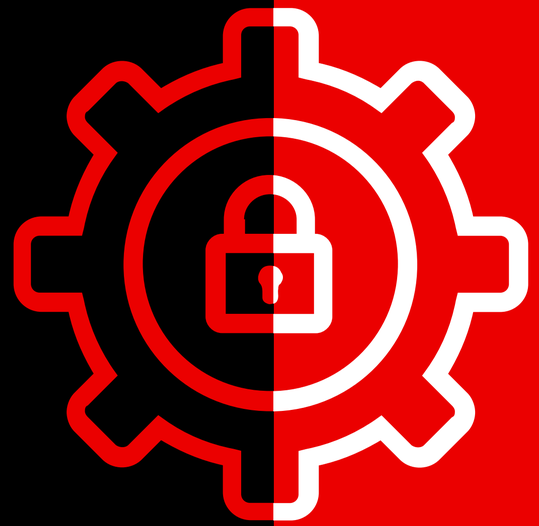
CROWDSTRIKE

Detener las ciberamenazas en los servicios financieros

Cumple los requisitos normativos en lugar de con las exigencias de los adversarios en una época donde las ciberamenazas van en aumento



El panorama competitivo y operativo de las organizaciones de servicios financieros está cambiando y evolucionando. La demanda de experiencias personalizadas y fluidas exige una seguridad y una privacidad de datos más sólidas.

Si a esto le sumamos el crecimiento exponencial de los sistemas basados en la nube y en datos, las organizaciones de servicios financieros se convierten en uno de los objetivos principales de los ciberataques. El Informe Global sobre Amenazas muestra que el número de ataques contra los servicios financieros aumenta cada año.

El cumplimiento normativo no es negociable

¿Te estás adaptando lo suficientemente rápido para detener a los adversarios?

¿Estás poniendo en marcha medidas para cumplir con las próximas normativas, como la directiva NIS2 de la UE y la Ley de Resiliencia Operativa Digital (DORA)?

Estar al día de las tendencias de ciberseguridad te ayuda a evitar los problemas operativos y financieros, así como los daños a la reputación que causan los ataques. También te ayuda a evitar las cuantiosas multas asociadas al incumplimiento de la normativa.

Sanciones para las empresas del sector financiero que incumplen la normativa o no informan de incidentes:

10 mills. de EUR

Hasta 10 millones de EUR o el 2 % de la facturación anual mundial para NIS2.

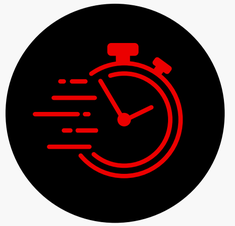
5 mills. de EUR

Hasta 5 millones de EUR o el 2 % de la facturación anual mundial para DORA.

▶ **Nuestros expertos en ciberseguridad te ayudan a navegar por los cambios normativos más recientes.**

¿Qué está sucediendo en el mundo de la ciberseguridad y qué significa para los servicios financieros?

7 PRINCIPALES CONCLUSIONES PARA LAS ORGANIZACIONES DE SERVICIOS FINANCIEROS DEL **INFORME GLOBAL SOBRE AMENAZAS** DE 2024



1. Los ataques son más sofisticados y se producen más rápido

El tiempo que se tarda en acceder a una red se ha reducido drásticamente:

- El tiempo de propagación medio es más de un 25 % más rápido que en 2023, con 62 minutos.
- El ataque más rápido registrado es de tan solo 2 minutos y 7 segundos.

¿QUÉ PUEDES HACER?

Cumplimiento

Actualiza y prueba los planes de respuesta a incidentes con regularidad para cumplir los requisitos NIS2 relacionados con la gestión y notificación rápida de incidentes.

Acción

Acelera los tiempos de detección y respuesta ante incidentes con soluciones avanzadas de detección y respuesta para endpoints (EDR).

- **Ponte al día rápido. Utiliza la tecnología centrada en el adversario con el tiempo de detección más rápido (probado en las evaluaciones de MITRE ATT&CK®), adaptada al sector de los servicios financieros.**

2. El malware y los métodos de ataque están evolucionando

El **75 %** de los ataques son ahora sin malware, en comparación con el 40 % en 2019.

A medida que mejora la identificación de las amenazas, los adversarios buscan nuevas formas de evadir la seguridad. El robo de credenciales de identidad y los ataques de ingeniería socialhacen que las infracciones sean más difíciles de detectar.

¿QUÉ PUEDES HACER?

Cumplimiento

Implementa controles de acceso estrictos y supervisa las actividades de los usuarios para cumplir los requisitos de NIS2 sobre la protección de las redes y de los sistemas de información.

Acción

Mejora la protección de la identidad con la autenticación multifactor (MFA).

- **Utiliza servicios de Threat Hunting para conocer las nuevas técnicas de los adversarios.**

3. Han aumentado las intrusiones en la nube

Las intrusiones orientadas a la nube han aumentado en un **110 %** en un año.

Los ciberadversarios aprovechan los puntos débiles de las configuraciones de seguridad en la nube para realizar el ataque desde dentro del servicio en la nube de la víctima.

¿QUÉ PUEDES HACER?

Cumplimiento

Asegúrate de que los proveedores de nube cumplen los estándares y las prácticas recomendadas de NIS2 para proteger los servicios y los datos basados en la nube.

Acción

Adopta marcos integrales de seguridad en la nube, incluida la gestión de identidades y accesos (IAM), el cifrado y la supervisión continua.

- **No esperes a que los adversarios se infiltren en tus sistemas financieros. Busca la ayuda de expertos para evitar los ataques.**

4. Se están explotando las relaciones con terceros

El software comercial procedente del sector de la tecnología fue el origen de la mayoría de relaciones de confianza explotadas.

Los adversarios dirigen cada vez más sus ataques hacia las cadenas de suministro y los proveedores externos para acceder a las redes de las instituciones financieras, aprovechándose de su naturaleza interconectada y de confianza.

¿QUÉ PUEDES HACER?

Cumplimiento

Desarrolla e implementa políticas de gestión de riesgos de terceros para satisfacer los requisitos mejorados de NIS2 para la seguridad de la cadena de suministro.

Acción

Realiza evaluaciones y auditorías de seguridad rigurosas de todos los proveedores externos. Implementa requisitos de ciberseguridad contractuales para los proveedores.

- **Los adversarios obtienen una gran rentabilidad de los ataques a las relaciones con terceros. Asegúrate de que los estándares de seguridad de los proveedores son tan rigurosos como los tuyos.**

5. Los adversarios utilizan la IA generativa

Los adversarios podrían utilizar la IA de forma indebida para obtener información, sobre todo en situaciones donde los usuarios tienen menos conocimientos digitales.

La IA ha reducido los conocimientos necesarios para realizar ataques sofisticados y generalizados.

¿QUÉ PUEDES HACER?

Cumplimiento

Actualiza regularmente las estrategias de ciberseguridad para abordar las amenazas de IA emergentes y satisfacer los requisitos de NIS2 en lo que respecta a la gestión de amenazas proactiva.

Acción

Mantente al día sobre las amenazas basadas en IA y plantéate la posibilidad de añadir herramientas de ciberseguridad con IA para detectar y contrarrestar estas técnicas avanzadas.

- **Utiliza la potencia transformadora de la IA generativa en los flujos de trabajo de seguridad para proteger tu negocio.**

6. La protección de la identidad debe ser una prioridad

Nuestro Informe Global sobre Amenazas de 2024 comparte ejemplos reales donde el phishing y la explotación de las vulnerabilidades del software hacen posible el robo de credenciales.

Las identidades son uno de los principales objetivos de las ciberintrusiones. El número de ataques realizados con credenciales robadas para obtener acceso no autorizado es cada vez mayor.

¿QUÉ PUEDES HACER?

Cumplimiento

Adopta las prácticas recomendadas del sector para la gestión de identidades y accesos (IAM), como las que tenemos en marcha, para cumplir los requisitos de NIS2 para la protección de identidades.

Acción

Implementa soluciones sólidas para la gestión de identidades y accesos (IAM), que incluyan la detección de anomalías y la supervisión en tiempo real.

▶ **Adelántate a las amenazas modernas con una plataforma unificada para evitar los ataques basados en la identidad.**

7. Es necesario reducir el tiempo de respuesta y de detección

Por lo general, los adversarios buscan ampliar su acceso más allá del punto inicial de contacto, y tardan una hora de media. Después, pueden causar estragos en tan solo segundos.

La rapidez de detección y respuesta ante los ciberataques es fundamental. Los retrasos pueden aumentar el daño causado por la brecha.

¿QUÉ PUEDES HACER?

Cumplimiento

Desarrolla y prueba regularmente planes de respuesta ante incidentes para garantizar una acción rápida y cumplir los estrictos plazos de presentación de informes que exige la NIS2.

Acción

Invierte en herramientas de análisis y supervisión avanzadas que ofrezcan visibilidad en tiempo real sobre la actividad de la red.

El cumplimiento de la normativa no es negociable, sobre todo para las instituciones financieras. Ignorarlo expone a tu organización, y a tus clientes, a riesgos innecesarios.

Crea un equipo de cumplimiento específico para supervisar de forma regular los avances en la normativa y garantizar que las prácticas de ciberseguridad estén actualizadas. Asegúrate de que realizan auditorías de cumplimiento de forma periódica y de que actualizan las políticas para cumplir los requisitos de NIS2, DORA y otros marcos normativos.

Los expertos en ciberseguridad te ayudan a navegar por los cambios normativos más recientes.

Lee el Informe Global sobre Amenazas 2024 de CrowdStrike

7 Principales conclusiones del Informe Global sobre Amenazas 2024 de CrowdStrike

1. Los ataques son más sofisticados y se producen más rápido
2. El malware y los métodos de ataque están evolucionando
3. Han aumentado las intrusiones en la nube
4. Se están explotando las relaciones con terceros
5. Los adversarios utilizan la IA generativa
6. La protección de la identidad debe ser una prioridad
7. Es necesario reducir el tiempo de respuesta y de detección

DESCARGAR EL INFORME

CROWDSTRIKE

Acerca de CrowdStrike

CrowdStrike (Nasdaq: CRWD), líder mundial en ciberseguridad, ha redefinido la seguridad moderna con la plataforma nativa para la nube más avanzada del mundo, para proteger aspectos fundamentales del riesgo empresarial: las cargas de trabajo, la identidad y los datos, tanto en los endpoints como en la nube.

Gracias a CrowdStrike Security Cloud y una inteligencia artificial de talla mundial, la plataforma CrowdStrike Falcon® se nutre de indicadores en tiempo real, inteligencia sobre amenazas, información de las herramientas evolutivas de los adversarios y telemetría enriquecida con datos de toda la empresa, para facilitar detecciones hiperprecisas, protección y remediación automatizadas, Threat Hunting de élite y observación de vulnerabilidades por prioridades.

Desarrollada expresamente en la nube con una arquitectura de agente ligero único, la plataforma Falcon ofrece un despliegue rápido y escalable, una protección y un rendimiento superiores, una menor complejidad y una rentabilidad inmediata.

CrowdStrike. We Stop Breaches.