Resiliencia ante ataques de ransomware en 2026

El ransomware se ha convertido en una de las amenazas más disruptivas para las organizaciones de cualquier tamaño y sector. No se trata solo de un ataque tecnológico, sino de un riesgo operativo, legal y reputacional que puede paralizar totalmente la actividad. Por ello, en un entorno donde los incidentes aumentan y se sofistican, la resiliencia se ha consolidado como una prioridad estratégica.

¿Qué es el ransomware y cómo opera?

El ransomware es un tipo de ataque que **cifra o bloquea la información crítica** de una organización, generalmente con el objetivo de exigir un rescate económico. Su evolución ha dado lugar a variantes cada vez más dañinas:

- **Cifrado de datos:** el atacante inutiliza documentos, bases de datos o sistemas completos.
- **Robo de información (exfiltración):** previo al cifrado, extraen datos para presionar a la víctima.
- **Doble y triple extorsión:** amenazan con publicar información, realizar ataques DDoS o contactar a clientes y proveedores.
- **Ransomware-as-a-Service (RaaS):** grupos criminales ofrecen kits listos para usar a atacantes sin conocimientos avanzados.
- **IA ofensiva:** la inteligencia artificial se emplea para generar campañas de phishing automatizadas, diseñar malware adaptable o negociar rescates a través de chatbots.

Evolución y tendencias actuales

Según la empresa de seguridad ZSCALER, en España, los incidentes de ransomware crecieron más de un 116 % en 2025 con respecto al año anterior, entrando en el top 15 de países más afectados y siendo uno de los países europeos donde el ransomware ha crecido con más fuerza en el último año.

A escala internacional, podemos observar un mayor uso de ransomware basado en IA y automatización, ataques contra identidades digitales, especialmente Active Directory y un aumento del modelo RaaS, que “democratiza” el crimen y multiplica la actividad.

Aun así, hay señales positivas, gracias a mejores defensas y copias de seguridad más robustas, el 49 % de las empresas españolas ya logra recuperarse en menos de una semana, y los costes medios de recuperación han caído más de un 66 % respecto al año anterior, según el último informe de Sophos sobre El Estado del Ransomware.

Exigencias normativas clave (España y UE)

El contexto regulatorio se ha endurecido notablemente, especialmente desde 2024 con la entrada en vigor de nuevas directivas:

NIS2 obliga a empresas esenciales e importantes a reforzar sus controles de seguridad y requiere:

- gestión continua de riesgos,
- trazabilidad de incidentes,
- formación del personal,
- evaluación de la cadena de suministro,
- notificación de incidentes significativos en plazos muy reducidos.

DORA exige capacidades robustas de continuidad, pruebas de resiliencia, gestión de proveedores críticos y reportes obligatorios.

ENS (Esquema Nacional de Seguridad) requiere controles estrictos de confidencialidad, integridad, disponibilidad y monitorización.

RGPD obliga a notificar brechas de datos personales en un plazo máximo de 72 horas y exige demostrar diligencia, medidas técnicas adecuadas y documentación de los procesos.

En conjunto, estas normas sitúan la resiliencia en el centro de las obligaciones legales, no como una recomendación, sino como una exigencia.

Estrategias de resiliencia y recomendaciones

Para resistir y recuperarse eficazmente, las organizaciones deben adoptar una combinación de medidas tecnológicas, organizativas y operativas.

- **Copias de seguridad seguras:** inmutables, cifradas, aisladas y probadas regularmente.
- **Segmentación y Zero Trust:** limitar el movimiento lateral dentro de la red.
- **Actualizaciones y parches continuos:** evitar que vulnerabilidades conocidas se conviertan en puertas de entrada.
- **Formación del personal:** el phishing sigue siendo el principal vector de ataque.
- **Monitorización inteligente:** el uso de IA para detectar patrones anómalos acelera la respuesta.

- **Planes específicos de recuperación** para identidades, entornos críticos y aplicaciones esenciales.
- **Simulacros periódicos** que verifican la velocidad real de recuperación.
- **Servicios 24/7** o centros SOC que aseguren detección continua.

Conclusiones

El ransomware continuará evolucionando, integrando nuevas técnicas de presión, sofisticación y automatización. En este contexto, la resiliencia ya no es una opción: es el elemento que marca la diferencia entre una crisis gestionada y un colapso operativo.

Las organizaciones que adoptan una estrategia integral que combina prevención, monitorización, copias seguras, procedimientos claros y cumplimiento normativo, estarán en mejores condiciones para afrontar un ataque y proteger su continuidad de negocio.

Antonio J. Gómez

Coordinador del área de ciberseguridad de AES