cohaerentis

# Medidas preventivas ataques ransomware

Mediante el ransomware, los atacantes toman el control de equipos, servidores, bases de datos y, con carácter general, información cuyo acceso cifran y por cuyo rescate piden una cantidad de dinero en criptomonedas.

Estos ataques pueden prevenirse con **medidas organizativas**, **físicas** y **tecnológicas. Debe verificarse cuáles de estas medidas todavía no han sido implementadas en la organización, y adoptarse para prevenir futuros ataques**:

- ☐ Parches instalados y gestionados
- ☐ Sistemas de detección de antimalware
- ☐ Sistemas de backups separados para que el posible ataque no afecte a las copias de seguridad (debe tener se en cuenta que, el hecho de que las copias de seguridad pudieran verse cifradas por el ataque, plantearía cuestiones sobre la calidad de las medidas de seguridad previas implementadas por el responsable del tratamiento y debería ser adecuadamente revisado durante la investigación, dado que un buen sistema de copias de seguridad debe estar almacenado con seguridad sin acceso desde el sistema principal, de lo contrario, podría ser comprometido por el mismo ataque.
- ☐ Educación en materia de seguridad a los empleados para detectar estos tipos de ataques.
- ☐ Mantener el firmware, sistemas operativos, aplicaciones de software de servidores, clientes y componentes de red, así como cualquier máquina en la red (incluidos dispositivos wifi) actualizados.
    - ☐ Verificar que todas las medidas razonables están implementadas, que son efectivas y que se mantienen debidamente actualizadas cuando los tratamientos o las circunstancias cambian.
- ☐ Diseñar y organizar los sistemas de tratamiento e infraestructuras en segmentos o aislar sistemas de datos y redes para evitar la propagación del malware en sistemas de la organización o en sistemas externos.
- ☐ Implementar procedimientos actualizados de copias de seguridad, securizados y cuyo funcionamiento sea testeado.
    - ☐ Los dispositivos de las copias de seguridad a medio y largo plazo deben mantenerse separados de los sistemas en producción y aislados fuera del alcance de terceros incluso en caso de un ataque que tenga éxito.
- ☐ Disponer de software antimalware debidamente actualizados y efectivos e integrados en los sistemas.
- ☐ Disponer de sistemas de firewall y de intrusión actualizados y efectivos.
    - ☐ Dirigir todo el tráfico a través del firewall y sistemas de detección, incluso en el casos de teletrabajo (por ejemplo, utilizando conexiones VPN para garantizar la seguridad al acceder a Internet)
- ☐ Formar a los trabajadores para reconocer y prevenir ataques. El responsable del tratamiento debe proporcionar los medios para establecer si los correos electrónicos y mensajes obtenidos por otros medios de comunicación son confiables y auténticos.

- [ ] Los empleados deben estar capacitados para reconocer cuándo se ha producido un ataque de este tipo para desconectar su sistema de la red y notificar inmediatamente a las personas responsables de TI.
- [ ] Restaurar los datos desde la copia de seguridad.
- [ ] Reenvío o replicación de todos los logs de registro a un servidor central, incluyendo el sellado de tiempo criptográfico de las entradas del registro.
- [ ] Cifrado fuerte y autenticación, en particular para el acceso root a los sistemas de TI, gestión adecuada de claves y contraseñas.
- [ ] Realizar test de penetración y vulnerabilidad con carácter periódico.
- [ ] Establecer un equipo de respuesta ante incidentes de seguridad informática o respuesta ante emergencias informáticas.
- [ ] Al evaluar las contramedidas, se debe revisar el análisis de riesgos.

En el caso de que no se implementen estas medidas, será necesario realizar una Evaluación de Riesgo adicional.