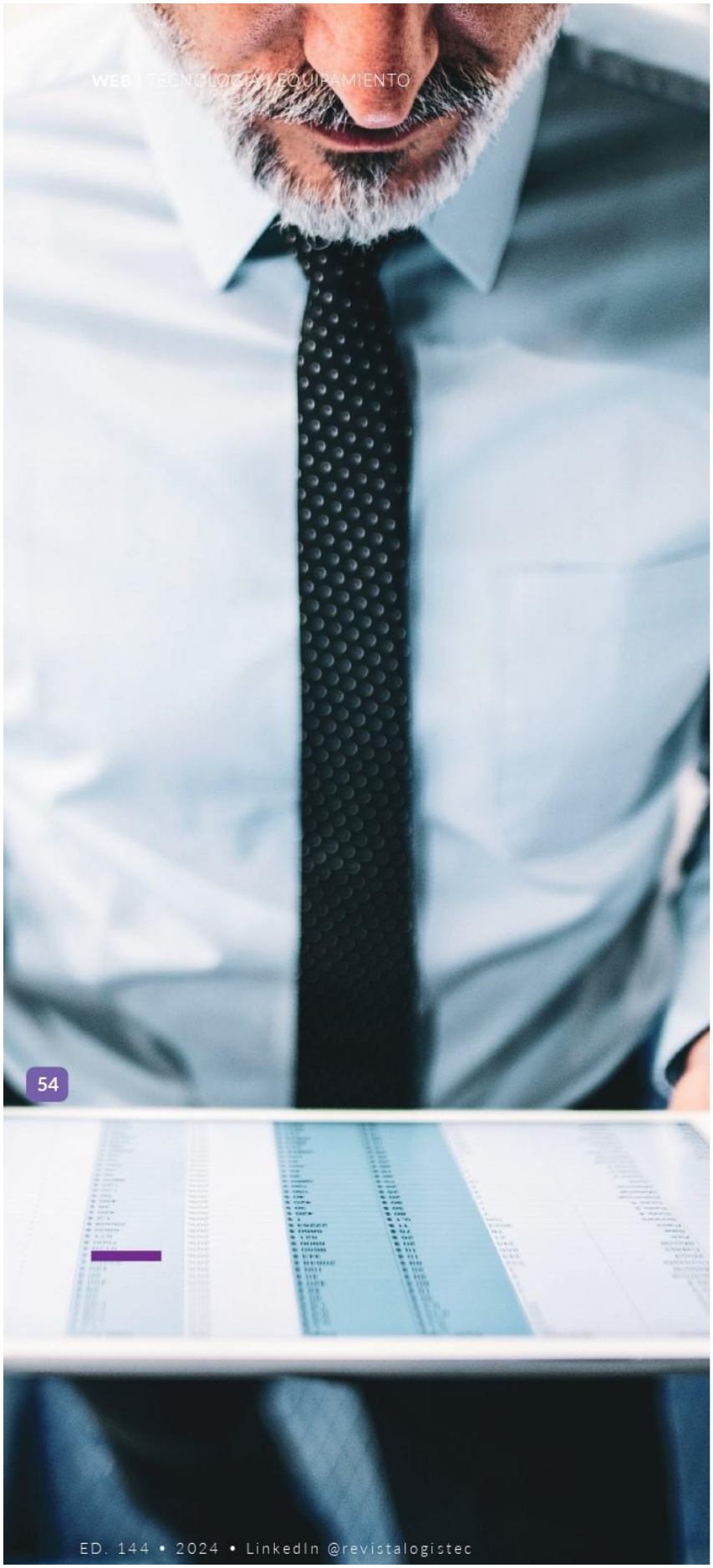
LITORALPRESS

Fecha: 21-10-2024
Medio: Revista Logistec
Supl. : Revista Logistec
Tipo: Actualidad
Título: CIBERSEGURIDAD: EL TALÓN DE AQUILES EN LA TRANSFORMACIÓN DE SUPPLY CHAIN

Pág. : 56
Cm2: 532,0
VPE: $ 759.116

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: Positiva



CIBERSEGURIDAD: EL TALÓN DE AQUILES EN LA TRANSFORMACIÓN DE SUPPLY CHAIN

IMAGINA QUE TU CADENA DE SUMINISTRO ES UNA GRAN AVENTURA, DONDE CADA PAQUETE VIAJA POR UN LABERINTO GLOBAL DE ALMACENES, CAMIONES Y BARCOS, ENFRENTANDO DESAFÍOS Y OBSTÁCULOS EN SU CAMINO. PERO, AL IGUAL QUE EN TODA BUENA HISTORIA, HAY VILLANOS OCULTOS AL ACECHO: LOS CIBERATAQUES. ESTOS HACKERS Y AMENAZAS DIGITALES SON COMO LOS PIRATAS MODERNOS, BUSCANDO INFILTRARSE EN TUS SISTEMAS, ROBAR INFORMACIÓN Y CAUSAR CAOS. ¿EL HÉROE DE ESTA HISTORIA? LA CIBERSEGURIDAD.

A medida que la tecnología revoluciona el transporte y la logística, las amenazas también evolucionan. Los delincuentes no buscan solo interceptar un camión; ahora intentan capturar tus datos y sabotear tus operaciones desde la comodidad de su teclado. La ciberseguridad, entonces, se convierte en ese escudo invisible que protege cada eslabón de tu cadena de suministro. Ya no se trata solo de mover productos de un punto A a un punto B, sino de hacerlo de manera segura y blindada contra los piratas cibernéticos.

Ante esta realidad, que afecta a grandes, medianas y pequeñas compañías, la ciberseguridad es una disciplina que ha cobrado creciente relevancia en las últimas décadas, debido al aumento exponencial del uso de tecnologías digitales y la conectividad global. Su propósito es proteger los sistemas informáticos, redes, dispositivos y datos de ataques maliciosos, accesos no autorizados y otros riesgos

LITORALPRESS

Fecha: 21-10-2024
Medio: Revista Logistec
Supl. : Revista Logistec
Tipo: Actualidad
Título: CIBERSEGURIDAD: EL TALÓN DE AQUILES EN LA TRANSFORMACIÓN DE SUPPLY CHAIN

Pág. : 57
Cm2: 506,8
VPE: $ 723.178

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: Positiva

cibernéticos. Los inicios de la ciberseguridad están intrínsecamente ligados al desarrollo de la informática y la conectividad en red. El primer evento que podría considerarse un hito en la historia de la ciberseguridad ocurrió en los años 70, con la aparición de Creeper, el primer virus informático. Este malware fue creado como un experimento por Bob Thomas, quien trabajaba en BBN Technologies, para ver si un programa podía moverse entre computadoras conectadas por la red ARPANET, la precursora de Internet. Aunque Creeper no era malicioso, provocó que se desarrollara el primer antivirus, llamado Reaper.

Sin embargo, fue durante la década de los 80 cuando la preocupación por la seguridad informática comenzó a tomar forma. Uno de los casos más emblemáticos fue el gusano de Morris en 1988. Creado por Robert Tappan Morris, el gusano se extendió rápidamente por Internet, afectando alrededor del 10% de las computadoras conectadas en aquel entonces. Este incidente subrayó la vulnerabilidad de las redes y provocó que el gobierno estadounidense comenzara a desarrollar regulaciones más estrictas en torno a la seguridad en línea.

Por tanto, la ciberseguridad es una disciplina en evolución. Con la creciente interconexión de dispositivos en la era del Internet de las Cosas (IoT), las Smart city y la expansión del 5G, los retos de la seguridad cibernética se expanden hacia nuevos horizontes. Los ataques serán más complejos y dirigidos, lo que obliga a una colaboración más estrecha entre gobiernos, empresas y expertos en ciberseguridad para proteger los ecosistemas digitales globales.

COSTOS DE UN ATAQUE PREMEDITADO

La ciberseguridad se ha convertido en una prioridad estratégica para las empresas de todo el mundo, ya que el entorno digital crece exponencialmente y, con él, las amenazas cibernéticas. Los ataques no solo comprometen la seguridad de los datos, sino que también generan graves impactos económicos.

Los costos relacionados con la ciberseguridad van más allá de la simple implementación de medidas de protección: involucran pérdidas por brechas de seguridad, daño reputacional, sanciones legales y la inversión en herramientas y personal especializado.

Cuando una empresa es víctima de un ciberataque, los efectos financieros pueden ser devastadores. Estos costos se dividen en varios componentes: pérdida de datos y recuperación, pérdida de ingresos por interrupciones operativas, costos legales y sanciones, daño reputacional y costos de mitigación post-ataque.

Si llevamos estas situaciones a la industria logística sus efectos pueden ser críticos, sobre todo, si afecta la continuidad de las operaciones. A la luz de estos riesgos, muchas empresas invierten en medidas preventivas para evitar ser víctimas de ciberataques. Sin embargo, estas inversiones también representan un costo considerable, tal como lo dejó en evidencia el reporte anual Costo f Data Breach de IBM que reveló que el costo promedio por filtraciones de datos en 2024 en Latinoamérica es de US 2,76 millones, a medida que las filtraciones se vuelven más disruptivas y aumentan aún más las demandas de los equipos de ciberseguridad.

Según el estudio, las empresas de los sectores industrial y financiero experimentaron las filtraciones más costosas de la región, con costos promedio de US 3,54 millones y US 3,22 millones, respectivamente. Los ataques de phishing fueron el vector inicial de ataque más común, representando el 16% de los incidentes y un costo promedio de US $2,91 millones por filtración. El reporte también muestra que la IA juega un papel crucial en la reducción del impacto de las filtraciones de datos en las organizaciones de Latinoamérica. Los hallazgos evidencian que el 31% de las empresas de la región ahora están usando ampliamente seguridad impulsada por IA y automatización para prevenir y hacer frente a las filtraciones, lo que ha llevado a una reducción en los ciclos de vida. De hecho, las organizaciones con un amplio uso de seguridad impulsada por IA y automatización experimentaron filtraciones que fueron 83 días más cortas en promedio, comparado con quienes no usan estas tecnologías.

"Con la evolución de los ciberataques, las organizaciones no pueden permitirse poner la seguridad en un segundo plano y menos aún, considerando las ventajas que las tecnologías con IA entregan a los equipos de seguridad", dijo Juan Carlos Zevallos, Gerente de IBM Security Software para Latinoamérica.

"La seguridad impulsada por IA y la automatización ayuda a ganar tiempo en el lado de los defensores, sin mencionar que el ahorro de tiempo reduce los costos de las filtraciones y, por ende, las disrupciones en los negocios. Las organizaciones de la región que invierten en seguridad impulsada por IA y automatización están mejor equipadas para detectar y recuperarse de las filtraciones", añadió el ejecutivo.

El reporte también llama la atención sobre la importancia del almacenamiento y la correcta gestión de los datos. En la región, el 43% de las filtraciones involucraron datos almacenados en múltiples entornos y 26% involucraron datos almacenados sólo en la nube pública.

Las filtraciones que involucran varios tipos de entornos también fueron las más costosas de remediar, con un promedio de US $2,94 millones. Según el reporte de 2024, los tres principales factores que ayudan a reducir los costos de las filtraciones de datos en América Latina son los equipos de respuesta a incidentes, los planes/pruebas de respuesta a incidentes y el cifrado.

Otros hallazgos del reporte sobre las filtraciones de datos en 2024 incluyen:

LITORALPRESS

Fecha: 21-10-2024
Medio: Revista Logistec
Supl. : Revista Logistec
Tipo: Actualidad
Título: CIBERSEGURIDAD: EL TALÓN DE AQUILES EN LA TRANSFORMACIÓN DE SUPPLY CHAIN

Pág. : 58
Cm2: 484,4
VPE: $ 691.233

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: Positiva

Las credenciales siguen siendo un problema. En 14%, las credenciales robadas o comprometidas fueron el segundo vector inicial más común, llevando los costos de filtraciones a US 2,89 millones en América Latina. Además, debido a la complejidad de las investigaciones de las filtraciones, los costos de detección y escalada aumentaron un 10% en comparación con el año anterior.

El tiempo es un factor relevante en la región. El ciclo de vida promedio de una filtración es de 301 días. Sin embargo, las empresas que tardaron menos de 200 días en identificar y contener una filtración incurrieron en un costo promedio de US $2,40 millones. Por el contrario, las filtraciones con ciclos de vida mayores a 200 días costaron US $3,12 millones en promedio.

Ricardo Seguel
Director Académico
Magíster de Ciberseguridad de la Facultad de Ingeniería y Ciencia UAI.

La escasez de personal de seguridad incrementó los costos de las filtraciones. El principal factor que amplifica los costos de las filtraciones en América Latina fue la escasez de habilidades de seguridad (en US $167.226), en un momento en que las organizaciones están compitiendo para adoptar tecnologías de IA Generativa, que traerán beneficios, pero también se espera que introduzcan nuevos riesgos para los equipos de seguridad.

Otros factores que contribuyeron al aumento en el costo de filtraciones fueron: no conformidad con la regulación (en US 163.450) y la complejidad de los sistemas de seguridad (en US $146.760).

Los costos de las filtraciones pasaron a los consumidores. El 63% de las organizaciones en el mundo declararon que incrementarían el costo de bienes o servicios debido a una filtración este año (vs. 57% el año pasado). Esto marca el tercer año consecutivo en que las organizaciones estudiadas declararon que tomarían esta acción.

MIRADA DE EXPERTOS

Las cadenas de suministro pueden ser especialmente propensas a las amenazas cibernéticas porque están compuestas por múltiples proveedores, fabricantes y otras organizaciones de terceros. Dado que cada organización suele tener acceso a los mismos datos y sistemas, determinar qué entidad es responsable de un incidente puede resultar difícil. La complejidad de la red de la cadena de suministro también puede dificultar la identificación de vulnerabilidades críticas.

Un ciberataque exitoso en una cadena de suministro puede afectar significativamente las operaciones de una organización. Esto genera contratiempos como interrupciones comerciales, pérdidas monetarias y daños a la reputación. Por eso es fundamental garantizar la seguridad, tal como lo recalcaron los expertos en esta materia, Juan Pablo Arias, gerente de ingeniería de Fortinet y Ricardo Seguel, director académico magíster de ciberseguridad de la Facultad de Ingeniería y Ciencia de la Universidad Adolfo Ibáñez (UAI).

Juan Pablo Arias
Gerente de ingeniería de Fortinet

La ciberseguridad es un desafío clave en la logística y el transporte y así lo entienden los entrevistados. En los últimos años, la ciberseguridad ha pasado de ser un tema lejano, a convertirse en un aspecto central para todas las empresas, especialmente aquellas dentro de una cadena de distribución. Según Juan Pablo "todos somos blancos, independientemente del tamaño de la empresa".

"Esto es especialmente preocupante en industrias como la logística, donde la digitalización avanza a pasos agigantados, exponiendo nuevos riesgos", enfatizó el ejecutivo de Fortinet, quien enfatizó además que los cibercriminales han evolucionado. "Si antes eran exploradores que buscaban "botar páginas" para demostrar su habilidad, hoy los ataques tienen un claro objetivo económico. El ransomware es uno de los ejemplos más comunes de estos ciberataques, secuestrando información crítica y extorsionando a las empresas para liberar los datos. Mientras más digitalices, más vulnerable puedes ser, lo que nos recuerda que el proceso de digitalización debe ir de la mano con inversiones sólidas en ciberseguridad", señaló.

La ciberseguridad en la industria logística aún enfrenta barreras, principalmente por la falta de inversión y conciencia a nivel organizacional. Según Arias, muchas veces se comete el error de delegar la ciberseguridad solo al equipo de TI, cuando en realidad "es un problema de toda la organización. La 'ciberconciencia' debe instalarse en todos los niveles, desde el personal operativo hasta la alta dirección", agregó.

Para abordar estos desafíos, el gerente de ingeniería de Fortinet propone un enfoque basado en tres pilares: tecnología, procesos y personas. En cuanto a la tecnología, es fundamental contar con herramientas modernas como el EDR (Endpoint Detection and Response), que va más allá de los antiguos antivirus. El segundo pilar son los procesos. Las empresas deben tener un plan de continuidad de negocio que les permita reaccionar ante un ataque. "Aunque hagamos una mega inversión en tecnología, nos van a atacar igual", asegura Arias.

Por ello, es crucial que se practiquen simulaciones de ciberataques para estar preparados y saber cómo actuar. Finalmente, el pilar más importante son las personas. Juan Pablo destaca que "el 80% de los ataques de ransomware están asociados al phishing", una práctica que aprovecha la ingenuidad o descuido de los empleados. Todos, desde el personal de base hasta el gerente general, deben estar alineados con las medidas de seguridad, ya

LITORALPRESS

Fecha: 21-10-2024
Medio: Revista Logistec
Supl. : Revista Logistec
Tipo: Actualidad
Título: CIBERSEGURIDAD: EL TALÓN DE AQUILES EN LA TRANSFORMACIÓN DE SUPPLY CHAIN

Pág. : 59
Cm2: 244,9
VPE: $ 349.434

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: Positiva

que "si la gente no está en sintonía con esas medidas, no se saca nada". Por su parte, Ricardo Seguel apunta al desafío estratégico que implica la ciberseguridad para la continuidad operacional, por lo cual -aseguró- esta materia dejó de ser un tema exclusivo de sectores altamente regulados, como la banca o el retail, para convertirse en una prioridad transversal en la industria logística.

Seguel, destacó que las empresas de logística, tanto grandes como pequeñas, se enfrentan a crecientes demandas de seguridad para proteger la continuidad de sus operaciones. Esto es especialmente importante en el contexto de la nueva Ley Marco de Ciberseguridad, que obligará a todas las empresas a cumplir con estrictos requisitos normativos.

Empresas reguladas ya llevan años invirtiendo en ciberdefensa, pero el reto actual recae en las pequeñas y medianas empresas (pymes), que tradicionalmente han sido más lentas en adoptar estas medidas. Sin embargo, proveedores de sectores críticos como la banca y el retail están exigiendo a sus socios comerciales cumplir con estándares de seguridad certificados, lo que ha acelerado la necesidad de que muchas pymes logísticas se pongan al día en términos de ciberseguridad. El director académico del magíster de Ciberseguridad de la UAI recalcó que la ciberseguridad no es solo una cuestión de tecnología, sino un asunto estratégico que involucra procesos, personas y cumplimiento normativo.

"Ciberseguridad es sinónimo de continuidad operacional", afirmó el académico de la UAI, y añadió que las empresas logísticas que no adopten estas medidas podrían enfrentar interrupciones en su operación, lo que afectaría su capacidad de cumplir con contratos, SLA, y en última instancia, podría llevar a la pérdida de clientes. La digitalización también ha incrementado la importancia de proteger las tecnologías operativas, como los sistemas de Internet de las Cosas (IoT) que están conectados en centros de distribución, puertos y flotas de transporte. El riesgo ya no se limita a los sistemas de TI tradicionales, sino que también incluye los dispositivos y sensores en terreno.

Ricardo Seguel advirtió que el primer paso para avanzar en esta dirección es que las empresas, especialmente sus directorios, reconozcan la ciberseguridad como una prioridad estratégica. "Implementar un plan de gobernanza en ciberseguridad y cumplimiento normativo es esencial para garantizar la protección contra amenazas y mitigar los riesgos operacionales en un sector tan crítico como el logístico", recalcó.

Finalmente, es tiempo de que la ciberseguridad se convierta en una prioridad para todos en la industria. Así que, antes de enviar tu próximo cargamento, asegúrate de que tu cadena de suministro esté equipada con el mejor "superhéroe" digital que puedas tener: la ciberseguridad. ■