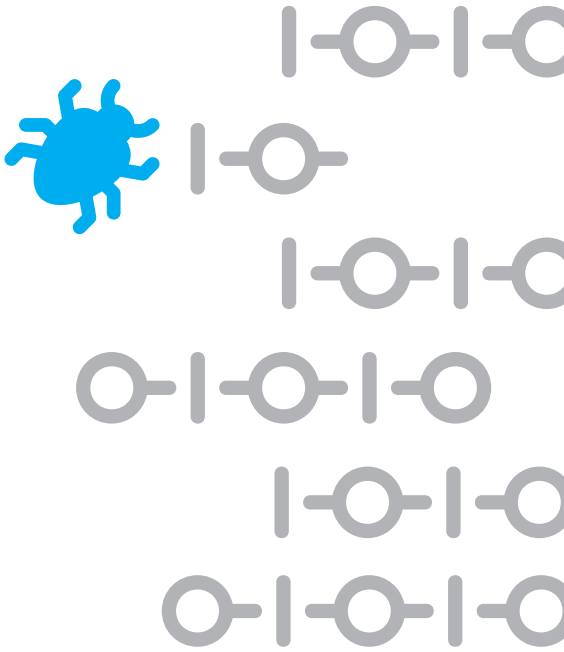
CÓMO PROTEGERSE FRENTE A UN ransomware



Los ataques de ransomware **han crecido exponencialmente** en los últimos años. Los expertos atribuyen este crecimiento a la negligencia de las personas **al clicar en correos electrónicos de phishing y anuncios infectados**. El daño se puede evitar con una mayor conciencia del usuario y junto con las prácticas de seguridad adecuadas. Las empresas deben conocer los riesgos y tomar las precauciones adecuadas para minimizar el impacto en caso de infección.

En esta **guía básica de Ackcent Cybersecurity** explicamos las mejores prácticas que puede realizar una empresa para protegerse frente a un posible ataque.

Las fases

por las que pasa una empresa ante un ransomware son las siguientes:

1. PREPARACIÓN
2. IDENTIFICACIÓN
3. CONTENCIÓN
4. REMEDIO
5. RECUPERACIÓN

ackcent cybersecurity

1 PREPARACIÓN

- Asegurarse de que todos los sistemas *Endpoint* de la empresa están actualizados.
- Comprobar que los productos de seguridad del usuario y de seguridad perimetral (*gateway* de correo electrónico, cachés de *proxy*) estén actualizados.
- Aumentar el conocimiento de soporte de TI con respecto a la amenaza de ransomware.
- Asegurarse de tener copias de seguridad exhaustivas, recientes y fiables de los datos de los usuarios locales y de la red.

IDENTIFICACIÓN 2

- Detectar los cambios en el comportamiento masivo de los ficheros del sistema operativo.
- Notificar en el caso de que se reciban emails profesionales extraños que contienen archivos adjuntos (por ejemplo: facturas, notificaciones...).
- Alertar cuando se muestra un mensaje que explica que los documentos han sido cifrados y en el que, generalmente, se solicita un rescate económico.

3 CONTENCIÓN

- Desconectar inmediatamente todos los equipos que se han detectado como comprometidos en la red.
- Si no se puede aislar el equipo, desconectar o cancelar las unidades compartidas (NET USE x: \\ unc \ path \ / DELETE).
- Bloquear el tráfico sospechoso y a los C&C de ransomware identificados.
- Envío automático de las muestras no detectadas, la URL maliciosa sin clasificar, los nombres de dominio e IP a su proveedor de seguridad.

REMEDIO 4

- Eliminar los binarios y las entradas de registro relacionadas (si las hubiera) de perfiles comprometidos (% ALLUSERSPROFILE% o% APPDATA%) y% SystemDrive%.
- Si el paso anterior no es posible, realizar una instalación limpia del equipo.

5 RECUPERACIÓN

- Revisar todos los mecanismos de seguridad para que los binarios maliciosos identificados sean bloqueados.
- Asegurarse de que se ha resuelto por completo la incidencia, evitando la posibilidad de que se pueda volver a reproducir.
- Comprobar que el tráfico de red vuelve a la normalidad.
- Restaurar los documentos de los usuarios desde copias de seguridad.