, pero ahora los sensores y dispositivos monitorean, rastrean y automatizan, se utiliza hardware y software para manejar tanto el equipo operacional como los sistemas. Los sectores con infraestructura crítica como son el energético, industrial, manufacturero, de logística, gas y petróleo, telecomunicaciones y administración de luz y agua dependen fuertemente en la TO.

Los criminales cibernéticos buscan atacar los ambientes TO, como intentaron hacerlo en la planta de tratamiento de agua en Oldsmar, Florida a principios del 2021. En ese incidente uno de los autores de amenazas logró tener acceso a la tecnología operacional en la planta e intentó envenenar el agua utilizada por miles de residentes de la población. Afortunadamente, el ataque fue detenido antes de que el agua quedara contaminada.

Se pueden pasar por alto las vulnerabilidades dentro de los ambientes de TO, ya que muchas organizaciones actualmente se enfocan a mejorar los ambientes tradicionales de la TI y a reforzar esas defensas. En 2022 ya no se pueden ignorar los ambientes TO.



5 LAS CADENAS DE SUMINISTRO ESTÁN EN RIESGO

Ataques enfocados a distintas cadenas de suministro han creado un caos masivo para el sector público y privado por igual. Aunque el asalto se enfoque a una sola organización, el resultado afecta de manera substancial, ya que muchos otros dependen de la organización que ha sido blanco del ataque.

En 2021 varias interrupciones importantes en las cadenas de suministro fueron atribuidas a una seguridad cibernética comprometida, incluyendo aquellas en Kaseya, un proveedor de TI y administración de soluciones de seguridad; Colonial Pipeline, un operador de ductos de petróleo y gas; y JBS Foods, un proveedor de alimentos.

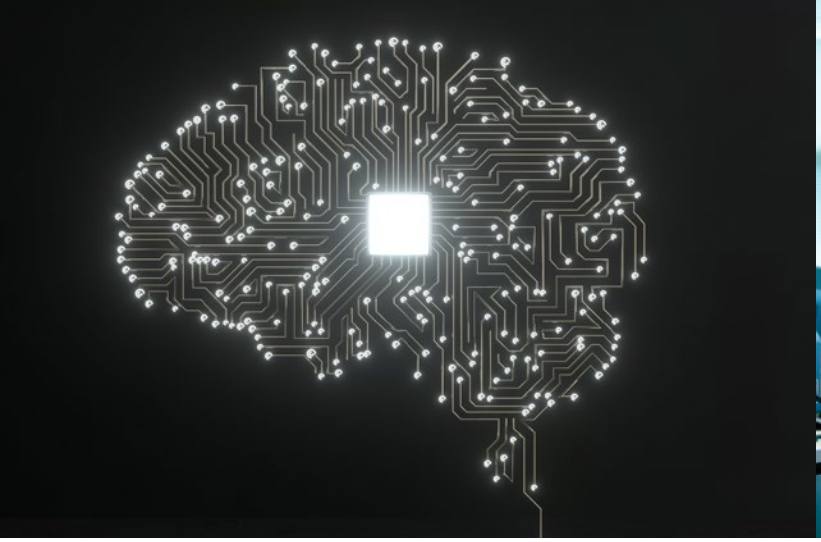
Los autores de amenazas van a seguir desplegando esta estrategia que ya ha demostrado ser muy rentable, las interrupciones en la cadena de suministro van a continuar a lo largo de todo el 2022.

6 ESCASEZ DE TALENTO EN MATERIA DE CIBERSEGURIDAD

El reclutamiento y retención de especialistas en ciberseguridad para afrontar los retos que presenta el actual ambiente de amenazas cibernéticas será un reto muy significativo en el 2022.

Hasta el año 2021, se estimaba que había 4.19 millones de profesionales en ciberseguridad alrededor del mundo, un incremento de más de 700,000 desde el 2020, de acuerdo con un estudio del Grupo de Trabajo en Ciberseguridad del Consorcio 2021, elaborado por Sistema Internacional de Información para la Certificación en Seguridad. A pesar del rápido crecimiento de la fuerza de trabajo en ciberseguridad, el estudio también indica que “la demanda global de profesionales en ciberseguridad sigue sobrepasando la oferta”. Esto ha resultado en un hueco en la fuerza de trabajo en materia de ciberseguridad.

Además, la ciberseguridad ya no es un riesgo de tecnología de la información o de seguridad de la información, es un riesgo de gobernabilidad empresarial. Las organizaciones no sólo necesitan hacer una fuerte inversión en el reclutamiento, capacitación y retención de una fuerza de trabajo con experiencia y amplios conocimientos en materia de tecnología de la información y seguridad de la información, sino que también necesitan atraer y retener talento con capacidad para apoyar las metas y objetivos de ciberseguridad de la organización.



7 DEPENDENCIA EN APRENDIZAJE AUTOMATIZADO E INTELIGENCIA ARTIFICIAL

Muchas organizaciones se están inclinando hacia o considerando el uso de soluciones automatizadas: inteligencia artificial y machine learning (aprendizaje automatizado) para apoyar las funciones operacionales y del negocio. Algo de esto parece haber sido impulsado por la pandemia de COVID-19.

Mientras que la automatización y aprendizaje automatizado han estado presentes desde hace mucho tiempo, son tecnologías relativamente nuevas para los usos tan sofisticados que se les está dando. Con la tecnología moderna, pueden surgir problemas con la codificación, mala configuración, pruebas insuficientes y conflictos con otros sistemas y plataformas.

Mientras más y más organizaciones se mueven hacia soluciones automatizadas o están considerando hacerlo, los riesgos de ciberseguridad asociados con estas tecnologías deben ser administrados de manera muy apropiada y efectiva. Las organizaciones también deben entender que la eficiencia y el ahorro en costos que hacen que el aprendizaje automatizado y la inteligencia artificial resulten tan atractivos, también llevará a los autores de amenazas a utilizar las mismas tecnologías.

8 MAYOR CONCIENTIZACIÓN EN CIBERSEGURIDAD & CULTURA

Es difícil cuantificar en cifras el daño que han causado los autores de amenazas a lo largo de los últimos años, pero el impacto negativo que estos ataques han tenido en las personas, empresas privadas y entidades públicas es inmenso.

Un posible impacto positivo del actual ambiente de riesgo cibernético es la mayor concientización sobre la necesidad de actuar de manera diligente, contar con estrategias de administración de riesgo y resiliencia empresarial. En una encuesta del 2021, Gartner encontró que el 88% de los consejos de administración ven ahora a la ciberseguridad como un riesgo para el negocio, un incremento del 58% comparado con 2016.

Con un mayor cumplimiento de las obligaciones y mucha más atención por parte de los medios acerca de la ciberseguridad, los individuos, organizaciones privadas y entidades gubernamentales seguirán tomando medidas mucho más significativas para mejorar su concientización sobre el ambiente de amenaza cibernética y desarrollar resiliencia, ya que no pueden darse el lujo de no hacerlo.

9 MAYOR COLABORACIÓN ENTRE LOS SECTORES PÚBLICO Y PRIVADO

Históricamente la cibernética ha sido considerada como un problema de TI, pero un reporte recientemente publicado por el Consejo Internacional de J.P. Morgan destacó que "la cibernética es el arma más poderosa del mundo, desde el punto de vista político, económico y militar". Combatir y mitigar este riesgo solo puede lograrse a través de una responsabilidad compartida.

Mientras que en los últimos años el gobierno federal de alguna forma ha promovido el colaborar y compartir información, incluyendo la Ley para Compartir Información sobre Ciberseguridad del 2015, han habido desarrollos significativos en 2021 llevando este llamado a nuevas alturas.

En mayo, el Presidente Biden emitió una orden ejecutiva que dejaba en claro la necesidad de colaborar y compartir información cuando se trate de inteligencia en cuestión de amenazas. Posteriormente, en agosto, se reunió con líderes del sector privado (incluyendo la industria de tecnología, de servicios financieros, energía y agua, educación y aseguradoras) para discutir la necesidad de hacer frente a las amenazas en ciberseguridad.

Seguramente en el 2022 veremos un llamado más fuerte a la colaboración entre el sector público y privado, así como dentro de las industrias y los distintos tipos de negocios. Una organización o industria por sí sola no podrá combatir los riesgos cibernéticos, necesita haber colaboración a lo largo y ancho de sectores, entre la empresa privada y la pública y más allá de las fronteras.

"La cibernética es el arma más poderosa del mundo desde el punto de vista político, económico y militar"

— CONSEJO INTERNACIONAL DE J.P. MORGAN

10 CONDICIONES TENSAS EN EL MERCADO DE SEGUROS

Quienes ya tienen una póliza o aquellos prospectos que desean adquirir un seguro podrán ver que el mercado de seguro cibernético seguirá presionado en 2022.

La alta frecuencia y severidad substancial de reclamaciones, así como una mayor aplicación de la legislación y regulación, han ocasionado que los mercados de seguro cibernético requieran de ciertos controles mínimos para calificar para un seguro, limitar la cobertura y reducir la capacidad y los límites, además de solicitar de manera indispensable la participación del asegurado en la potencial pérdida por medio de coaseguros que oscilan entre 25% y hasta 50%. Las aseguradoras no han mostrado ningún indicio de que las primas y el escrutinio de reaseguro se vaya a moderar en 2022.

Sin embargo, están surgiendo nuevos participantes en el mercado de seguros en jurisdicciones con mayor sofisticación como Reino Unido o Estados Unidos, dando cierto viso de capacidad adicional en el mercado. Cada aseguradora tiene su propia propuesta de valor y está tratando de hacer olas en el mercado de seguros cibernético con algunas estrategias, incluyendo:

1. Un mejor análisis, demostrando las debilidades en controles;
2. La automatización de ciertos procesos de reaseguro y reclamaciones;
3. Desarrollo de resiliencia cibernética para quienes tienen una póliza desde el inicio de su relación con la aseguradora.
4. Servicios de prevención de pérdida como cursos de phishing a empleados y análisis de puertos abiertos en la red pública de las compañías.

Sin embargo, la necesidad de contar con estrictos controles no va a cambiar y la expectativa en costos continuará al alza, replicando las estrategias globales de las compañías de seguros.

Para más información puedes ponerte en contacto con la Práctica Global de Lockton en Cibernética y Tecnología en cyber@lockton.com

También puedes contactar a Ricardo Millán Gerente de Líneas Financieras en Lockton México:

ricardo.millan@lockton.com

SABÍAS QUE...

- En los últimos 12 meses, el costo promedio por cada dato expuesto fue de USD$250.
- El costo promedio en 2021 de infracciones regulatorias se incrementó a USD$4.2 millones.
- Las empresas necesitan 287 días en promedio para identificar y responder a un ataque cibernético.
- El costo promedio de brechas de seguridad aumentaron a USD$4.2 millones, y en Estados Unidos ascendió a USD$9 millones.
- Por cada registro perdido o robado de información personal identificable se pagan USD$180.
- 20% de las brechas de seguridad son ocasionadas por credenciales comprometidas.
- Los costos promedios por ransomware ascienden a USD$4.6 milllones, sin contar el pago de rescate.
- Las brechas de seguridad donde el trabajo remoto fue el factor causante, el costo promedio fue de USD$4.9 millones.

FUENTE
https://www.ibm.com/downloads/cas/DJ4Z5MYX

UNCOMMONLY INDEPENDENT

