CIPHRAVERSE

CIPHRAVERSE WHITE PAPER

Ransomware in Companies With No IT Team

An SME with no IT department is not a smaller target for ransomware, it just takes longer to notice and to react. Encryption rarely comes through an exotic vulnerability: it arrives through a stolen or reused credential on remote access, an internet-facing service left unpatched, or an email attachment opened without checking the sender.

Why the backup decides the outcome

When ransomware encrypts your machines, the gap between a few hours of disruption and a weeks-long crisis usually comes down to one thing: whether a recoverable backup exists. Many attackers look for that backup before encrypting anything. If it sits on the same network, reachable with the same credentials as everything else, it gets encrypted or deleted too. A copy that stays permanently connected is just another folder, not a backup.

The practical minimum

Limited resources do not require an in-house security team, but they do require a baseline:

- Offline or immutable backups, disconnected from the network or protected against modification
- Restores that are actually tested, not copies that get created and never opened
- Multi-factor authentication on every remote access point: VPN, remote desktop, email and admin panels
- Priority patching for anything exposed to the internet, starting with remote access

The first hours

If it happens, isolate the affected machines without shutting them down or reinstalling: powering off destroys evidence you need to understand how the attackers got in. Decide in advance who to call, your security provider or your MSP, before the incident, not during it. If there are signs that personal data was affected, there is a duty to assess notifying the supervisory authority, and the regulation sets the usual window for that at 72 hours. Preparation shows precisely in those first hours.