Negocios conectados: la dependencia digital alimenta el riesgo

QBE

Introducción

Las personas y las organizaciones de todo el mundo dependen cada vez más de las tecnologías digitales. Los ordenadores y las herramientas de inteligencia artificial (IA) están permitiendo y automatizando tareas empresariales tanto sencillas como complejas a medida que los dispositivos inteligentes conectan fábricas, vehículos y otros equipos a Internet.

Los mercados tecnológicos mundiales crecerán exponencialmente en los próximos cinco años. Se prevé que el mercado de la IA como servicio (AIaaS) se multiplique por nueve, y pasaría de unos 200 000 millones de dólares a 1 850 000 millones, el del software como servicio (SaaS) por tres, hasta 850 000 millones, y el de la infraestructura como servicio (IaaS) por cinco, hasta 532 000 millones, lo que demuestra la magnitud de las oportunidades que presentan las tecnologías digitales emergentes.

Sin embargo, los ciberdelincuentes han estado robando datos confidenciales para extorsionar y estafar a empresas de todos los tamaños y sectores, mientras que otros actores maliciosos han estado utilizando la tecnología para perturbar a sus oponentes e impulsar sus narrativas ideológicas.

Perturbación tecnológica mundial

El apagón masivo que afectó a los sistemas que ejecutaban el sensor Falcon de CrowdStrike el 19 de julio ha puesto de manifiesto la interdependencia y vulnerabilidad de los sistemas tecnológicos globales. La interrupción ha costado a las empresas de la lista Fortune 500 unos daños estimados en 5400 millones de dólares y 25 000 millones de dólares en valor de sus acciones, sin incluir a Microsoft.

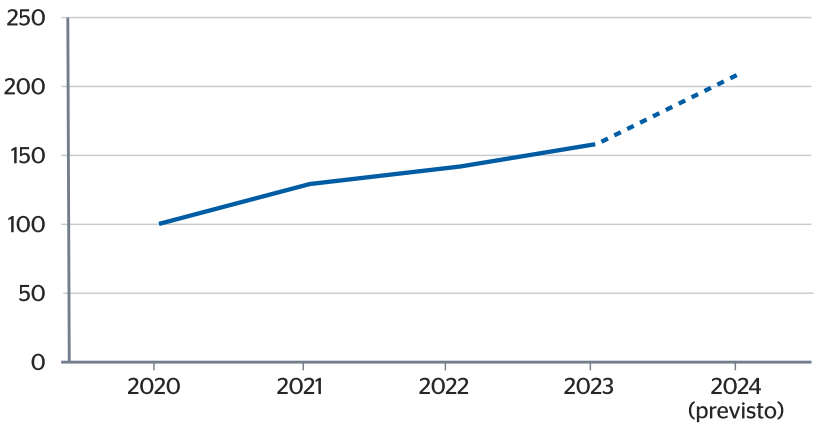
La actualización de contenido defectuosa de CrowdStrike dejó fuera de servicio unos 8,5 millones de ordenadores Windows, menos del 1 % de todos los dispositivos Windows, perturbando industrias en todo el mundo, pero más gravemente la aviación, el transporte y la sanidad. Los ciberdelincuentes aprovecharon la oportunidad para lanzar campañas de phishing con señuelos relacionados con CrowdStrike, buscando comprometer los sistemas, robar datos y extorsionar a las víctimas. En este caso, el incidente de CrowdStrike fue un error más que una perturbación intencionada; sin embargo muchos incidentes cibernéticos son y serán intencionadamente perturbadores.

En junio de 2017, el ciberataque masivo NotPetya tuvo como objetivo organizaciones ucranianas, pero finalmente provocó infecciones en toda Europa, Norteamérica y Asia Pacífico. El malware NotPetya, que se hizo pasar por *ransomware*, afectó a sectores críticos como el transporte, la logística y el sector de los envíos, causando unos daños estimados en 10 000 millones de dólares. Aunque afectó a muchos menos dispositivos que el incidente de CrowdStrike, su naturaleza intencionada provocó un mayor grado de perturbación.

A medida que crecen las interdependencias tecnológicas, esperamos que más incidentes cibernéticos perturben a muchas empresas en un solo ataque, lo que significa que las empresas tienen más probabilidades de experimentar un evento cibernético perturbador. Los actores maliciosos también pueden dirigirse a empresas específicas para causar mayores daños, ya sea extorsionando rescates o desestabilizando a rivales geopolíticos.

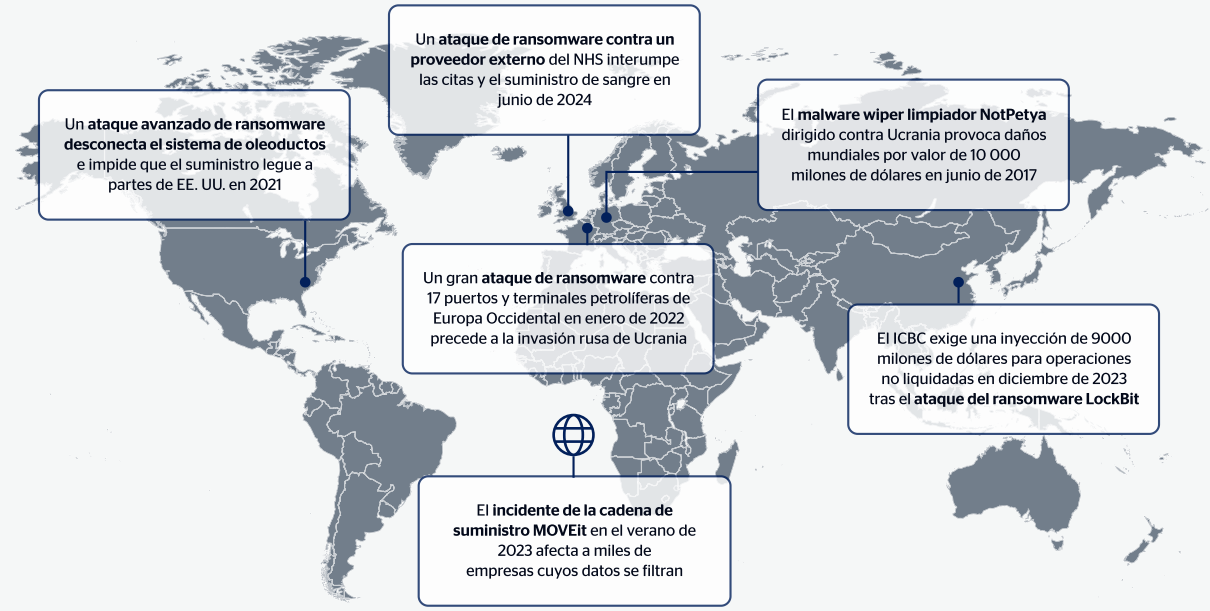
> El incidente de CrowdStrike ha costado a las empresas Fortune 500 un daño estimado en 5,4 mil millones de dólares y una pérdida de 25 mil millones de dólares en valor de acciones.

Número de ciberataques destructivos y alarmantes registrados, desde 2020



Fuente: Control Risks

Incidentes importantes de amenazas cibernéticas desde 2017



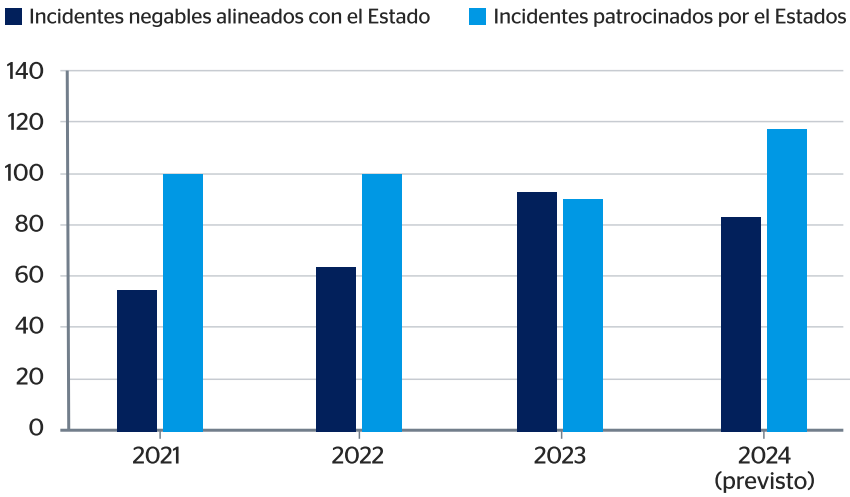
Ataques indirectos

La mayor competencia geopolítica hace que el mundo sea cada vez más multipolar. Los ciberactores vinculados a los Estados tienen cada vez más intención de perturbar las infraestructuras nacionales críticas (CNI), por ejemplo a través de programas *ransomware*. Estos ataques pueden estar impulsados por acontecimientos geopolíticos como los conflictos en curso entre Israel y Hamás o entre Ucrania y Rusia, y manifestarse como ataques cibercriminales o activistas dirigidos por el Estado contra entidades de sectores estratégicos fuera del teatro del conflicto. Las organizaciones del sector energético son objetivos muy atractivos para los ciberataques indirectos, que pueden desestabilizar los mercados financieros y los gobiernos.

Las empresas del sector energético son objetivos muy atractivos para los ciberataques, los cuales pueden desestabilizar mercados financieros y gobiernos.

Algunos estados han destinado recursos para crear y mantener identidades de activistas cibernéticos con el propósito de realizar ataques disruptivos y destructivos, con el fin de mantener una negación plausible, evitando así ser atribuidos o recibir sanciones diplomáticas Las organizaciones CNI son objetivos atractivos para las amenazas indirectas, ya que los actores de las amenazas sienten que pueden perturbarlas sin provocar necesariamente una respuesta. También están proliferando las unidades de espionaje que se hacen pasar por grupos de *ransomware* con motivaciones financieras, lo que refuerza la elevada amenaza vinculada al Estado para la propiedad intelectual sensible y los datos corporativos.

Número de ataques proxy no estatales significativos y campañas registradas vinculadas al Estado, desde 2021



Fuente: Control Risks

Un *ransomware* vinculado a Rusia ataca 17 terminales petroleras europeas antes de la invasión de Ucrania

Una serie de ataques de *ransomware* a gran escala tuvo como objetivo terminales portuarias de Bélgica, Alemania y los Países Bajos en enero de 2022. Los ataques, muy probablemente originados por actores patrocinados por Rusia, inutilizaron los sistemas informáticos, afectando a las operaciones de carga de productos petrolíferos de los puertos. Los ataques se llevaron a cabo tres semanas antes de la invasión rusa de Ucrania, lo que ilustra cómo los ataques indirectos se dirigen a sectores y geografías secundarios.

Los ataques de *ransomware* en 2023 crecieron un 74% respecto a 2022.

Factores de los crecientes incidentes de ciberamenazas

Geopolítica

Las tensiones entre EE. UU. y China, la creciente multipolaridad y los conflictos en curso impulsan el desbordamiento perturbador a escala mundial contra víctimas intencionadas y no intencionadas

Ransomware

Las bandas de ciberdelincuentes son más activas y perturbadoras que nunca, con un mayor volumen de ataques, enormes ingresos y mayores exigencias de rescate

Amenazas de terceros

Los proveedores de infraestructuras, servicios de software, hosts de datos y tecnologías son la primera línea cibernética y, cad a vez más, los objetivos prioritarios

Tecnologia

Los avances de la IA introducen rápidamente nuevos riesgos, mientras que el aumento de la conectividad y la interdependencia aumentan la superficie de ataque en constante expansion.

Control Risks

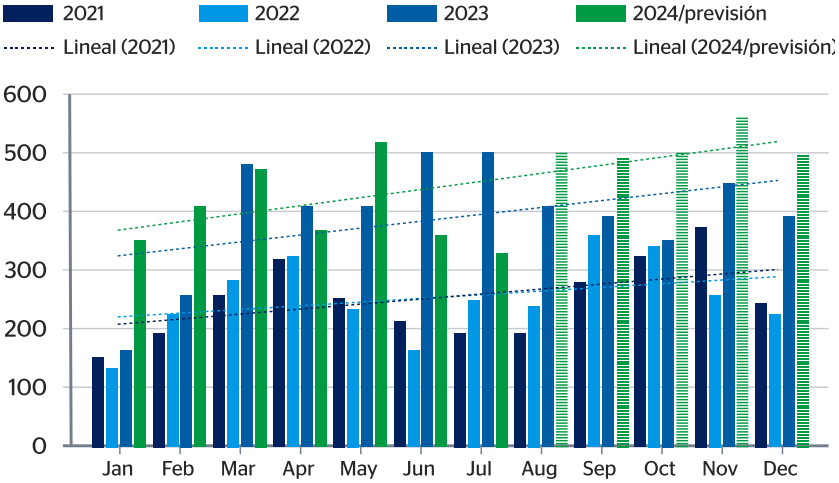
Ransomware

Aumentan los ingresos al incrementarse el número de ataques

Los ataques de *ransomware* en 2023 aumentaron un 74 % respecto a 2022, y el pago total de rescates por parte de las víctimas superó los 1000 millones de dólares en todo el mundo. Después de que las fuerzas del orden acabaran con el grupo Hive en 2022, el ecosistema cibercriminal se fragmentó y se filtró el código del *ransomware*, lo que permitió a grupos de menor capacidad llevar a cabo sus propios ataques.

Este resurgimiento del *ransomware* ha continuado en 2024, con el número de víctimas nombradas públicamente alcanzando los totales mensuales más altos de los últimos tres años *(*nótese que el gráfico de abajo incluye MOVEit, un incidente de 2023 que provocó un alto volumen de víctimas. En términos reales, las cifras de 2024 son significativamente superiores a las de 2023 si no se tiene en cuenta el incidente MOVEit como una anomalía).*

Número de víctimas de ransonware nombradas en sitios de filtración de datos



Fuente: Control Risks

Número de víctimas nombradas públicamente por grupos de extorsión de *ransomware* y filtración de datos

2021	2022	2023	2024 (previsión)	2025 (previsión)
2964	2981	4698	4800	5200

Fuente: Control Risks

Análisis sectorial

Los ataques de *ransomware* se dirigieron en gran medida a los sectores manufacturero, sanitario, informático, educativo y gubernamental en 2023. Como la resistencia varía según los sectores, los atacantes se dirigen cada vez más a todos los sectores verticales, pero se centran en la fabricación y la sanidad, donde la interrupción de las operaciones tiene repercusiones punitivas.

El *ransomware* supone una gran amenaza para las organizaciones de fabricación y producción, ya que el 65 % del sector ha informado de un ataque de *ransomware* en 2023, con un pago medio por rescate de 2,4 millones de USD. Entre las víctimas del sector, el 62 % pagó rescates para recuperar los datos robados.

> Las organizaciones de servicios sanitarios que sufrieron ataques de *ransomware* pasaron de 214 en 2022 a 389 en 2023, lo que implica un aumento del 81.7%.

No se dispone de información suficiente para calcular con precisión la demanda media, ya que esta variará significativamente según las zonas geográficas, los sectores y las organizaciones. Sin embargo, es muy probable que las grandes organizaciones muy vulnerables a las interrupciones operativas se enfrenten a peticiones de rescate de decenas de millones de dólares, y las organizaciones más pequeñas, de cientos de miles. Es probable que las organizaciones que se enfrentan a las mayores peticiones de rescate pertenezcan a los sectores sanitario, gubernamental, de TI y comunicaciones y manufacturero.

Las organizaciones sanitarias también resultan muy atractivas, al igual que las que almacenan grandes volúmenes de información personal identificable (IPI) e información sanitaria protegida (IPS) y las que tienen requisitos críticos de tiempo de actividad. Esta orientación también está impulsada por la percepción de que el sector sanitario tiene una madurez de ciberseguridad comparativamente más débil que otras industrias. El número de organizaciones sanitarias que se enfrentaron a un ataque de *ransomware* aumentó de 214 en 2022 a 389 en 2023, un incremento del 81,7 %.

Caza mayor

Los grupos de *ransomware* utilizan cada vez más tácticas de «caza mayor», identificando a entidades de altos ingresos y perfil para extorsionarlas en sus ataques. La caza mayor permite a los grupos de *ransomware* aumentar el pago medio del rescate mediante exigencias iniciales más elevadas de lo que una pequeña y mediana empresa podría permitirse, así como aprovechar la interrupción de las operaciones de un gran número de clientes o consumidores de estas víctimas.

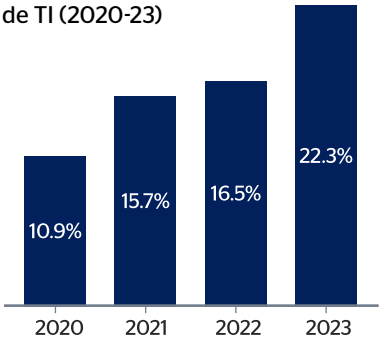
En los últimos años, las fuerzas de seguridad han logrado un mayor éxito en la desarticulación de grupos de *ransomware*, como ejemplifican el desmantelamiento del *ransomware* Hive y los desmantelamientos parciales de los prolíficos grupos LockBit y BlackCat. Por ello, los grupos de *ransomware* han tratado de maximizar el pago de rescates mediante la caza mayor antes de que las fuerzas del orden les den alcance y confisquen sus activos e infraestructuras. El pago medio por rescate en 2023 aumentó a 2 millones de dólares, frente a los 400 000 dólares del año anterior. La media se ha visto significativamente afectada por la caza mayor, ya que algunos actores de la amenaza han exigido más de 50 millones de dólares. Sin embargo, la mediana de la demanda de rescate se ha mantenido igual, en torno a los 300 000 dólares.

Los actores de amenazas también ven a las grandes organizaciones como más propensas a pagar un rescate. Por término medio, el 61 % de las organizaciones con unos ingresos anuales de 5000 millones de dólares pagan rescates tras un ataque, frente al 25 % de las organizaciones con unos ingresos anuales inferiores a 10 millones de dólares. Algunas víctimas con grandes ingresos perciben la interrupción de las operaciones como algo más costoso que pagar un rescate.

El ataque de LockBit al ICBC ilustra la amenaza oportunista del *ransomware* para el sector financiero

En noviembre de 2023, el grupo de *ransomware* LockBit atacó la rama de servicios financieros del Banco Industrial y Comercial de China (ICBC), con sede en Estados Unidos, interrumpiendo las operaciones en el mercado de bonos del Tesoro estadounidense. Esto incluyó el desvío forzoso de operaciones financieras e impidió a ICBC Financial Services liquidar operaciones del Tesoro para otros operadores del mercado, lo que significó que ICBC tuvo que inyectar 9000 millones de dólares a su unidad estadounidense. Es probable que los atacantes se infiltraran en la red del ICBC a través de un equipo Citrix NetScaler sin parches que les permitió eludir las medidas de autenticación.

Proporción de incidentes cibernéticos globales que qfectan a tereros proveedores de TI (2020-23)



Fuente: Control Risks

Riesgo para la cadena de suministro

Incidentes de terceros

Al menos el 22 % de todas las violaciones de la ciberseguridad en 2023 fueron probablemente el resultado del seguimiento de incidentes de terceros. Para gestionar este riesgo de terceros, que es difícil de mitigar, las organizaciones deben adoptar las mejores prácticas a nivel interno para reforzar su resistencia frente a las infracciones externas y el seguimiento de los objetivos después de incidentes importantes, al tiempo que tienen en cuenta la postura ante el riesgo, las estrategias de mitigación y las pólizas de seguros de sus proveedores de TI externos.

Sector

Para los ciberdelincuentes y los actores de amenazas vinculadas al Estado, los proveedores de TI, como las organizaciones de software como servicio (SaaS), son un objetivo prioritario. En 2023, el 75 % de los incidentes con terceros se originaron en ataques a proveedores de servicios y software.

Porcentaje de infracciones comunicadas a terceros en 2023, por sectores

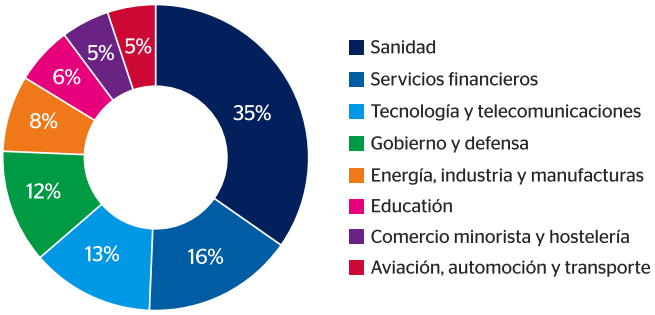


Gráfico: Control Risks • Fuente: Security Scorecard

Más del 75% de los incidentes de terceros en 2023 se deben a solo tres vulnerabilidades en la cadena de suministro.

Los ataques de día cero pueden ser los más impactantes para los grupos de *ransomware*

Los grupos de *ransomware* ven las cadenas de suministro de TI como objetivos atractivos debido a la oportunidad de golpear a muchas organizaciones de distintos sectores a través de un único ataque. Dichas organizaciones tienen elevados requisitos de tiempo de actividad, que pueden aprovecharse en las negociaciones del rescate. En 2023, el 64 % de las filtraciones a terceros estaban relacionadas con el grupo de *ransomware* Clop, que explotaba un fallo de día cero (una vulnerabilidad desconocida y sin parches en un sistema o dispositivo), y el 61 % de las filtraciones a terceros se atribuían a la vulnerabilidad MOVEit, lo que pone de relieve cómo los riesgos de terceros pueden evolucionar hasta convertirse en impactos directos en los clientes de la cadena de suministro. El gráfico siguiente muestra que más del 75 % de los incidentes con terceros en 2023 son atribuibles a solo tres vulnerabilidades de la cadena de suministro.

Porcentaje de incidentes con terceros en 2023, por vulnerabilidad

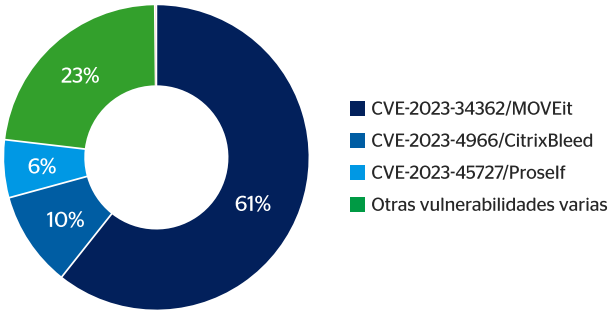
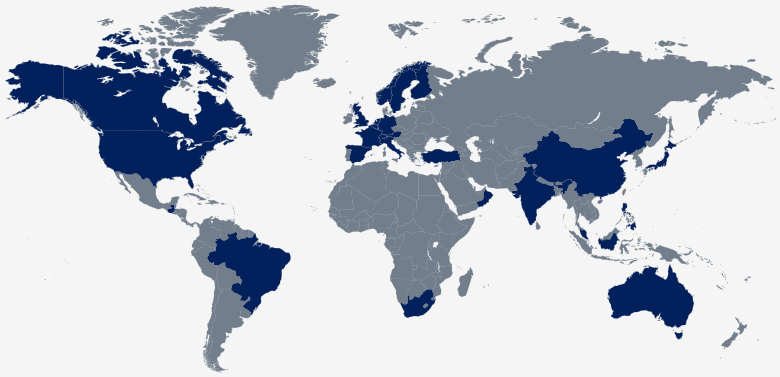


Gráfico: Control Risks • Fuente: Security Scorecard

La campaña MOVEit demuestra que la violación de los datos de los proveedores de TI puede tener amplias repercusiones

Tras explotar una vulnerabilidad de día cero en el servicio de transferencia de archivos MOVEit en mayo de 2023, el grupo de ciberdelincuentes Clop robó archivos de organizaciones que desconocían que estaban expuestas a dicha vulnerabilidad. La oleada de incidentes de robo de datos y extorsión por filtración de datos afectó al menos a 2180 organizaciones. Es probable que Clop haya cobrado más de 100 millones de dólares en pagos de rescates.

Distribución geográfica de las víctimas de MOVEit



Tecnología

Amenazas en la nube

Desde que las organizaciones han adoptado los servicios en la nube, los actores de las amenazas han desarrollado herramientas y tácticas para obtener un acceso más fácil y persistente a las aplicaciones basadas en la nube, explorar una red infectada y encontrar más vulnerabilidades. Navegar a través de configuraciones basadas en la nube también les permite eludir los protocolos de detección típicos, como el análisis avanzado de IP. Los actores vinculados al Estado y los ciberdelincuentes sofisticados también se han trasladado ellos mismos a la nube, exfiltrando datos a su propio almacenamiento en la nube.

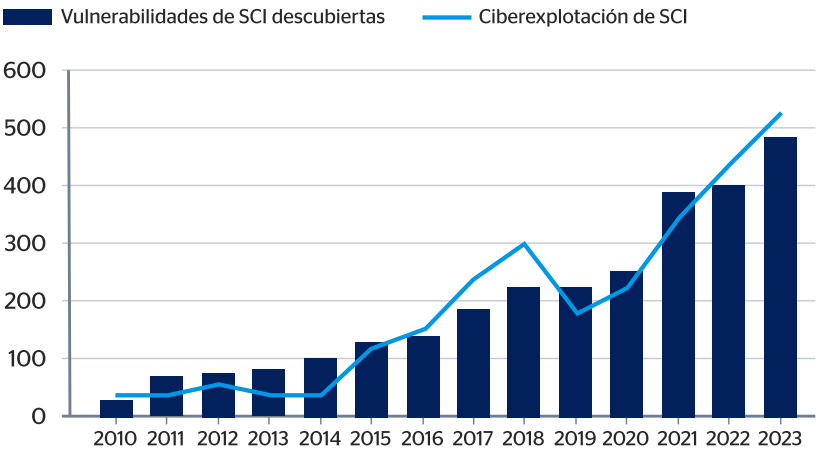
Tecnología operativa y adopción del IdC

Los ataques de *ransomware* contra organizaciones del sector industrial aumentaron un 50 % en 2023 en comparación con 2022. Los ataques exitosos que interrumpen la tecnología operativa (TO) —el software y el hardware que supervisan y controlan los equipos industriales— ayudan a los ciberdelincuentes a extorsionar pagos, ya que la interrupción operativa supone un mayor castigo económico que el rescate. La perturbación de las TO también puede cumplir objetivos estratégicos para los actores vinculados al Estado. Perturbar los procesos de fabricación puede resultar lucrativo o estratégicamente valioso, o ambas cosas.

La ingeniería, la fabricación y los servicios públicos son objetivos atractivos para los ataques que afectan a la TO. Los actores de amenazas de diversas capacidades han apuntado cada vez más a la TO que utiliza controladores o dispositivos expuestos a Internet. Una marcada proliferación de los dispositivos del Internet de las cosas (IdC) —hardware conectado de forma inalámbrica a las redes— probablemente exacerbó esas amenazas a la TO, sobre todo en los sectores de la fabricación y los servicios públicos. Una segmentación eficaz de la red y la limitación o eliminación completa de los puertos expuestos a Internet reducen el riesgo de un ataque perturbador contra la TO.

> Los ataques de *ransomware* contra organizaciones del sector industrial aumentaron un 50% en 2023.

Número de vulnerabilidades en SCI vs incidentes que explotan vulnerabilidades en SCI 2010-23



Fuente: Control Risks

> Las empresas aprovecharán cada vez más la inteligencia artificial y las técnicas de automatización para identificar ciberataques.

Activistas atacan la tecnología operativa y cortan el suministro de agua

En diciembre de 2023, el grupo activista Cyber Av3ngers, vinculado a Irán, atentó contra un sistema privado de suministro de agua en Erris (Irlanda). Aprovechando los controladores lógicos programables (PLC) fabricados por la empresa israelí Unitronics, los ataques provocaron un corte de agua de dos días a los residentes locales. Cyber Av3ngers reivindicó los ataques que afectaron a PLC como parte de su campaña dirigida contra productos y organizaciones israelíes en medio del conflicto entre Israel y Hamás.

IA

De las herramientas de IA exclusivamente preprogramadas para tareas específicas que requieren la intervención humana, se está pasando actualmente a la IA de memoria limitada o estrecha, que puede utilizar conjuntos de datos masivos para tomar decisiones. Por ejemplo, las herramientas de IA generativa de código abierto pueden escribir código para malware o mejorar muchas de las tácticas tradicionales empleadas por los actores de amenazas vinculadas al Estado y los grupos de ciberdelincuentes, como el spearphishing y los ataques de malware.

A medida que la IA sea más fácilmente accesible y proliferen los grandes modelos lingüísticos (LLM), los actores de amenazas de menor capacidad, como los ciberdelincuentes y los ciberactivistas, podrán lanzar ataques de mayor envergadura con mayor rapidez. Este aumento de la capacidad en escala y ritmo será el impacto más significativo en el panorama de las ciberamenazas.

Los delincuentes están desplegando herramientas de IA generativa para crear deepfakes de empleados y ejecutivos de confianza con el fin de estafar a organizaciones de todos los tamaños. A principios de este año, una organización mundial perdió 20 millones de dólares a través de un ataque de deepfake. Estos planes no son nuevos, ya se ha informado de algunos en 2019, pero su frecuencia y sus posibilidades de éxito están aumentando considerablemente; las habilidades necesarias para llevarlos a cabo disminuyen a medida que mejora la tecnología.

Por el contrario, la IA ya desempeña un papel en la detección de comportamientos maliciosos en las redes corporativas, y esperamos que siga mejorando las capacidades de ciberseguridad en general con una mayor eficacia de las actividades de seguridad y defensa. Las organizaciones aprovecharán cada vez más la IA generativa y las técnicas de automatización para identificar los ciberataques frente a un panorama de amenazas innovador, motivado y en constante cambio.

Diversificación de tecnologías

La nube y las tecnologías emergentes han proporcionado a las organizaciones soluciones de infraestructura rentables. Sin embargo, la mayor adopción de la infraestructura como servicio y de la IA como servicio ha aumentado la superficie de ataque de los actores de amenazas, ofreciendo mayores oportunidades de infectar a múltiples víctimas por incidente.

El aumento de los dispositivos IoT ha permitido que ciberataques más perturbadores afecten a servicios públicos esenciales, como la distribución de agua. Los avances en IA generativa han permitido a los ciberdelincuentes crear deepfakes de ejecutivos para facilitar los ataques de ingeniería social. Los actores de amenazas vinculados al Estado y los ciberactivistas están recurriendo a soluciones cibercriminales para influir en las elecciones o financiar campañas. Una amplia gama de actores de amenazas están desarrollando sus propias herramientas y aprovechando la IA para automatizar la preparación de los ataques y desplegar el malware. La adopción de tecnologías emergentes a diversos grados de ritmo y escala según el sector y la geografía está ampliando la superficie de ataque, mientras las organizaciones luchan por mantenerse preparadas.

Conclusión

La interdependencia tecnológica, impulsada por los avances en la interconectividad, la IA y las tecnologías emergentes, ha brindado oportunidades a los ciberactores para afectar a las empresas. La inestabilidad de los conflictos mundiales, los cambios geopolíticos y el auge de la economía cibercriminal pueden propiciar mayores riesgos para las organizaciones que adopten tecnologías emergentes en sus prácticas de trabajo.

La interdependencia entre sectores y empresas hará que estos riesgos sean inevitables, ya que los actores de las amenazas dan prioridad al desarrollo de malware sofisticado para afectar a los entornos TO o a terceros proveedores de servicios y software. La IA y otras tecnologías seguirán desarrollándose, ayudando a reducir y prevenir una serie de amenazas que tratan de aprovechar la interdependencia tecnológica.

Una estrategia de transformación digital asegurada contra las amenazas futuras puede ser el catalizador del éxito. Las estrategias de mitigación de riesgos deben tener en cuenta la creciente probabilidad de que se produzcan incidentes cibernéticos e impulsar de forma proactiva la resiliencia, al tiempo que se implementan protocolos de respuesta para reaccionar con rapidez ante las incursiones cibernéticas.

Annex – key references

"Global *ransomware* threat expected to rise with AI, NCSC warns", ncsc.gov.uk
"2023 *Ransomware* Attack Report", blackfog.com
"*Ransomware* Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline", chanalysis.comv
"#Stop*Ransomware*: CLOP *Ransomware* Gang Exploits CVE-2023-34362 MOVEit Vulnerability", cisa.gov
"Two-day water outage in remote Irish region caused by pro-Iran hackers", therecord.media
"NCC Group Releases Annual Cyber Threat Monitor Report 2023", nccgroup.com
"*Ransomware* Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double", dni.gov
"The State of *Ransomware* 2024", sophos.com
"The State of *Ransomware* in Manufacturing and Production 2024", sophos.com
"Helping our customers through the CrowdStrike outage", blog.microsoft.com
"Dragos 2023 OT Cybersecurity Year in Review", dragos.com
"Global Third-Party Cybersecurity Breach Report", securityscorecard.com

Se ha publicado una corrección el 9 de octubre de 2024 para rectificar una cifra errónea en el informe en la página 7. A nivel mundial, un total de 389 organizaciones del sector sanitario sufrieron ataques de ransomware en 2023 (Control Risks, 2024).

Ciberseguro QBE

Los productos cibernéticos de QBE protegen frente a la gama de riesgos asociados a la tecnología digital y proporcionan un apoyo fundamental en caso de ciberataque. La oferta incluye QCyberProtect, una nueva póliza de seguro cibernético global para una cobertura consistente en todo el mundo, para las pérdidas derivadas de los riesgos cibernéticos actuales y emergentes, incluyendo, pero no limitado a, la seguridad de la red, la responsabilidad de privacidad, las interrupciones de negocio de TI y no TI y la pérdida de reputación.

Cobertura a medida y servicio individual

Para garantizar tu protección, los suscriptores de QBE trabajan en estrecha colaboración con los clientes para crear una cobertura que se adapte a tus necesidades específicas. Nos tomamos el tiempo necesario para comprender tu negocio y ofrecerte una cobertura a medida que te proteja frente a los riesgos cibernéticos actuales y emergentes.

Ayudamos a gestionar losriesgos

No solo cubrimos los riesgos, sino que le ayudamos a gestionarlos y reducirlos. Ofrecemos herramientas de apoyo a la gestión de riesgos que incluyen:

- QBE QCyberPrepare: una sala de seguridad en línea para ayudar a los clientes a prepararse para un incidente cibernético.
- Acceso gratuito al Portal de Gestión de Riesgos Cibernéticos de QBE, que ofrece una amplia gama de información sobre los riesgos cibernéticos, así como la forma de asegurarse de que está protegido contra ellos.

Apoyo en caso de crisis

QBE ofrece asistencia las 24 horas del día en caso de sufrir un incidente cibernético. Eso podría implicar proporcionar un equipo forense para averiguar cómo se produjo la brecha cibernética y cómo solucionar el problema; asesoramiento jurídico para abordar los requisitos reglamentarios; o gestionar una declaración a los medios de comunicación para minimizar cualquier impacto en la reputación.

Para más información, visita qbeespana.com/productos/cyber/

Este informe
está elaborado
para QBE por
Control Risks

QBE European Operations

QBE Europe SA/NV, Sucursal en España
Paseo de la Castellana, 31 – 5ª Planta
28046 Madrid, Spain
+34 91 789 39 50
QBEespana.com

641209/2405