Checkliste Disaster Recovery

Ist Ihr Unternehmen auf den Katastrophenfall vorbereitet? Testen Sie Ihre Disaster-Recovery-Strategie:

	Ja	Nein
Gelten spezielle Service Level Agreements (SLAs) für Ihre Systeme und Anwendungen?	☐	☐
Gibt es eine Übersicht aller SLAs?	☐	☐
Sind Sie sicher, dass die SLAs im Katastrophenfall eingehalten werden können?	☐	☐
Gibt es in Ihrem Unternehmen einen Disaster Recovery Plan?	☐	☐
Ist der Disaster Recovery dokumentiert?	☐	☐
Gibt es diesen Plan auch in ausgedruckter Form?	☐	☐
Wurde die Wiederherstellung nach diesem Plan getestet?	☐	☐
Werden regelmäßige Recoverytests durchgeführt? Falls ja, wie oft?	☐	☐
monatlich	☐	☐
quartalsweise	☐	☐
seltener	☐	☐
Wird der Disaster Recovery Plan regelmäßig, z. B. im Zuge der Tests, überprüft und ggf. angepasst?	☐	☐
Sind alle Komponenten (Systeme, Kabel, Dosen, etc.) sauber beschriftet?	☐	☐
Steht diese Dokumentation auch in ausgedruckter Form zur Verfügung?	☐	☐
Gibt es für die einzelnen Schritte zur Wiederherstellung einen dedizierten Verantwortlichen?	☐	☐
Ist für alle leicht zugänglich dokumentiert, wie der Verantwortliche im Notfall erreicht werden kann?	☐	☐
Sind alle relevanten Systeme und Komponenten ausfallsicher konzipiert? (Hot- oder Cold Standby)	☐	☐
Gibt es ein Ausfallrechenzentrum?	☐	☐
Sind im Katastrophenfall zusätzliche Ressourcen schnell zu beschaffen?	☐	☐
Ist im Katastrophenfall zusätzliches Personal verfügbar, um z. B. Prozesse oder die Wiederanlaufzeit zu beschleunigen?	☐	☐
Eignet sich die in Ihrem Unternehmen eingesetzte Backuplösung für die Wiederherstellung großer Datenmengen, z. B. durch parallele Restores?	☐	☐
Kann auf Daten/Systeme/Applikationen bei Bedarf innerhalb weniger Minuten, z. B. aus einem Snapshot, zugegriffen werden?	☐	☐
Können Daten/Systeme/Applikationen bei Bedarf per Live-Mount zur Verfügung gestellt werden?	☐	☐
Können unternehmenskritische Daten und Applikationen beim Ausfall physischer Systeme temporär problemlos auf andere virtuelle Systeme oder in die Cloud verschoben werden?	☐	☐
Können betroffene Systeme problemlos auch auf anderer Hardware wiederhergestellt werden, falls die gleiche Hardware nicht oder nicht mehr zur Verfügung steht?	☐	☐
Wie viel Ausfall kann Ihr Unternehmen sich leisten?	☐	☐
keinen	☐	☐
bis 2 Stunden	☐	☐
bis 4 Stunden	☐	☐
bis 8 Stunden	☐	☐
bis 12 Stunden	☐	☐
bis 24 Stunden	☐	☐
länger als einen Tag	☐	☐
Ist die eingesetzte Backuplösung gegen Angriffe von Ransomware geschützt?	☐	☐
Wie schützen Sie Ihre Backup-Daten vor der Verschlüsselung durch Ransomware?	☐	☐
Offline-Kopie (z. B. Tape)	☐	☐
Eingeschränkte Zugriffsrechte (WORM-Funktionalität)	☐	☐
Blockieren unerwünschter Zugriffe (Whitelisting)	☐	☐
Unveränderbare Daten (Immutable Backups)	☐	☐

Diese Checkliste wurde uns freundlicherweise von der Cristie Data GmbH zur Verfügung gestellt.