Conperience

WHITEPAPER FÜR ENTSCHEIDER

Resilienz, die sich rechnet.

Wie Unternehmen Ausfallsicherheit, Regulierung und Innovation in einer IT-Strategie vereinen.

NIS2 | Dual Use | Souveräne KI | Business Continuity

Ausgabe 2026 · www.conperience.com

MANAGEMENT SUMMARY

Die Kernaussagen auf einer Seite

IT-Ausfälle sind keine Frage des Ob, sondern des Wann. Wer seine Notfallvorsorge klug plant, erfüllt Pflichten, senkt Risiken – und schafft gleichzeitig Raum für Innovation.

01 **Die Lage hat sich verschärft.**

Ransomware, Ausfälle bei Cloud- und IT-Dienstleistern sowie geopolitische Risiken treffen zunehmend auch den Mittelstand.

02 **Resilienz ist Pflicht, nicht Kür.**

NIS2 nimmt die Geschäftsleitung persönlich in die Verantwortung. Versicherer und Kunden verlangen Nachweise über Notfallvorsorge und getestete Wiederherstellung.

03 **Klassische Notfallvorsorge gilt als totes Kapital.**

Ein Ausweich-Rechenzentrum, das nur auf den Ernstfall wartet, ist schwer zu rechtfertigen – und wird deshalb oft zu klein oder gar nicht umgesetzt.

04 **Dual Use löst das Dilemma.**

Die Backup-Infrastruktur arbeitet im Alltag für Tests, Analysen und KI – und übernimmt im Notfall sofort die kritischen Systeme.

05 **Eigene Infrastruktur ist die Basis für souveräne KI.**

Sensible Daten bleiben im Haus, Abhängigkeiten von einzelnen Anbietern sinken.

06 **Resilienz rechnet sich.**

Bereits wenige vermiedene Ausfalltage können die jährlichen Kosten der Vorsorge übersteigen. Dual Use verbessert die Rechnung zusätzlich.

07 **Der Weg ist planbar.**

In fünf Schritten von der Analyse bis zum getesteten Notfallbetrieb – pragmatisch und passend zur Größe Ihres Unternehmens.

01 DIE NEUE LAGE

Wenn die IT steht, steht das Geschäft

Aufträge, Produktion, Logistik, Buchhaltung, Kundenkontakt: Fast jeder Prozess hängt heute an IT. Gleichzeitig haben sich die Risiken grundlegend verändert.

Cyberangriffe

Ransomware gilt seit Jahren als größte Bedrohung für Unternehmen. Angreifer verschlüsseln nicht nur, sie stehlen vorher Daten und zielen gezielt auf die Datensicherung. Phishing und Betrug werden durch KI glaubwürdiger und zahlreicher.

Ausfälle bei Anbietern

Cloud-Plattformen, Software-as-a-Service und IT-Dienstleister fallen aus – durch Störungen, fehlerhafte Updates oder Angriffe. Wer vollständig auf einen Anbieter setzt, steht im Ernstfall mit ihm still.

Geopolitische Risiken

Sanktionen, Handelskonflikte und staatlich gesteuerte Angriffe sind keine Theorie mehr. Abhängigkeiten von Anbietern außerhalb Europas werden zum strategischen Risiko.

Lieferkette

Angreifer kommen immer häufiger über Partner, Dienstleister oder Software-Updates ins Unternehmen. Ihre Sicherheit ist nur so stark wie das schwächste Glied.

rund 9 von 10

Unternehmen in Deutschland waren laut Bitkom-Studie zum Wirtschaftsschutz zuletzt von Datendiebstahl, Spionage oder Sabotage betroffen.

Quelle: Bitkom, Studie Wirtschaftsschutz

> Die entscheidende Frage ist nicht, ob ein schwerer Ausfall kommt – sondern wie schnell Ihr Unternehmen danach wieder arbeitet.

02 PFLICHT STATT KÜR

Resilienz ist Chefsache – auch rechtlich

IT-Sicherheit und Notfallvorsorge sind für viele mittelständische Unternehmen längst gesetzliche Pflicht. Und die Verantwortung liegt ausdrücklich bei der Geschäftsleitung.

NIS2: Mit dem NIS2-Umsetzungsgesetz fallen in Deutschland Zehntausende Unternehmen unter die Regeln – häufig schon ab 50 Mitarbeitenden oder 10 Millionen Euro Jahresumsatz in den betroffenen Branchen. Gefordert sind unter anderem Risikomanagement, Notfallmanagement, Backup und Wiederherstellung, Sicherheit in der Lieferkette und Meldepflichten.

§

Haftung der Geschäftsleitung

Die Geschäftsleitung muss Maßnahmen billigen, ihre Umsetzung überwachen und regelmäßig an Schulungen teilnehmen. Bei Pflichtverletzungen droht persönliche Haftung.

€

Anforderungen der Versicherer

Cyberversicherer fragen nach getrennten, unveränderlichen Backups, Mehr-Faktor-Anmeldung und Notfallplänen. Lücken verteuern die Police oder gefährden die Leistung.

✓

Erwartungen der Kunden

Große Auftraggeber geben ihre Pflichten an Zulieferer weiter: Fragebögen, Audits und Nachweise entscheiden zunehmend über Aufträge.

Was Prüfer, Versicherer und Kunden sehen wollen

- ✓ Eine dokumentierte Analyse der geschäftskritischen Prozesse und Systeme
- ✓ Festgelegte Ziele für tragbare Ausfallzeit (RTO) und tragbaren Datenverlust (RPO)
- ✓ Einen aktuellen Notfallplan mit klaren Zuständigkeiten
- ✓ Regelmäßige, dokumentierte Wiederherstellungstests
- ✓ Eine geschützte Kopie der Daten außer Haus

Hinweis: Diese Übersicht ersetzt keine Rechtsberatung. Ob und in welchem Umfang Ihr Unternehmen betroffen ist, sollte im Einzelfall geprüft werden.

03 DAS DILEMMA

Warum klassische Notfallvorsorge als totes Kapital gilt

> „Wir zahlen viel Geld für etwas, das hoffentlich nie gebraucht wird."

Diesen Satz hören wir in fast jedem Gespräch über Notfallvorsorge. Er beschreibt ein echtes Dilemma: Ein Ausweich-Rechenzentrum oder eine vollständige Ersatzinfrastruktur kostet Geld für Hardware, Strom, Lizenzen und Betrieb – und steht doch die meiste Zeit ungenutzt da.

Die Folgen sind in vielen Unternehmen zu beobachten:

Die Investition wird aufgeschoben

Notfallvorsorge konkurriert mit Projekten, die sichtbaren Nutzen bringen – und verliert.

Sie wird zu klein dimensioniert

Im Ernstfall reicht die Kapazität nicht, um alle kritischen Systeme zu betreiben.

Sie wird nicht getestet

Was nie genutzt wird, veraltet unbemerkt. Ob es funktioniert, zeigt sich erst im Notfall.

Sie wird abgeschafft

Bei der nächsten Sparrunde fällt der „ungenutzte" Posten als Erstes weg.

Das eigentliche Problem: Notfallvorsorge wird als reiner Kostenblock betrachtet. Solange das so ist, bleibt sie ein schwer zu verteidigender Posten. Die Lösung liegt darin, die Vorsorge so zu gestalten, dass sie auch im Alltag Wert schafft.

04 DER DUAL-USE-ANSATZ

Backup-Infrastruktur, die im Alltag arbeitet

Bei einer Dual-Use-Strategie übernimmt das Ausweich-Rechenzentrum zwei klar getrennte Rollen – abhängig davon, ob der Hauptstandort läuft oder ausgefallen ist.

IM NORMALBETRIEB

Sinnvolle, nicht geschäftskritische Aufgaben

Tests, Analysen, KI-Projekte und Schulungsumgebungen – das Rechenzentrum arbeitet täglich und schafft Mehrwert.

NOTFALL →

IM NOTFALL

Die kritischen Systeme haben Vorrang

Alltagsaufgaben werden verdrängt, das Rechenzentrum übernimmt sofort die geschäftskritischen Systeme.

Typische Nutzungen im Normalbetrieb

Entwicklung und Test

Realistische Testumgebungen nah am produktiven System.

Wiederherstellungstests

Backups regelmäßig zurückspielen und Notfälle üben – ohne Störung des Betriebs.

Datenanalyse und Reporting

Auswertungen auf Datenkopien entlasten die produktiven Systeme.

KI-Workloads

Modelle trainieren und erproben, Daten lokal und souverän verarbeiten.

Schulung und Sandbox

Umgebungen für Mitarbeitende, Schulungen und Pilotprojekte.

Lastverteilung

Lastspitzen abfangen oder ausgewählte Systeme aktiv-aktiv betreiben.

DER DUAL-USE-ANSATZ

Nutzen und Voraussetzungen

Der Nutzen für Entscheider

- ✓ **Bessere Wirtschaftlichkeit:** Die Investition arbeitet täglich, nicht nur im Ernstfall.
- ✓ **Höhere Resilienz:** Ein ständig genutztes Rechenzentrum ist nachweislich funktionsfähig – keine bösen Überraschungen.
- ✓ **Getestete Wiederherstellung:** Wichtig für NIS2, Auditoren und Cyberversicherer.
- ✓ **Innovation ohne Zusatzinvestition:** Raum für KI, Tests und neue Projekte.
- ✓ **Souveränität:** Eigene Infrastruktur statt vollständiger Abhängigkeit von der Cloud.

Worauf Sie achten müssen

- **Klare Rangfolge:** Im Notfall steht fest, welche Systeme verdrängt werden und welche hochfahren – automatisiert und dokumentiert.
- **Kapazitätsplanung:** Der Notbetrieb muss auch dann funktionieren, wenn das Rechenzentrum vorher ausgelastet war.
- **Trennung und Sicherheit:** Getrennte Netzsegmente und unveränderbare Backups schützen die Notfallsysteme.
- **Räumliche Entfernung:** Weit genug vom Hauptstandort, damit regionale Ereignisse nicht beide treffen.
- **Lizenzen:** Aktive Nutzung kann zusätzliche Lizenzkosten auslösen – vorab prüfen.
- **Daten in Testumgebungen:** Echte Daten erfordern Datenschutzmaßnahmen wie Anonymisierung.

> Ein Rechenzentrum, das täglich arbeitet, ist ein Rechenzentrum, von dem Sie wissen, dass es im Ernstfall funktioniert.

Wichtig: Dual Use funktioniert nur mit einer klaren Trennung zwischen Alltags- und Notfallbetrieb. Die Rangfolge der Systeme gehört in den Notfallplan und sollte regelmäßig geübt werden.

05 KI SOUVERÄN NUTZEN

Eigene Infrastruktur als Basis für sichere KI

Künstliche Intelligenz wird geschäftskritisch. Und alles, was geschäftskritisch ist, muss sicher, souverän und ausfallsicher sein.

KI automatisiert Routinearbeit, macht Wissen nutzbar und entlastet Teams. Gleichzeitig entstehen neue Risiken: Mitarbeitende kopieren vertrauliche Daten in öffentliche KI-Tools, Abhängigkeiten von einzelnen Anbietern wachsen, und der EU AI Act verlangt unter anderem KI-Kompetenz im Unternehmen.

Daten bleiben im Haus

Sensible Kunden-, Konstruktions- oder Personaldaten werden auf eigener Infrastruktur verarbeitet – nicht in fremden Clouds.

Weniger Abhängigkeit

Eigene oder europäische Modelle reduzieren das Risiko von Preis- und Bedingungsänderungen einzelner Anbieter.

Rechenleistung, die schon da ist

Im Dual-Use-Rechenzentrum stehen Kapazitäten für Training und Erprobung bereit – ohne Zusatzinvestition.

Kontrolle und Nachvollziehbarkeit

Zugriffsrechte, Protokollierung und Datenhaltung liegen in Ihrer Hand – wichtig für Datenschutz und Regulierung.

> **Die Verbindung:** Dieselbe Infrastruktur, die Ihr Unternehmen im Notfall rettet, wird im Alltag zur Plattform für souveräne KI-Projekte. Resilienz und Innovation schließen sich nicht aus – sie bedingen einander.

06 PRAXISBEISPIEL

Weiterarbeiten, auch wenn der Hauptstandort ausfällt

Branche Elektrobranche

Standort Hamburg

Größe Mittelstand, rund 250 Mitarbeitende

Thema Erhöhung der Resilienz

AUSGANGSLAGE

Der gesamte Betrieb läuft auf einem Proxmox-Cluster mit drei Nodes am Hauptstandort. Bei einem Ausfall des gesamten Standorts gibt es keinen Ort, an dem der Betrieb weiterlaufen kann.

ZIEL

Ein externes Rechenzentrum übernimmt bei Ausfall des Hauptstandorts und stellt alle Systeme bereit. Die Mitarbeitenden verbinden sich wie im Notfallplan vorgesehen und arbeiten weiter.

LÖSUNG

Erweiterung der Proxmox-Umgebung auf ein zweites Rechenzentrum. Über den Proxmox Backup Server werden Snapshots übertragen und dort einsatzbereit vorgehalten.

1–3 h
RPO, bewusst bandbreitenverträglich gewählt

≈ 4 h
RTO, durch Tests sicher nachgewiesen

2
Rechenzentren, Haupt- und Ausweichstandort

100 %
der Systeme im Ausweich-Rechenzentrum verfügbar

Warum kein direkter Failover im Cluster? Ein automatisches Umschalten über beide Standorte hätte eine sehr hohe Bandbreite erfordert – unverhältnismäßig teuer. Die Übertragung von Snapshots erreicht mit der vorhandenen Anbindung ein Schutzniveau, das zu den tatsächlichen Anforderungen passt. Genau diese Abwägung zwischen Aufwand und Nutzen ist der Kern guter Architekturberatung.

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

07 WIRTSCHAFTLICHKEIT

Was ein Ausfall kostet – und was Vorsorge kostet

Die Kosten eines Ausfalls stehen selten auf einer einzigen Rechnung. Wer sie einmal strukturiert betrachtet, sieht die Vorsorge mit anderen Augen.

Die Kosten eines Ausfalls

- **Entgangener Umsatz:** Aufträge, die nicht angenommen, produziert oder ausgeliefert werden
- **Produktivitätsverlust:** Löhne für Arbeitszeit ohne Leistung
- **Vertragsstrafen und Schadenersatz:** verpasste Liefertermine und Service-Zusagen
- **Wiederherstellung:** Forensik, externe Hilfe, Überstunden und Nacharbeit
- **Folgeschäden:** Kundenverlust, Reputationsschaden, höhere Versicherungsprämien

Die Kosten der Vorsorge

- Hardware, Speicher und Netzanbindung am Ausweichstandort (abgeschrieben über die Nutzungsdauer)
- Rechenzentrumsfläche, Strom und Kühlung oder entsprechende Dienstleistung
- Lizenzen für Sicherung, Replikation und Betrieb
- Betreuung, Tests und Pflege des Notfallplans

Die Faustformel: Ausfallkosten pro Tag = (Jahresumsatz ÷ Arbeitstage × Anteil des betroffenen Umsatzes) + Personalkosten pro Tag + Zusatzkosten für Wiederherstellung und Folgeschäden.

WIRTSCHAFTLICHKEIT

Eine Beispielrechnung

Die folgenden Werte sind **fiktive Annahmen** für ein mittelständisches Unternehmen mit 250 Mitarbeitenden und 50 Mio. € Jahresumsatz. Sie dienen der Veranschaulichung und ersetzen keine individuelle Betrachtung.

Szenario: 5 Arbeitstage Ausfall ohne Vorsorge

Position	Betrag
Entgangener Umsatz (50 Mio. € ÷ 220 Tage × 5 Tage × 60 % betroffen)	≈ 680.000 €
Personalkosten ohne Leistung (250 × 300 € × 5 Tage × 50 %)	≈ 190.000 €
Wiederherstellung, Forensik, externe Hilfe	≈ 120.000 €
Vertragsstrafen und Folgeschäden (Annahme)	≈ 100.000 €
Geschätzter Gesamtschaden	**≈ 1,1 Mio. €**

Vorsorge mit Dual-Use-Rechenzentrum pro Jahr

Position	Betrag
Infrastruktur am Ausweichstandort (abgeschrieben)	≈ 60.000 €
Betrieb, Lizenzen, Anbindung	≈ 50.000 €
Tests, Übungen, Pflege des Notfallplans	≈ 20.000 €
Abzüglich ersetzter Test- und Analyseumgebungen (Dual Use)	≈ – 40.000 €
Netto-Kosten der Vorsorge pro Jahr	**≈ 90.000 €**

≈ 1 : 12

In diesem Beispiel entsprechen die jährlichen Netto-Kosten der Vorsorge weniger als einem halben Ausfalltag. Selbst wenn ein schwerer Ausfall nur alle paar Jahre eintritt, rechnet sich die Vorsorge – zusätzlich zu den Pflichten aus NIS2 und den Anforderungen der Versicherer.

Fiktive Beispielwerte zur Veranschaulichung. Ihre Zahlen ermitteln wir gern gemeinsam mit Ihnen.

08 FAHRPLAN

In fünf Schritten zum getesteten Notfallbetrieb

Pragmatisch, herstellerneutral und passend zur Größe Ihres Unternehmens.

1

Analyse

Geschäftskritische Prozesse, Systeme und Abhängigkeiten erfassen. Tragbare Ausfallzeiten (RTO) und Datenverluste (RPO) gemeinsam mit der Geschäftsleitung festlegen.

Ergebnis: Business-Impact-Analyse und Prioritäten

2

Zielbild und Architektur

Ausweichstandort, Sicherungs- und Replikationsverfahren sowie die Dual-Use-Nutzung im Alltag planen – passend zu Bandbreite, Budget und vorhandener Infrastruktur.

Ergebnis: Architekturkonzept mit Aufwand und Nutzen

3

Umsetzung

Infrastruktur aufbauen, Sicherungen und Replikation einrichten, Netzsegmente trennen und unveränderliche Backups anlegen.

Ergebnis: einsatzbereite Ausweich-Infrastruktur

4

Notfallplan und Rangfolge

Rollen, Alarmierung, Wiederanlaufreihenfolge und die Verdrängung der Alltagsaufgaben im Notfall dokumentieren.

Ergebnis: IT-Notfallplan und Notfallhandbuch

5

Test und Übung

Wiederherstellung und Umschaltung regelmäßig testen, Ergebnisse dokumentieren und Pläne verbessern.

Ergebnis: nachgewiesene Wiederanlaufzeit für Prüfer und Versicherer

09 SELBSTCHECK

Zehn Fragen für die Geschäftsleitung

Beantworten Sie die Fragen ehrlich. Zählen Sie für jedes „Ja“ zwei Punkte, für „Teilweise“ einen Punkt.

01	Wissen wir, welche Prozesse geschäftskritisch sind und wie lange sie ausfallen dürfen?	☐ Ja ☐ Teilw. ☐ Nein
02	Haben wir für unsere wichtigsten Systeme RTO und RPO festgelegt?	☐ Ja ☐ Teilw. ☐ Nein
03	Wissen wir, ob wir unter NIS2 fallen, und kennt die Geschäftsleitung ihre Pflichten?	☐ Ja ☐ Teilw. ☐ Nein
04	Gibt es eine geschützte, unveränderliche Kopie unserer Daten außer Haus?	☐ Ja ☐ Teilw. ☐ Nein
05	Könnten wir weiterarbeiten, wenn unser Hauptstandort mehrere Tage ausfällt?	☐ Ja ☐ Teilw. ☐ Nein
06	Wurde in den letzten zwölf Monaten eine vollständige Wiederherstellung getestet?	☐ Ja ☐ Teilw. ☐ Nein
07	Gibt es einen aktuellen Notfallplan – auch auf Papier?	☐ Ja ☐ Teilw. ☐ Nein
08	Kennen wir unsere Abhängigkeiten von Cloud- und IT-Dienstleistern?	☐ Ja ☐ Teilw. ☐ Nein
09	Nutzen wir unsere Notfall-Infrastruktur auch im Alltag sinnvoll?	☐ Ja ☐ Teilw. ☐ Nein
10	Gibt es Regeln für den Einsatz von KI und den Umgang mit Daten dabei?	☐ Ja ☐ Teilw. ☐ Nein

16–20 Punkte

Gut aufgestellt. Halten Sie Ihre Vorsorge durch regelmäßige Tests lebendig.

9–15 Punkte

Solide Basis mit Lücken. Priorisieren Sie die offenen Punkte.

0–8 Punkte

Dringender Handlungsbedarf. Beginnen Sie mit Analyse und Notfallplan.

ÜBER CONPERIENCE

Challenges simplified.

Wir sind Ihr unabhängiger Ansprechpartner für Technologie, Architektur, Resilienz und Datensouveränität – hersteller- und produktneutral, vom Mittelstand bis zum Konzern.

Wie ein Fachanwalt oder der Arzt Ihres Vertrauens hören wir zuerst zu, analysieren unabhängig und empfehlen, was für Ihr Unternehmen richtig ist – nicht, was sich am besten verkaufen lässt. Hinter uns steht ein großes Team erfahrener Spezialistinnen und Spezialisten: von ISO-Zertifizierung, NIS2 und Business Continuity Management bis zur Netzwerk- und Sicherheitstechnik.

Resilienz-Check

Kompakte Bestandsaufnahme mit Bericht für die Geschäftsleitung.

Workshop Geschäftsleitung

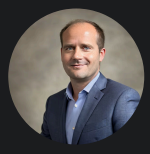
Pflichten, Risiken und eine Krisenübung am realistischen Szenario.

Dual-Use-Konzept

Ihre Notfall-Infrastruktur wirtschaftlich und souverän geplant.



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.