

Disaster Recovery (DR): Notfallvorsorge für IT und Lieferkette

Disaster Recovery (DR) umfasst alle organisatorischen, technischen und vertraglichen Maßnahmen, um nach einem schweren Störfall den Betrieb kritischer Systeme, Prozesse und Lieferbeziehungen wiederherzustellen. Für technische Einkäufer betrifft DR nicht nur die eigene IT, sondern insbesondere die Ausfallsicherheit von Zulieferern und Fertigungsstandorten. Ein funktionierender DR-Konzept reduziert Stillstandszeiten, schützt Vertragsbeziehungen und sichert die Lieferfähigkeit gegenüber Endkunden. Im Folgenden werden Begriffsabgrenzung, Methoden, Kennzahlen, Risiken und aktuelle Entwicklungen praxisnah erläutert.

Das Wichtigste in Kürze

- Disaster Recovery bezeichnet die geplante Wiederherstellung kritischer Systeme und Prozesse nach einem Ausfall oder Katastrophenfall.
- Zentrale Planungsgrößen sind Recovery Time Objective (RTO) und Recovery Point Objective (RPO).
- Im Einkauf zählt vor allem die DR-Fähigkeit von Lieferanten: Fertigungs-/IT-Ausfälle dort können direkte Lieferausfälle verursachen.
- DR-Anforderungen sollten vertraglich fixiert werden, etwa über ein Master Service Agreement (MSA) mit dokumentierten Ausfallkonzepten.
- Regelmäßige Tests und Übungen sind Pflichtbestandteil eines wirksamen DR-Konzepts; unverprobte Pläne bieten in der Praxis kaum Schutz.
- DR ist Teil des Business Continuity Managements und eng mit Risikomanagement und Lieferantenausfallplanung verzahnt.

Definition: Disaster Recovery

Disaster Recovery (DR) ist die Gesamtheit von Maßnahmen, Verfahren und technologischen Lösungen, um nach einem schwerwiegenden Störfall – etwa Brand, Cyberangriff, Naturkatastrophe oder großflächigem IT-Ausfall – den Geschäftsbetrieb wiederherzustellen. DR ist ein Teilbereich des Business Continuity Managements (BCM) und konzentriert sich auf die technische und prozessuale Wiederanlaufphase.

Abgrenzung zur Business Continuity

Business Continuity zielt darauf ab, kritische Prozesse während einer Störung aufrechterhalten zu können, etwa durch Ausweichstandorte oder Notbetriebe. Disaster Recovery beginnt dort, wo ein Betrieb unterbrochen wurde, und beschreibt die planvolle Rückkehr zum Normalzustand. In der Praxis werden beide Disziplinen häufig in einer Organisationseinheit gebündelt, weil sie auf dieselben Risikoanalysen und Prozesspriorisierungen zurückgreifen.

Bedeutung für den technischen Einkauf

Für Einkäufer hat DR eine doppelte Dimension: zum einen die Absicherung der eigenen

Einkaufssysteme und Beschaffungsprozesse, zum anderen die Notfallfähigkeit der Lieferanten. Fällt ein Zulieferer durch Brand, Ransomware oder Maschinenausfall aus, entsteht unmittelbar ein Lieferengpass mit möglichen Konventionalstrafen und Imagefolgen. DR-Anforderungen gehören daher zunehmend zur Lieferantenauswahl und -bewertung, etwa innerhalb eines Lieferantenratingmodells oder eines Preferred Supplier Program.

Methoden und Vorgehen im Disaster Recovery

Ein wirksames DR-Konzept folgt einem strukturierten Zyklus aus Risikoanalyse, Priorisierung, Maßnahmenplanung, Dokumentation und Test. Der Einkauf kann diesen Prozess aktiv mitgestalten, insbesondere bei Lieferantenabhängigkeiten und vertraglichen Absicherungen.

Business Impact Analysis und Priorisierung

Ausgangspunkt ist eine Business Impact Analysis (BIA): Sie identifiziert kritische Prozesse, Systemschnittstellen und Zulieferleistungen und bewertet die Folgen eines Ausfalls. Häufig kommt dabei eine ABC-Analyse zum Einsatz, um Prozesse und Lieferanten nach Kritikalität zu klassifizieren. Auf dieser Basis werden realistische Recovery-Ziele definiert, die anschließend die Grundlage für technische Maßnahmen und vertragliche Zusagen bilden.

RTO und RPO als Planungsgrößen

Die Recovery Time Objective (RTO) legt fest, innerhalb welcher Zeit ein System oder Prozess nach dem Ausfall wieder laufen muss. Die Recovery Point Objective (RPO) beschreibt, wie viele Daten höchstens verloren gehen dürfen, also den zulässigen zeitlichen Abstand zwischen letzter Sicherung und Ausfallzeitpunkt. Beide Werte bestimmen Aufwand und Kosten der DR-Maßnahmen erheblich: kurze RTO- und RPO-Werte erfordern typischerweise redundante Systeme, Spiegelrechenzentren oder Notfertigungen und treiben die Gesamtkostenrechnung einer Absicherungsstrategie nach oben.

Technische und organisatorische Maßnahmen

Zu den bewährten Maßnahmen gehören redundant ausgelegte Rechenzentren oder Cloud-Regionen, dokumentierte und getestete Backups, Notfall-Spielpläne mit klarer Rollenverteilung sowie Ersatzteillage für kritische Produktionsanlagen. Organisatorisch braucht es eine Notfallorganisation mit vertretenen Freigabegrenzen Einkauf und Entscheidungsrechten, damit auch dann handlungsfähig bleibt, wenn Führungskräfte nicht erreichbar sind.

Disaster Recovery in der Lieferkette

Die größte DR-Lücke entsteht in der Praxis oft nicht in der eigenen IT, sondern bei Zulieferern. Ein systematisches Lieferanten-DR-Management prüft und fordert die Notfallfähigkeit entlang der gesamten Supply Chain ein.

DR-Anforderungen in der Lieferantenauswahl

Bereits bei der Lieferantenaquise und im Angebotsprozess sollten DR-Fähigkeiten abgefragt werden: Ausfallkonzepte, doppelte Fertigungslinien, alternative Standorte, IT-Sicherheitsnachweise und Notfallkontakte. In Angebotswertungsstufen lässt sich die DR-Reife als eigenes Bewertungskriterium abbilden. Sofern das Beschaffungsvolumen eine Mehrfachstrategie erlaubt, unterstützt die Supply Base Optimization dabei, kritische Bauteile nicht von einem einzigen Anbieter abhängig zu machen.

Vertragliche Verankerung

DR-Zusagen entfalten nur Wirkung, wenn sie vertraglich greifbar sind. Ein Master Service Agreement (MSA) kann Pflichten zu Ausfallkonzepten, Meldeprozessen, Wiederanlaufzeiten und Testnachweisen festlegen. Ergänzend regeln Change-Order-Klauseln und ein klarer Abweichungsworkflow Menge, wie bei Störungen mit Mengen- oder Terminabweichungen umzugehen ist. Für den Extremfall sollte die Möglichkeit eines Transfer of Work zu einem Zweitlieferanten sowie eine Termination for Convenience geprüft und verhandelt werden; die rechtliche Wirksamkeit einzelner Klauseln ist stets im Einzelfall zu prüfen.

Störungsmanagement und Wiederanlauf

Tritt der Notfall ein, zählen definierte Eskalationswege, kurze Meldekette und ein dokumentiertes Verhandlungsprotokoll über Sofortmaßnahmen. Für produktionsnahe Störungen beim Lieferanten bewährt sich ein strukturiertes 8D-Containment, das Sofortmaßnahmen (Containment), Ursachenanalyse und Nachweise zur Wirksamkeit vorgibt. Parallel prüft der Einkauf Ausweichquellen, behält Luftfrachtkosten-Komponenten für Nottransporte im Blick und dokumentiert alles für spätere Anspruchsbeurteilung.

Wichtige KPIs für Disaster Recovery

Disaster Recovery lässt sich nur steuern, wenn Wiederherstellungsfähigkeit messbar gemacht wird. Die folgenden Kennzahlen haben sich in der Praxis als Kerngrößen etabliert und lassen sich auch auf Lieferantenbeziehungen übertragen.

Zeit- und Datenbezogene Kennzahlen

Neben RTO und RPO ist die tatsächliche Recovery Time bei Übungen die aussagekräftigste Kennzahl: Sie zeigt, ob geplante und realisierte Wiederanlaufzeiten auseinanderfallen. Die Testabdeckung gibt an, welcher Anteil kritischer Systeme und Prozesse durch geprüfte DR-Pläne abgesichert ist. Bei Lieferanten kann zusätzlich die Zeit bis zur Ausfallmeldung gemessen werden, da späte Meldungen Puffer für Ausweichbeschaffung verringern.

Erfolgs- und Kostenkennzahlen

Die Test-Erfolgsquote widerspiegelt, wie viele DR-Übungen die definierten Ziele erreichen. Ergänzend lassen sich Wiederanlaufkosten pro Störfall sowie die Verfügbarkeit kritischer Systeme über das Jahr erfassen. Im Einkauf lohnt zudem die Kopplung an die Lieferantenleistungsbewertung: Lieferanten, die DR-Anforderungen wiederholt nicht erfüllen, sollten im Rating sichtbar abgewertet werden. Alle Kennzahlen sollten aus einer etablierten Basis stammen und als Richtwerte, nicht als harte Branchenkonstanten interpretiert werden.

Risiken, Kontrollen und Compliance

DR-Projekte scheitern häufig nicht an der Technik, sondern an veralteten Plänen, unklaren Verantwortlichkeiten und ungetesteten Annahmen. Der Einkauf kann hier als Kontrollinstanz für Lieferanten-DR wirken.

Typische Risiken

Häufige Schwachpunkte sind: Pläne, die seit Jahren nicht getestet wurden; persönliche Abhängigkeiten von einzelnen Experten; fehlende Kenntnis über Unterauftragnehmer der Lieferanten; ungesicherte

Datenübernahmen bei Wechseln; und Ransomware-Szenarien, die auch Backups verschlüsseln. Weitere Risiken entstehen, wenn bei Notvergaben offenbarungs- oder dokumentationspflichtige Schritte übersprungen werden – hier helfen Match-&-Merge-Regeln, um Bestelldaten und Dokumentation konsistent zu halten.

Kontrollen und Audits

Lieferanten-DR lässt sich über Selbstauskünfte, Auditkriterien und Nachweispläne prüfen. Kritische Lieferanten aus der BIA sollten in regelmäßigen Abständen auditiert werden, wobei der Control-Plan-Ansatz aus der Qualitätssicherung sinngemäß nutzbar ist: definierte Prüfpunkte, dokumentierte Reaktionen, Verantwortlichkeiten. Ergebnisse fließen in die Lieferantenleistungsbewertung und in das Lieferantenratingmodell ein. Automatische Vertragsverlängerung ohne zwischenzeitliche DR-Prüfung sollte vermieden werden.

Compliance und Dokumentation

Je nach Branche und Rechtsrahmen bestehen Anforderungen an Ausfallsicherheit und Dokumentation, etwa aus Qualitätsmanagementnormen, Sicherheitsvorgaben oder Kundenanforderungen. Diese sollten mit der Rechts- und Compliance-Abteilung im Einzelfall geprüft werden. Generell gilt: Eine lückenlose, versionierte DR-Dokumentation ist sowohl bei Kundenaudits als auch bei Versicherungsfragen hilfreich.

Aktuelle Entwicklungen beim Disaster Recovery

Cyberbedrohungen, geopolitische Lieferkettenrisiken und regulatorische Anforderungen erhöhen den Stellenwert von DR in Industrie und Einkauf. Gleichzeitig verändern Cloud- und Automatisierungstechnologie die Umsetzungsformen.

Cyberisiken als DR-Treiber

Ransomware und supply-chain-übergreifende IT-Angriffe sind in den letzten Jahren zu einem der häufigsten DR-Auslöser geworden. Darum rücken IT-Sicherheitsnachweise und Cyber-Resilience der Zulieferer stärker in Lieferantenaudits. Konzepte wie unveränderbare (immutable) Backups und netzwerkgetrennte Sicherungskopien finden in der Praxis verbreitete Anwendung.

Resilienz statt reiner Kostenoptimierung

Viele Einkaufsorganisationen justieren ihre Strategien neu: statt maximaler Konsolidierung hin zu ausgewogener Resilienz mit Zweitquellen, regionalen Alternativen und Pufferbeständen bei A-Teilen. Risiko- und Gesamtkostenrechnung werden zusammengedacht – ein Notfallpuffer oder ein Zweitstandort wird als Prämie gegen Ausfallkosten bewertet, nicht nur als Mehrkosten. Dienste zur Content Enrichment von Artikelstammdaten helfen dabei, Alternative und Zweitquellen systematisch zu identifizieren.

Automatisierung und Cloud-basiertes DR

Cloud-Plattformen ermöglichen heute Disaster-Recovery-Szenarien, die früher mittelständischen Unternehmen verwehrt waren, etwa automatisierte Replikation und geographisch verteilte Systeme. Auch im Einkauf automatisieren digitale Werkzeuge die Ausfallfrüherkennung, etwa durch Lieferantenmonitoring und strukturierte Risiko-Scores. Wichtig bleibt: Technologie ersetzt nicht die Übung – Menschen, Entscheidungswege und vertragliche Absicherungen müssen den Notfall mittragen.

Typische Kennzahlen

RTO (Recovery Time Objective): prozessabhängig, oft Stunden bis Tage

Zeitziel für die Wiederanlaufzeit kritischer Systeme oder Lieferprozesse

RPO (Recovery Point Objective): typischerweise Minuten bis 24 Stunden

Maximal tolerierbarer Datenverlust; bestimmt Backup-Frequenz

Test-Erfolgsquote DR-Übungen: > 90 %

Anteil der Übungen, die definierte Ziele erreichen

Testabdeckung kritischer Prozesse: > 95 %

Anteil A-Kritikalität-Prozesse mit getestetem DR-Plan

Meldedauer Lieferantenausfall: < 24 Stunden

Zeit zwischen Störungseintritt und Meldung an den Einkauf

Praxisbeispiel

Ein mittelständischer Maschinenbauer bezog ein kritisches Gussbauteil von einem Alleinlieferanten. Nach einem Brand im Gießereibetrieb des Zulieferers stand die eigene Endmontage nach drei Wochen still, da es weder Zweitquelle noch vertraglich vereinbarte Ausfallkonzepte gab. Im Nachgang baute das Unternehmen ein Lieferanten-DR-Management auf:

- Business Impact Analysis über alle Bauteile mit ABC-Analyse zur Kritikalitätsklassifizierung
- Aufbau einer qualifizierten Zweitquelle und Verankerung von DR-Anforderungen im Master Service Agreement (MSA) inklusive definierten Wiederanlaufzeiten
- Jährliche DR-Selbstauskünfte und Audits bei A-Lieferanten mit Ergebnisfluß in die Lieferantenleistungsbewertung
- Verhandlung einer Transfer-of-Work-Option und dokumentierte Eskalationswege samt 8D-Containment für den Störfall

Fazit

Disaster Recovery ist im industriellen Einkauf weit mehr als eine IT-Aufgabe: Es sichert die Lieferfähigkeit und schützt vor Existenz gefährdenden Ausfällen bei kritischen Zulieferern. Entscheidend sind realistische RTO- und RPO-Ziele, eine saubere Priorisierung nach Kritikalität und vertraglich verankerte Pflichten. Unverprobte Pläne bieten in der Praxis keinen Schutz – regelmäßige Tests und Audits sind unverzichtbar. Einkäufer, die DR-Fähigkeit systematisch in Auswahl, Bewertung und Verträge integrieren, verwandeln Notfallvorsorge in einen echten Wettbewerbsvorteil.

Häufige Fragen

Was bedeutet Disaster Recovery einfach erklärt?

Disaster Recovery beschreibt alle Maßnahmen, um nach einem schweren Störfall wie Brand, Cyberangriff oder Maschinenausfall den Betrieb wiederherzustellen. Es ist Teil des Business Continuity Managements und konzentriert sich auf die Wiederanlaufphase. Zentrale Ziele sind definierte Wiederanlaufzeiten (RTO) und minimale Datenverluste (RPO).

Was ist der Unterschied zwischen Disaster Recovery und Business Continuity?

Business Continuity sorgt dafür, dass kritische Prozesse während einer Störung möglichst weiterlaufen

können. Disaster Recovery beginnt danach und stellt den ordnungsgemäßen Betrieb wieder her. Beide Disziplinen nutzen gemeinsame Risikoanalysen und werden in der Praxis oft gemeinsam organisiert.

Was sind RTO und RPO?

Die Recovery Time Objective (RTO) gibt an, innerhalb welcher Zeit ein System oder Prozess nach dem Ausfall wieder verfügbar sein muss. Die Recovery Point Objective (RPO) definiert, wie viele Daten höchstens verloren gehen dürfen. Beide Werte bestimmen Aufwand und Kosten der DR-Maßnahmen maßgeblich.

Wie prüft der Einkauf die Disaster-Recovery-Fähigkeit von Lieferanten?

Bewährt sind DR-Fragebögen und Selbstauskünfte bei der Lieferantenakquise, Auditkriterien für kritische Lieferanten und vertragliche Pflichten etwa im Master Service Agreement. Ergebnisse sollten in das Lieferantenrating einfließen. Zusätzlich helfen Mehrfachquellenstrategien und dokumentierte Notfallkontakte.

Wie oft sollte ein Disaster-Recovery-Plan getestet werden?

Üblich und vielfach empfohlen ist mindestens ein Test pro Jahr für kritische Systeme und Prozesse, bei hohen Anforderungen auch häufiger oder in Teilszenarien. Wichtig ist, Ergebnisse zu dokumentieren und den Plan danach anzupassen. Ungetestete Pläne bieten im Ernstfall häufig keinen funktionsfähigen Schutz.

Welche Kosten verursacht Disaster Recovery?

Die Kosten reichen von Redundanzen in IT und Fertigung über Backup-Infrastruktur bis zu Schulungen und Tests. In der Praxis werden typischerweise Gegenwerte zwischen wenigen Prozent und zweistelligen Prozentanteilen der betroffenen IT- oder Prozesskosten genannt, je nach Zielwerten. Eine Gesamtkostenrechnung sollte die Kosten gegen potenzielle Ausfallfolgekosten stellen.