CIPHRAVERSE

WHITE PAPER CIPHRAVERSE

Ransomware en empresas sin equipo de IT

Una pyme sin departamento de IT no es un objetivo menor de un ataque de ransomware, solo tarda más en detectarlo y en reaccionar. El cifrado casi nunca entra por una vulnerabilidad exótica: llega por una credencial de acceso remoto robada o reutilizada, un servicio expuesto a internet sin actualizar, o un archivo adjunto de correo electrónico abierto sin verificar el remitente.

Por qué decide la copia de seguridad

Cuando el ransomware cifra los equipos, la diferencia entre una interrupción de horas y una crisis de semanas suele ser una sola cosa: si existe una copia de seguridad recuperable. Muchos atacantes buscan esa copia antes de cifrar nada. Si la copia de seguridad es accesible desde la misma red, con las mismas credenciales que el resto de sistemas, también queda cifrada o borrada. Una copia conectada de forma permanente es una carpeta más, no una copia de seguridad.

El mínimo práctico

Con recursos limitados no hace falta un departamento de seguridad propio, pero sí una base mínima:

- Copias de seguridad offline o inmutables, desconectadas de la red o protegidas contra modificación
- Restauraciones probadas de verdad, no solo copias que se generan y nunca se abren
- Autenticación multifactor en todo acceso remoto: VPN, escritorio remoto, correo y paneles de gestión
- Parcheo prioritario de cualquier servicio expuesto a internet, empezando por el acceso remoto

Las primeras horas

Si ocurre, aísla los equipos afectados sin apagarlos ni reinstalarlos: apagar borra evidencia útil para entender cómo entraron. Ten decidido de antemano a quién llamar, tu proveedor de ciberseguridad o tu MSP, antes de que ocurra. Si hay indicios de que se han visto afectados datos personales, existe la obligación de evaluar la notificación a la autoridad de control, y el RGPD fija en 72 horas el plazo habitual para hacerlo. La preparación se nota precisamente en las primeras horas.