
Checkliste zur Backup-Sicherheit

8 Checks für jede Kundenumgebung, mit denen MSPs Angreifern zuvorkommen.

- ☐ Der Backup-Agent läuft unter einem dedizierten Dienstkonto ohne Domänen-Admin-Rechte und ohne Schreibzugriff auf produktive Freigaben.
- ☐ Die Zugangsdaten für den Backup-Speicher existieren nur in der Backup-Software, sind verschlüsselt gespeichert und werden mit keinem anderen System oder Benutzer geteilt.
- ☐ Der Backup-Speicher (lokal und in der Cloud) wird ausschließlich für Backups genutzt und ist in der Produktivumgebung weder als Netzlaufwerk eingebunden noch durchsuchbar.
- ☐ Die MFA für Backup-Konsolen und Admin-Konten ist phishingresistent (FIDO2 oder Hardware-Key) und basiert nicht auf Push-Benachrichtigungen.
- ☐ Der Speicher außerhalb des Standorts ist unveränderlich, und die zugehörigen Zugangsdaten und Verschlüsselungs-Keys sind außerhalb der Produktivumgebung dokumentiert.
- ☐ Die Aufbewahrungsfrist reicht weiter zurück als eine realistische Verweildauer und ist pro Job und pro Speicherort festgelegt.
- ☐ Wiederherstellungstests laufen nach Zeitplan und nach jeder wesentlichen Änderung, und die Ergebnisse werden protokolliert.
- ☐ Für jeden Kunden und jedes System gibt es eine gemessene RTO aus einem echten Wiederherstellungstest sowie eine dokumentierte Wiederherstellungsreihenfolge.