

BR-SYSTEMS · ENGLISH EDITION

Ransomware, backup and recovery

A resilient backup design assumes that attackers may reach ordinary administration.

Personally accountable · clearly documented · vendor-transparent

From concern to an owned action plan

This guide is designed for small and medium-sized organisations that need practical decisions rather than generic fear or a product-first answer.

How to use it

Work through the actions with the people who own the affected business processes. Mark what is already evidenced, assign an owner to every gap and agree a realistic review date.

Decision principles

01	Start from business impact and responsibility.
02	Prefer written evidence over assumed status.
03	Keep alternatives and exit paths visible.
04	Test recovery and operating processes, not only settings.

Important

This publication provides technical orientation. It is not legal advice, a certification or a guarantee of security. Current law, contracts, manufacturer documentation and the organisation's specific risk context remain authoritative.

Practical action checklist

Use the right-hand side of a printed copy for owner, evidence and due date.

01	Separate backup identities, management and network paths.
02	Use immutable or offline protection for critical recovery points.
03	Protect hypervisors, identity systems and backup catalogues first.
04	Monitor deletion, encryption and unusual administrative activity.
05	Keep recovery credentials and keys available out of band.
06	Define clean-room or isolated recovery procedures.
07	Test restoration without trusting the production environment.
08	Prioritise business services and technical dependencies.
09	Retain evidence before rebuilding compromised systems.
10	Review the incident and close the route used by the attacker.

A sensible next step

BR-Systems can help establish the baseline, prioritise the gaps and implement or operate the agreed measures. A short initial consultation is enough to determine whether that would be useful.

br-systems.eu · info@br-systems.eu · +49 179 160 1700