Conperience

WHITEPAPER FÜR ENTSCHEIDER

Datensicherung ist Chefsache.

Was die Geschäftsführung über Backup & Recovery wissen und entscheiden sollte – damit Ihr Unternehmen nach jedem Vorfall weiterarbeitet.

Backup & Recovery | RTO und RPO | NIS2 | IT-Resilienz

Ausgabe 2026 · www.conperience.com

MANAGEMENT SUMMARY

Die Kernaussagen auf einer Seite

Nach einem Cyberangriff oder Systemausfall zählt nur eins: wie schnell Ihr Unternehmen wieder arbeitsfähig ist. Ob das gelingt, entscheidet sich lange vorher – in der Geschäftsführung.

01 **Die Datensicherung ist das Ziel der Angreifer.**

Wer die Backups zerstört, macht Erpressung erfolgreich. Deshalb greifen Angreifer die Sicherungen zuerst an.

02 **Stillstand ist eine Geschäftszahl.**

Umsatzausfall, Löhne ohne Leistung, Vertragsstrafen und Vertrauensverlust – der Schaden reicht weit über die IT hinaus.

03 **Zwei Fragen muss die Geschäftsführung beantworten.**

Wie lange darf der Betrieb stillstehen (RTO)? Wie viel Arbeit darf verloren gehen (RPO)? Die IT kann das nicht allein entscheiden.

04 **Datensicherung ist Pflicht.**

NIS2, DSGVO, Cyberversicherer und Kunden verlangen funktionierende, getestete Wiederherstellung – und Nachweise.

05 **Ein Backup ist erst gut, wenn es zurückkommt.**

Entscheidend sind getestete Wiederherstellung, eine geschützte Kopie außer Haus und Unabhängigkeit von Einzelpersonen.

06 **Backup ist Teil der Resilienz.**

Erst im Zusammenspiel mit Notfallplan, Rollen und Übungen wird aus einer Sicherung echte Handlungsfähigkeit.

07 **Der Weg ist planbar.**

In sechs Schritten von der Analyse bis zur nachgewiesenen Wiederherstellung.

01 DIE LAGE

Warum die Datensicherung zum Hauptziel geworden ist

Angreifer wissen: Ohne funktionierende Datensicherung zahlt ein Unternehmen eher. Deshalb nehmen sie die Backups gezielt ins Visier – oft lange bevor sie zuschlagen.

Moderne Ransomware-Angriffe laufen selten in Minuten ab. Angreifer bewegen sich häufig Tage oder Wochen unbemerkt im Netzwerk. Ein typischer Ablauf:

1

Eindringen

Über eine Phishing-Mail, gestohlene Zugangsdaten oder eine ungepatchte Schwachstelle.

2

Rechte ausweiten

Schritt für Schritt bis zu Administratorrechten – und damit Zugriff auf zentrale Systeme.

3

Backups ausschalten

Sicherungen löschen, Aufbewahrung verkürzen oder Daten unbemerkt manipulieren.

4

Verschlüsseln und erpressen

Erst wenn keine Wiederherstellung mehr möglich scheint, wird Lösegeld gefordert.

> Unser Ziel ist nicht, Ihnen ein Backup zu verkaufen. Unser Ziel ist, dass Ihr Unternehmen nach jedem Vorfall weiterarbeitet.

Hinzu kommen Gefahren, die nichts mit Angreifern zu tun haben: Hardwaredefekte, Brand, Wasserschaden, versehentliches Löschen oder der Ausfall eines Dienstleisters. Eine gute Datensicherung schützt vor allen diesen Szenarien – wenn sie richtig geplant ist.

02 DIE FOLGEN

Was Sie ein Ausfall wirklich kostet

Stillstand ist keine IT-Kennzahl, sondern eine Geschäftszahl. Wenn Server, Warenwirtschaft oder E-Mail stillstehen, laufen die Kosten weiter – nur die Wertschöpfung nicht.

Umsatz

Aufträge, die nicht angenommen, produziert oder ausgeliefert werden.

Personal

Gehälter für Arbeitszeit ohne Leistung.

Verträge

Lieferverzug, Vertragsstrafen und gebrochene Service-Zusagen.

Vertrauen

Verunsicherte Kunden und Partner, Reputationsschaden.

Wiederanlauf

Nacharbeit, externe Hilfe, Forensik und Überstunden.

Folgekosten

Höhere Versicherungsprämien und verlorene Aufträge.

Zwei Fragen, die jede Geschäftsführung beantworten sollte

1

Wie viele Stunden Stillstand verkraftet Ihr Betrieb?

Daraus ergibt sich, wie schnell die Wiederherstellung gelingen muss.

Tragbare Ausfallzeit · RTO

2

Wie viel Arbeit darf im Ernstfall verloren gehen?

Daraus ergibt sich, wie oft gesichert werden muss.

Tragbarer Datenverlust · RPO

03 DIE RICHTIGEN ZIELE

RTO, RPO und MTTR – verständlich erklärt

Drei Kennzahlen übersetzen Ihre geschäftlichen Erwartungen in klare Ziele für Datensicherung, Notfallplanung und Budget. Stellen Sie sich einen Zeitstrahl vor: Was vor dem Vorfall liegt, bestimmt Ihren Datenverlust. Was danach kommt, Ihren Stillstand.



RTO – tragbare Ausfallzeit

Ab wann wird ein Ausfall wirklich teuer oder gefährlich? Selten für alle Systeme gleich: Der Onlineshop braucht Stunden, das Archiv kann Tage warten.

RPO – tragbarer Datenverlust

Wie alt dürfen die Daten nach einer Wiederherstellung höchstens sein? Ein RPO von 24 Stunden heißt: Im schlimmsten Fall ist ein Arbeitstag verloren.

MTTR – tatsächliche Dauer

Der Realitätscheck: Wie lange dauert die Wiederherstellung heute wirklich? Liegt sie über dem RTO, haben Sie ein Problem, das Sie jetzt kennen sollten.

Nicht jedes System braucht dasselbe Schutzniveau

Geschäftskritisch

z. B. Warenwirtschaft, Produktion, Onlineshop

Ausfall wird nach wenigen Stunden teuer. Häufige Sicherung und schneller Wiederanlauf haben Vorrang.

Wichtig

z. B. E-Mail, Dateiablage, Buchhaltung

Ein Tag Ausfall ist ärgerlich, aber überbrückbar. Tägliche Sicherung reicht meist aus.

Unterstützend

z. B. Archive, Intranet, Testsysteme

Kann einige Tage warten. Kostengünstige, aber zuverlässige Sicherung.

04 PFLICHT, NICHT KÜR

Compliance, Haftung und Versicherung

Eine funktionierende Datensicherung ist längst keine rein technische Entscheidung mehr. Gesetzgeber, Versicherer und Geschäftspartner erwarten, dass Sie Ihre Daten im Ernstfall wiederherstellen können – und das auch belegen.

NIS2 und Haftung der Geschäftsleitung

Die NIS2-Richtlinie nennt Backup-Management und Wiederherstellung ausdrücklich als Pflichtmaßnahmen. Die Geschäftsleitung betroffener Unternehmen muss diese Maßnahmen billigen, ihre Umsetzung überwachen und kann persönlich haftbar gemacht werden.

Datenschutz (DSGVO)

Wer personenbezogene Daten verarbeitet, muss nach Art. 32 DSGVO sicherstellen, dass Verfügbarkeit und Zugang zu diesen Daten nach einem Zwischenfall rasch wiederhergestellt werden können.

Cyberversicherung

Versicherer fragen gezielt nach getrennten, unveränderlichen Sicherungen und regelmäßigen Wiederherstellungstests. Fehlen sie, kann das die Prämie erhöhen oder im Schadensfall die Leistung gefährden.

Nachweisbarkeit

Berichte und Testprotokolle belegen, dass Ihre Datensicherung funktioniert – gegenüber Wirtschaftsprüfern, Auditoren, Versicherern und Kunden, die das in Lieferantenbewertungen zunehmend verlangen.

Für die Geschäftsführung heißt das: Die Frage „Funktioniert unsere Datensicherung?“ muss mit Belegen beantwortet werden können – nicht mit einem Bauchgefühl.

Hinweis: Diese Übersicht ersetzt keine Rechtsberatung.

05 IHR ANSPRUCH

Was Sie von Ihrer Datensicherung erwarten dürfen

Gewissheit statt Hoffnung

„Die Sicherung läuft doch“ reicht nicht. Entscheidend ist, ob sich Ihre Daten im Ernstfall tatsächlich wiederherstellen lassen. Regelmäßige Wiederherstellungstests und ein verständlicher Bericht schaffen Gewissheit.

Schnell wieder arbeitsfähig

Im Ernstfall zählt jede Stunde. Eine professionelle Lösung stellt geschäftskritische Systeme zuerst und in kürzester Zeit wieder bereit.

Unabhängig von Einzelpersonen

Im Notfall darf es nicht davon abhängen, ob der eine Kollege erreichbar ist. Wiederherstellungen sind dokumentiert und ohne Spezialwissen durchführbar.

Schutz vor Erpressung

Getrennte Kopien und unveränderliche Sicherungen können für einen festgelegten Zeitraum niemand ändern oder löschen – auch nicht mit Administratorrechten.

Die 3-2-1-Regel – das Fundament

3
Kopien Ihrer Daten
Das Original und zwei Sicherungen.

2
Verschiedene Speichermedien
Ein Defekt trifft nie alle Kopien gleichzeitig.

1
Kopie außer Haus
Getrennt vom Firmennetz, an einem anderen Ort.

Viele Unternehmen ergänzen die Regel heute um unveränderliche Kopien und regelmäßig geprüfte Wiederherstellungen.

06 DIE KOPIE AUSSER HAUS

Ihr Rettungsanker – sicher, getrennt und geschützt

Ist Ihr Standort nach Brand, Wasserschaden, Einbruch oder Cyberangriff nicht nutzbar, liegen Ihre Daten sicher woanders.

Wo diese externe Kopie liegt, ist eine Geschäftsentscheidung: an einem zweiten eigenen Standort, bei einem Cloud-Anbieter Ihrer Wahl oder in einem ISO-27001-zertifizierten Rechenzentrum. Entscheidend sind Kosten, Datenschutz, Standort – und die Frage, wie unabhängig Sie von einzelnen Anbietern bleiben wollen.

Getrennt vom Firmennetz

Ein Angriff auf Ihr Netzwerk erreicht die externe Kopie nicht.

Verschlüsselt übertragen

Die Daten verlassen Ihr Haus nur verschlüsselt.

Löschschutz (Insider Protection)

Selbst mit erbeuteten Zugangsdaten werden gelöschte Sicherungen für einen festgelegten Zeitraum in einem isolierten Bereich zurückgehalten.

Wächst mit Ihrem Bedarf

Mehr Daten, neue Standorte, zusätzliche Systeme – ohne neues Projekt.

> **Datensouveränität mitdenken:** Wer seine einzige Kopie bei demselben Anbieter hält wie die Produktivdaten, ist bei dessen Ausfall oder Vertragsänderung doppelt betroffen. Eine unabhängige Kopie ist auch eine Exit-Strategie – etwa für Microsoft 365.

07 PRAXISBEISPIEL

Die Datensicherung sicher außer Haus bringen

Branche Chemie | **Region** Süddeutschland | **Umfang** rund 40 virtuelle Server | **Daten** rund 30 TB

AUSGANGSLAGE

Die Datensicherung läuft zuverlässig, aber ausschließlich im eigenen Haus. Original und Sicherungen liegen am selben Standort – die 3-2-1-Regel ist nicht erfüllt.

ZIEL

Eine Kopie soll in eine gemanagte Cloud-Umgebung – verschlüsselt übertragen, in einem ISO-27001-zertifizierten Rechenzentrum, ohne eigenen Zweitstandort.

LÖSUNG

Anbindung der vorhandenen Backup-Software an einen Cloud-Dienst für Backup-Kopien. Die Sicherungen werden verschlüsselt in ein entferntes Rechenzentrum übertragen und dort gemanagt.

≈ 40	≈ 30 TB	3-2-1	ISO 27001
virtuelle Server eingebunden	Datenvolumen außer Haus	Regel erfüllt	zertifiziertes Rechenzentrum

Warum keine neue Backup-Software? Herstellerneutral heißt nicht, immer etwas Neues einzuführen. Die vorhandene Lösung funktionierte, das Team kannte sie, die Investition war getätigt. Statt einer Neuausrichtung wurde gezielt das fehlende Glied ergänzt: die Kopie außer Haus. Das spart Kosten, Zeit und Einarbeitung.

Weitere Praxisbeispiele: www.conperience.com/case-studies/

08 IHR WEG

In sechs Schritten zur verlässlichen Datensicherung

Eine gute Datensicherung beginnt nicht mit Technik, sondern mit der Frage, was Ihr Unternehmen im Ernstfall braucht.

1

Beratung und Analyse

Geschäftskritische Prozesse, tragbare Ausfallzeiten und offene Pflichten klären.

Ergebnis: Risiko- und Lückenanalyse für die Geschäftsleitung

2

Sicherungsstrategie

Was wird wie oft, wo und wie lange gesichert – nach der 3-2-1-Regel und mit Kopie außer Haus.

Ergebnis: dokumentiertes Datensicherungskonzept

3

Disaster-Recovery-Planung

Wiederanlaufreihenfolge, Ersatzsysteme und Anleitungen für den schweren Ausfall.

Ergebnis: Plan mit realistischen Wiederanlaufzeiten

4

Notfallkonzept

Rollen, Alarmierung, Kommunikation und Meldepflichten – im ganzen Unternehmen.

Ergebnis: Notfallhandbuch, das auch unter Druck funktioniert

5

Umsetzung

Herstellerneutral – im eigenen Haus, bei einem Cloud-Anbieter oder im zertifizierten Rechenzentrum.

Ergebnis: nachweislich wiederherstellbare Datensicherung

6

Tests und laufender Betrieb

Regelmäßige Wiederherstellungstests, Übungen und Berichte für Geschäftsleitung, Prüfer und Versicherer.

Ergebnis: dauerhafte Gewissheit statt einmaliger Einrichtung

09 SELBSTCHECK

Zehn Fragen für die Geschäftsleitung

Zählen Sie für jedes „Ja“ zwei Punkte, für „Teilweise“ einen Punkt.

01	Wissen wir, welche Systeme nach einem Ausfall zuerst wieder laufen müssen?	☐ Ja ☐ Teilw. ☐ Nein
02	Haben wir für diese Systeme RTO und RPO festgelegt – und freigegeben?	☐ Ja ☐ Teilw. ☐ Nein
03	Wurde in den letzten zwölf Monaten eine vollständige Wiederherstellung getestet?	☐ Ja ☐ Teilw. ☐ Nein
04	Wissen wir, wie lange eine Wiederherstellung tatsächlich dauert?	☐ Ja ☐ Teilw. ☐ Nein
05	Liegt eine Kopie unserer Daten außer Haus und getrennt vom Firmennetz?	☐ Ja ☐ Teilw. ☐ Nein
06	Sind unsere Sicherungen vor Löschung und Verschlüsselung geschützt?	☐ Ja ☐ Teilw. ☐ Nein
07	Funktioniert die Wiederherstellung auch ohne einzelne Schlüsselpersonen?	☐ Ja ☐ Teilw. ☐ Nein
08	Gibt es einen Notfallplan, der auch auf Papier verfügbar ist?	☐ Ja ☐ Teilw. ☐ Nein
09	Sind auch Cloud-Daten, etwa aus Microsoft 365, unabhängig gesichert?	☐ Ja ☐ Teilw. ☐ Nein
10	Könnten wir Prüfern oder unserer Cyberversicherung all das belegen?	☐ Ja ☐ Teilw. ☐ Nein

16–20 Punkte

Gut aufgestellt. Halten Sie Ihre Datensicherung durch Tests lebendig.

9–15 Punkte

Solide Basis mit Lücken. Schließen Sie die offenen Punkte gezielt.

0–8 Punkte

Dringender Handlungsbedarf. Beginnen Sie mit Analyse und Kopie außer Haus.

ÜBER CONPERIENCE

Beratung statt Produktverkauf.

Viele Anbieter beginnen mit ihrem Produkt. Wir beginnen mit Ihrem Unternehmen – und entwickeln eine Datensicherung, die zu Ihren Prozessen, Ihrer IT-Landschaft und Ihren Zielen passt.

Als unabhängiger Partner für Technologie, Architektur, Resilienz und Datensouveränität sind wir an keinen Hersteller gebunden. Bestehende Systeme beziehen wir ein, statt sie ohne Not zu ersetzen. Von der Analyse über Konzept und Notfallplanung bis zum laufenden Betrieb – ein Ansprechpartner, der Verantwortung übernimmt.

Backup-Check

Bestandsaufnahme Ihrer Datensicherung mit Bericht für die Geschäftsleitung.

RTO/RPO-Workshop

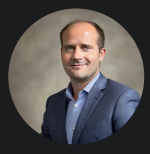
Zielwerte gemeinsam mit Geschäftsführung und Fachbereichen festlegen.

Offsite-Backup

Ihre Kopie außer Haus – verschlüsselt und im zertifizierten Rechenzentrum.



Christian Habel
Gründer & Geschäftsführer



Andreas Habel
Gründer & Geschäftsführer

TELEFON
(+49) 040 607 74 74 - 0

E-MAIL
info@conperience.com

WEB
www.conperience.com

Conperience GmbH · Burgblick 26 · 55595 Gutenberg · © 2026. Alle Angaben ohne Gewähr; dieses Whitepaper ersetzt keine Rechtsberatung.