THREATQUOTIENT

ThreatQ para empresas tecnológicas

La enorme superficie de ataque, la adopción precoz de nuevas tecnologías y la multiplicación de datos de gran valor crean un terreno propicio para la proliferación de ataques contra las empresas tecnológicas. Los ciberdelincuentes disponen de numerosos medios para lanzar ataques, y sus motivaciones son variadas. Además, pueden utilizar algunas empresas tecnológicas (proveedores de servicios gestionados, de almacenamiento en la nube y de servicios, soluciones de intercambio de archivos, etc.) como punto de partida para infiltrarse en otras empresas y sectores, ya que les proporcionan una infraestructura crítica.

A pesar de su experiencia tecnológica y de su compromiso con la innovación, las empresas tecnológicas siguen siendo víctimas de compromisos y fugas de datos. De hecho, Accenture informó de que las empresas tecnológicas son víctimas de un gran número de ataques graves: en 2021 se produjeron algo más de 240 intentos, y apenas 30 de ellos tuvieron éxito[1]. Cuando los ataques tienen éxito y se produce el robo de datos, el coste total medio asociado a una fuga de datos para las empresas tecnológicas se eleva en la actualidad hasta los 5 millones de dólares, lo que supone un aumento de casi el 2 % con respecto al año anterior[2].

DESAFÍOS PRINCIPALES

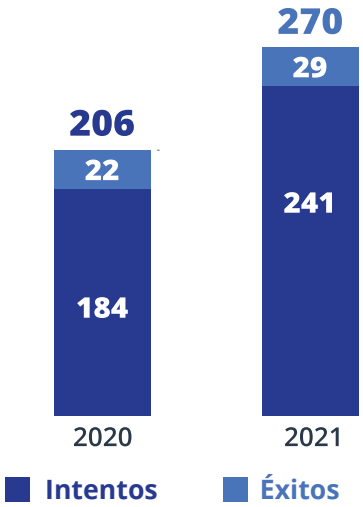
GRANDES SUPERFICIES DE ATAQUE

Las empresas tecnológicas se enfrentan a un desafío doble: proteger su propia infraestructura contra los ciberataques, y los productos y servicios que proporcionan a los clientes. Muchas recurren a modelos operativos distribuidos y en la nube para mejorar su agilidad y obtener una ventaja competitiva. Sin embargo, estos modelos pueden crear ángulos muertos y fallos de seguridad de los que pueden aprovecharse los ciberdelincuentes. Los compromisos no solo afectan a su entorno inmediato, sino que pueden tener también devastadores efectos en cadena. En los últimos años, empresas como LinkedIn, Facebook y Yahoo! han sido víctimas de ataques que afectaron a los usuarios de sus soluciones. Y a finales de mayo de 2023, MOVEit, una empresa de software de transferencia gestionada de archivos (MFT), descubrió una vulnerabilidad de día cero (zero-day). MOVEit se utiliza en los sectores sanitario, financiero, tecnológico y público[5]. La visibilidad de toda su infraestructura, así como un enfoque proactivo y anticipatorio de las operaciones de seguridad, ayudarán a las empresas tecnológicas a reforzar sus defensas.

ADOPCIÓN PRECOZ DE NUEVAS TECNOLOGÍAS

Un gran número de empresas de alta tecnología adoptan las nuevas tecnologías de forma precoz y están más dispuestas a asumir riesgos que sus homólogas de otros sectores. Absolutamente comprometidas con la innovación, las empresas tecnológicas y sus empleados adoptan más rápidamente dispositivos y aplicaciones de última generación, así como tecnologías abiertas que pueden no ser del todo seguras. Centradas en la colaboración, la creatividad y la comunicación con equipos a menudo distribuidos por todo el mundo, y trabajando frecuentemente con plazos ajustados para hacer frente a una competencia feroz, en ocasiones dan prioridad a la velocidad y sencillez en detrimento de la seguridad. Para resolver los fallos de seguridad generados por las nuevas tecnologías, necesitan información sobre las

MEDIA DE ATAQUES POR EMPRESA



Se produjeron de media **270 ataques** (acceso no autorizado a datos, aplicaciones, servicios, redes o dispositivos) por empresa a lo largo de un año, un **AUMENTO DEL 31 %** respecto a 2020[3].

nuevas amenazas emergentes y deben comprender su relevancia para la empresa, a fin de poder determinar cómo reducir los riesgos.

MULTIPLICACIÓN DE DATOS DE GRAN VALOR

Ya se trate de propiedad intelectual o de datos de empleados y clientes, las empresas tecnológicas disponen de una enorme cantidad de información de gran valor que resulta atractiva para los ciberdelincuentes. Los datos personales, como la información de tarjetas de crédito y los registros de los empleados, pueden utilizarse para cometer delitos de fraude o de usurpación de identidad, o revenderse a otros ciberdelincuentes. El coste medio de una fuga de datos por registro ha aumentado hasta alcanzar los 4,97 millones dólares para las empresas tecnológicas, lo que representa el cuarto coste más elevado de todos los sectores y superior a la media mundial, que se sitúa en los 4,35 millones de dólares[6]. Esta cifra incluye la detección, la escalación y la notificación de las amenazas, las medidas de corrección posfuga de datos y la pérdida de negocio[4]. Pero puede parecer insignificante en comparación con los incidentes en los que se produce la divulgación, robo o uso por un competidor de elementos de propiedad intelectual, como secretos comerciales y solicitudes de patentes sin publicar, situaciones que podrían en riesgo la viabilidad misma de la empresa. Las empresas tecnológicas necesitan conocimiento en tiempo real del modus operandi de los ciberdelincuentes y de las campañas, para así poder acelerar la respuesta a incidentes y reforzar la prevención.

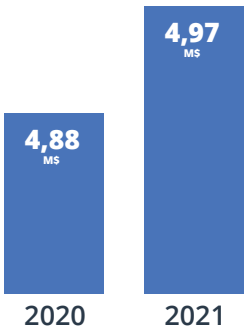
CREACIÓN DE OPERACIONES DE SEGURIDAD LÍDERES BASADAS EN DATOS

La plataforma ThreatQ, que sirve de centro de operaciones de inteligencia para muchos sectores, agrega y combina datos estructurados y no estructurados procedentes de cualquier fuente, interna y externa. La automatización elimina las tareas repetitivas y laboriosas para que los analistas puedan centrarse en el trabajo estratégico y de mayor prioridad. La plataforma también ofrece flexibilidad para compartir rápidamente información curada sobre amenazas, avisos e informes con una amplia variedad de actores internos y externos, incluidos los sectores de infraestructuras críticas.

CONSIGA MÁS CON THREATQ:

- **CONSOLIDE** todas las fuentes de información sobre amenazas y vulnerabilidades externas (por ejemplo, IT- ISAC y OSINT) e internas (por ejemplo, SIEM y EDR) en un repositorio central.
- **ELIMINE** el ruido y explore fácilmente enormes cantidades de datos sobre amenazas para centrarse en los activos y vulnerabilidades críticos.
- **PRIORICE** lo más importante para el entorno de sistema tecnológico.
- **INTEGRE** solamente indicadores pertinentes en sus directivas de seguridad.
- **PERSIGA PROACTIVAMENTE** toda actividad maliciosa que pueda señalar un compromiso de elementos de propiedad intelectual, fraude con tarjetas de pago o el compromiso de soluciones o servicios vendidos a los clientes, o susceptible de generar daños a empleados, clientes y a la propia empresa.
- **PONGA SU ATENCIÓN** en las vulnerabilidades de seguridad conocidas en exploits activos actualmente, que pueden afectar a su nivel de cumplimiento de normativas y de seguridad.
- **AGILICE EL ANÁLISIS** y la respuesta a ataques contra varios objetivos, como los sistemas internos, las tecnologías y dispositivos emergentes, las soluciones suministradas a los clientes y la infraestructura de apoyo.
- **TRANSFIERA AUTOMÁTICAMENTE** la inteligencia sobre amenazas a las herramientas de detección y respuesta.

COSTE MEDIO DE UNA FUGA DE DATOS EN EL SECTOR TECNOLÓGICO[6]



> El coste medio de una fuga de datos por registro ha aumentado hasta alcanzar los **4,97 millones de dólares** para las empresas tecnológicas, lo que representa el cuarto coste más elevado de todos los sectores y superior a la media mundial, que se sitúa en los 4,35 millones de dólares[6].

Solicite una demostración en directo de la plataforma ThreatQ y de ThreatQ TDR Orchestrator en www.threatq.com/demo.

1. https://www.accenture.com/us-en/industries/high-tech-index
2. https://www.ibm.com/downloads/cas/3R8N1DZJ
3. https://www.accenture.com/content/dam/accenture/final/a-com-migration/custom/us-en/invest-cyber-resilience/pdf/Accenture-State-Of-Cybersecurity-2021.pdf#zoom=40
4. https://www.zerofox.com/blog/top-5-industries-most-vulnerable-to-data-breaches-in-2023/
5. https://cyberint.com/blog/research/moveit-supply-chain-attack/
6. https://www.ibm.com/downloads/cas/3R8N1DZJ

ACERCA DE THREATQUOTIENT™

ThreatQuotient mejora las operaciones de seguridad fusionando diversas fuentes de datos, herramientas y equipos con el fin de agilizar la detección de amenazas y la respuesta. La plataforma de operaciones de seguridad de ThreatQuotient se basa en datos y ayuda a los equipos a priorizar los incidentes de seguridad, aplicar la automatización y colaborar en su resolución; permite tomar decisiones más fundamentadas; y optimiza el uso de recursos limitados integrando la tecnología y los procesos en un espacio de trabajo unificado. De esta forma se consigue reducir las detecciones irrelevantes, determinar qué amenazas son prioritarias y automatizar los procesos con datos precisos. Las funciones líderes en el sector de ThreatQuotient para la gestión de datos, la orquestación y la automatización cubren diferentes casos de uso, como la respuesta a incidentes, la caza de amenazas, el phishing dirigido, la clasificación de alertas y la priorización de vulnerabilidades, y también pueden servir como plataforma de inteligencia sobre amenazas. ThreatQuotient tiene su sede central en Virginia del Norte y centros de operaciones internacionales en Europa, Asia Pacífico y Oriente Medio-Norte de África. Para obtener más información, visite www.threatquotient.com.

TQ-IDB04-0823-02

20130 Lakeview Center Plaza, Suite 400 Ashburn, VA 20147 • ThreatQ.com
Sales@ThreatQ.com • +1 703 574-9885