

The background of the slide features a silhouette of a person in a suit walking away from the viewer on a path made of glowing light streaks. The path leads towards a bright, hazy horizon. The overall color palette is blue and white, with a large blue curved shape in the bottom right corner.

sonio.

Business Continuity ist kein IT-Projekt.

Es ist eine Überlebensstrategie

Business Continuity ist kein IT-Projekt.

Es ist eine Überlebensstrategie – und die meisten Unternehmen spielen sie auf gut Glück.

Naturkatastrophen, Cyberangriffe oder eine unglückliche Verkettung technischer Probleme können heute innert kürzester Zeit dazu führen, dass in einem Unternehmen nichts mehr geht. Das zeigt sich auch in der Schweiz ganz konkret: Beim Hochwasser im Wallis 2024 waren nach der Überflutung eines IT-Dienstleisters die Systeme von rund 30 Gemeinden beeinträchtigt. Und auch bei Ransomware-Angriffen kam es in den letzten Jahren wiederholt zu gravierenden Betriebsausfällen.

Die meisten Vorfälle gelangen nie an die Öffentlichkeit. Dem BACS wurden in den letzten Jahren jeweils über 100 Ransomware-Fälle gemeldet. Allerdings geht das Amt selbst davon aus, dass die tatsächliche Dunkelziffer deutlich höher liegt. Aus der Praxis lässt sich das nur bestätigen: Kaum ein Unternehmen hat heute noch keine Erfahrung mit einem erfolgreichen Phishing-Angriff, einem Malware-Vorfall oder einem grösseren Sicherheitsereignis gemacht.

ZUSAMMENFASSUNG

Cyberangriffe, Naturkatastrophen und technische Ausfälle können heute innert Stunden ein Unternehmen zum Stillstand bringen. Viele Organisationen glauben, mit einem Backup ausreichend vorbereitet zu sein. Die Realität sieht anders aus: Ein Backup allein ist kein Plan.

Dieses White Paper zeigt, warum Business Continuity ein ganzheitliches Thema ist, das weit über die reine Datensicherung hinausgeht. Das Zusammenspiel von Disaster Recovery, Cyber Resilience, klaren Notfallplänen und organisatorischer Verankerung ist entscheidend. Wir analysieren typische Schwachstellen aus der Praxis, zeigen auf, wo die grössten Lücken liegen, und erklären, mit welchem strukturierten Ansatz Unternehmen wirklich vorbereitet sind.

Sonio begleitet Unternehmen auf diesem Weg – als Architektur- und Umsetzungspartner für IT-Infrastruktur. Nicht als Produktlieferant, sondern als Partner, der weiss, wo angesetzt werden muss.

Und dennoch: Viele Unternehmen sind nicht vorbereitet. Wer eine Backup-Lösung betreibt, hält sich häufig für ausreichend geschützt. Diese Fehleinschätzung kann Sie teuer zu stehen kommen.

Das Missverständnis: Backup ist nicht Business Continuity

Im Gespräch mit IT-Verantwortlichen und Geschäftsleitungen begegnet uns immer wieder dieselbe Ausgangssituation: Die IT-Abteilung hat in Backup investiert, hat vielleicht sogar eine sogenannte DR-Site in einem anderen Rechenzentrum und trotzdem fehlen im Ernstfall entscheidende Voraussetzungen.

„Viele Unternehmen haben Daten gesichert, aber keinen Plan, wie sie den Betrieb wirklich wieder hochfahren.“

Warum? Weil diese DR-Sites vielfach eine von zwei Schwächen haben. Entweder werden sie laufend produktiv mitgenutzt und sind damit im Ernstfall ebenfalls betroffen. Oder sie sind zwar ein Backup-Standort, verfügen aber nicht über die nötigen Ressourcen – sprich Netzwerkkomponenten, Compute und Storage – für einen vollständigen Restore.

Aus der Praxis können wir bestätigen: Forensische Untersuchungen nach einem Cybervorfall blockieren Infrastrukturen oft mehrere Tage lang. In dieser Zeit ist selbst bei

vorhandenem Backup kein Restore möglich, weil die dafür benötigte Plattform schlicht nicht verfügbar ist. Das ist leider kein Einzelfall, sondern eher die Regel.

Drei strukturelle Problemfelder

Aus unserer Erfahrung und den geführten Gesprächen zeigen sich drei wiederkehrende Muster, egal ob wir mit einem KMU oder einem grossen Industrieunternehmen sprechen:

- **Fehlende Risikotransparenz:** Viele Unternehmen wissen nicht, was ein Ausfall wirklich kostet. Ohne diese Zahl ist jede Investitionsentscheidung im Bereich Business Continuity ein Blindflug.
- **Awareness-Lücke auf Managementebene:** Business Continuity gilt als IT-Thema. Dass es eine Führungsaufgabe ist, die vom Business definiert werden muss, ist in vielen Unternehmen noch nicht angekommen.
- **Technologie ohne Strategie:** Lösungen werden beschafft, ohne dass RTO (Recovery Time Objective) und RPO (Recovery Point Objective) mit dem Business abgestimmt sind. Die Infrastruktur existiert, aber sie passt nicht zu den tatsächlichen Anforderungen.

Die Realität hat sich verändert.

Ist Ihre Business Continuity darauf vorbereitet?

Business Continuity ist kein neues Thema. Allerdings haben sich die Rahmenbedingungen in den letzten Jahren fundamental verändert. Was früher als theoretisches Risiko galt, ist heute operative Realität.

Die Bedrohungslandschaft hat sich transformiert

Ransomware war noch vor wenigen Jahren eine Randerscheinung. Heute ist sie zur häufigsten Form eines ernsthaften IT-Ausfalls geworden. Angreifer sind professionell organisiert, ihr Wissen wird auf einschlägigen Plattformen gehandelt – und durch Künstliche Intelligenz lassen sich Angriffsmuster schneller als je zuvor entwickeln und optimieren. Wer heute noch denkt, «uns trifft das schon nicht», verschliesst seine Augen vor der Realität.

„ Die Frage ist längst nicht mehr, ob ein Unternehmen betroffen sein wird – sondern wann und wie gut es vorbereitet ist.

Gleichzeitig steigt die Komplexität der IT-Infrastrukturen. Hybride Umgebungen mit Cloud-Workloads, SaaS-Applikationen, On-Premises-Systemen und OT-Infrastrukturen schaffen neue Angriffsvektoren.

Eine Backup-Strategie, die für klassische On-Premises-Umgebungen konzipiert wurde, greift in dieser Welt schlicht nicht mehr.

Das ökonomische Gewicht von Ausfällen

Was kostet ein Ausfall wirklich? Diese Frage stellen sich zu wenige – und genau das ist das Problem. Aus realen Projekten kennen wir Zahlen, die das Bewusstsein schärfen: Ein produzierendes Unternehmen kann bei einem vollständigen IT-Ausfall täglich Schäden von 200'000 Franken und mehr erleiden, durch Produktionsstopp, Lieferunfähigkeit, Reputationsverlust und Vertragsstrafen. Wer diesen Wert kennt, relativiert die Kosten einer robusten BC-Strategie sofort.

RECHENBEISPIEL AUS DER PRAXIS

Ein Unternehmen mit 250 Mitarbeitenden, das bei einem IT-Ausfall täglich 200'000 CHF Schaden erleidet:

Eine Woche Ausfall: 1.4 Mio. CHF

Zwei Wochen: 2.8 Mio. CHF

Die Investition in eine vollständige BC-Lösung ist in der Regel ein Bruchteil davon.

Backup ist wichtig.

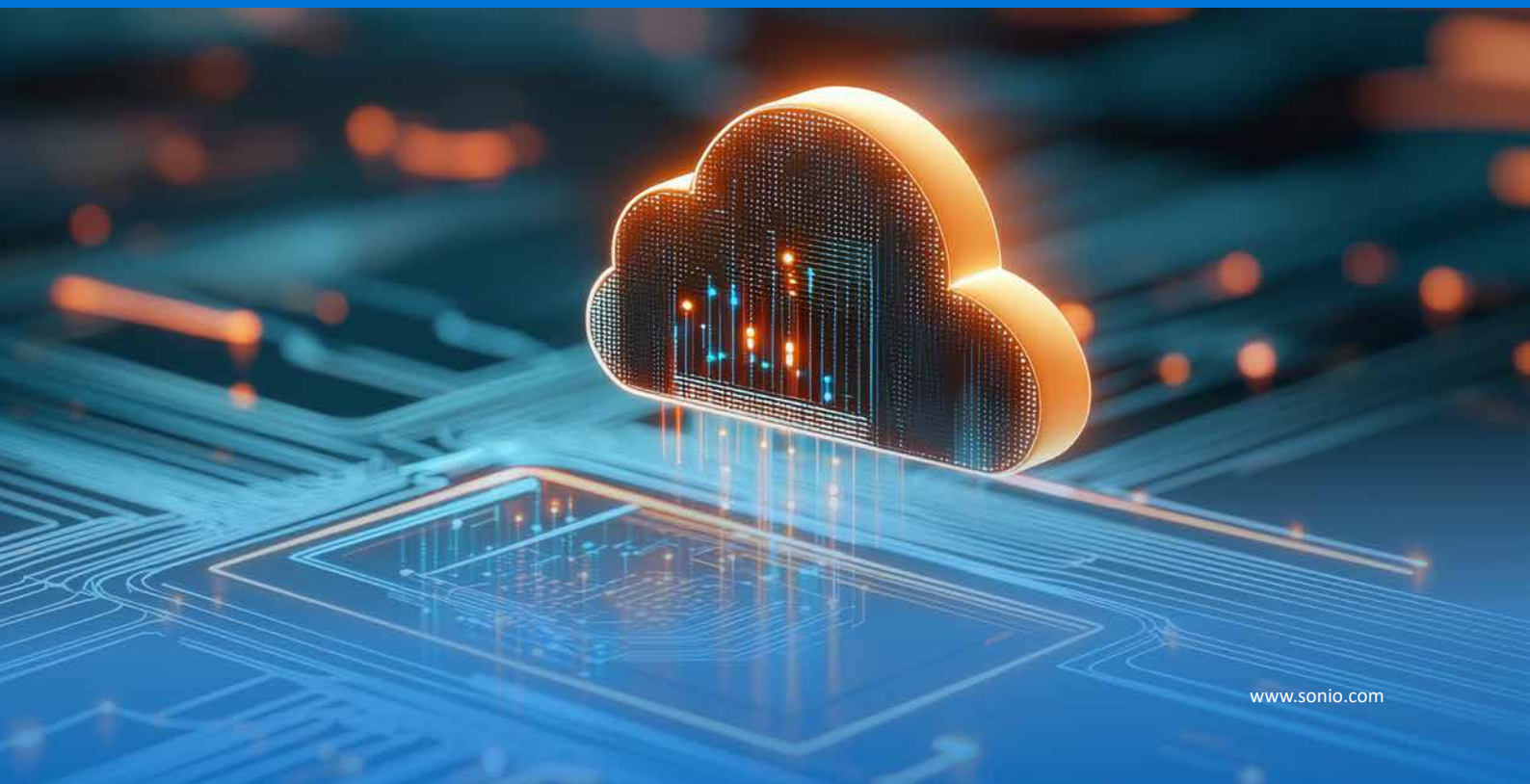
Das beste Backup bringt nichts, wenn der Betrieb trotzdem stillsteht.

Wenn wir mit Unternehmen über Business Continuity sprechen, ist eine Beobachtung fast universell: Die Diskussion beginnt mit Backup und endet dort auch häufig. Das ist verständlich, denn Backup ist das Sichtbarste und Greifbarste. Aber es ist halt eben nur ein Teil eines vielschichtigen Konzepts.

Business Continuity bedeutet: die Fähigkeit eines Unternehmens, nach einem unerwarteten und vor allem nicht gewünschten Ereignis – ob Cyberangriff,

physisches Disaster oder menschliches Versagen – den Betrieb so schnell wie möglich wieder aufzunehmen. Das erfordert definitiv mehr als Datenkopien. Es erfordert Strategie, Architektur, Organisation und regelmässiges Training.

” Backup schützt Daten.
Business Continuity schützt
das Unternehmen.



DIE VIER TRÜMPFE EINER ROBUSTEN BUSINESS-CONTINUITY-STRATEGIE

DAS ASS – Robustes Backup

Backup bildet das Fundament. Nicht nur Daten sichern, sondern widerstandsfähig gegen zwei Szenarien sein: erstens physischer Defekt oder Zerstörung von Hardware-Komponenten, zweitens Angriffe auf Daten durch Verschlüsselung, Kompromittierung oder Vernichtung. Das Ass ist wichtig. Aber es entscheidet die Partie nicht allein.

DAS NELL – Disaster Recovery

Disaster Recovery entscheidet über Geschwindigkeit. Die Fähigkeit, Services bei einem physischen Disaster zu überbrücken. Standortgetrennte Ressourcen für einen Failover, die nicht vom gleichen Ereignis betroffen sind – und die wirklich isoliert und nicht produktiv im Einsatz sind. Das Nell ist unscheinbar, aber spielentscheidend.

DER BUUR – Cyber Resilience

Cyber Resilience schützt das Backup selbst. Isolierte, saubere Umgebungen, getrennt vom Produktivbetrieb, die auch dann verfügbar sind, wenn die gesamte Produktionsinfrastruktur forensisch blockiert ist. Der Buur kontrolliert das Spiel und sorgt dafür, dass das Ass überhaupt spielbar bleibt.

DIE STÖCK – Notfallpläne

Detaillierte, unternehmensspezifische Pläne für Disaster- und Cybervorfälle. Keine eingekauften Schablonen, sondern Schritt-für-Schritt-Anleitungen, die im Zuge eines effektiven Restores erstellt und regelmässig getestet werden. Erst das Zusammenspiel aller vier Trümpfe schafft echte Business Continuity.



Die Jass-Analogie: Wer ein gutes Blatt hat, spielt nicht auf gut Glück

Das Kartenspiel Jass gehört zur Schweizer DNA, wie das Amen in die Kirche. Wer jassen kann, weiss: Zu einer guten Ausgangslage gehört ein guter Trumpf. Und ein guter Trumpf bedeutet vor allem, die höchsten Karten zu besitzen – Bauer («Buur»), 9 («Nell») und das Ass. Im Wunschtraum auch noch König mit Ober («Stöck»). Ein gutes Blatt hilft dabei, alle Stiche zu machen – einen sogenannten Match.

Und dieses Blatt muss bei jedem Unternehmen, egal welcher Grösse, aus denselben Stützpfeilern bestehen.

Beim Jassen können Sie einzelne Stiche machen. Doch die Partie gewinnt nur, wer ein gutes Blatt hat und es richtig spielt. Genauso ist es mit Business Continuity.

Wenn wir uns nun einen IT-Notfall vorstellen, dann verdunkelt sich der Raum, alles steht still, irgendwo dreht ein Monitoring-System am Rad und für einen Moment geht gar nichts mehr. In solchen Fällen müssen wir uns auf unsere Business-Continuity-Strategie verlassen können – auf unser gutes Blatt.

Struktur vor Software.

Technologie allein löst das Problem nicht.

Der häufigste Fehler bei der Einführung einer BC-Strategie ist, zu früh mit Technologie zu beginnen. Die Frage «Welches Backup-System kaufen wir?» kommt, bevor die Grundlagenfragen überhaupt beantwortet sind. Das führt dazu, dass Millionen für Lösungen ausgegeben werden, die an den tatsächlichen Anforderungen vorbeigehen.

Der richtige Ansatz beginnt beim Business – nicht bei der Infrastruktur.

Schritt 1: Business Impact verstehen

Bevor über Technologie gesprochen wird, müssen zuerst folgende Fragen beantwortet sein:

- Welche Systeme und Applikationen sind geschäftskritisch?
- Wie lange kann das Business ohne welches System auskommen?
- Was kostet ein Ausfall pro Stunde, pro Tag, pro Woche?
- Welche Abhängigkeiten bestehen zwischen Systemen und Prozessen?

Erst wenn diese Antworten vorliegen, lassen sich RTO (wie schnell müssen Systeme wieder laufen?) und RPO (wie alt dürfen die wiederhergestellten Daten sein?) definieren. Diese Werte sind die Grundlage für jede technische Entscheidung.

Schritt 2: Infrastruktur analysieren und Lücken identifizieren

Mit den definierten Anforderungen folgt eine ehrliche Bestandsaufnahme:

- Was ist heute vorhanden?
- Kann die bestehende Infrastruktur die definierten RTO und RPO erfüllen?
- Wo bestehen strukturelle Schwachstellen – bei Backup, DR oder Cyber Recovery?
- Sind SaaS-Daten, Cloud-Workloads und unstrukturierte Informationsbestände ebenfalls geschützt?
- Existieren unveränderbare (immutable) Backups und isolierte Recovery-Zonen?



Schritt 3: Architektur aufbauen mit den richtigen Prinzipien

Eine robuste Business-Continuity-Architektur im Infrastrukturbereich folgt klaren Grundsätzen:

PRINZIP	WAS ES BEDEUTET
3-2-1-1-0-Regel	3 Datenkopien (1 Original + 2 Backups), auf 2 verschiedenen Medien, 1 Kopie extern oder cloudbasiert, 1 Kopie offline und unveränderbar (Air Gap) – und 0 Fehler nach automatischen Wiederherstellungstests durch die Backup-Software.
Immutability	Backup-Daten müssen unveränderbar sein – kein Angreifer darf sie verschlüsseln oder löschen können.
Isolation	Recovery-Umgebungen müssen vollständig getrennt vom Produktivbetrieb sein.
Least Privilege	Minimale Zugriffsrechte für Backup-Administratoren und Recovery-Systeme.
Regelmässiges Testing	Restores müssen regelmässig durchgeführt und dokumentiert werden – nicht theoretisch, sondern in der Praxis.
Offline-Kopien	Mindestens eine Kopie muss vollständig vom Netz getrennt sein.

Schritt 4: Notfallpläne – die unterschätzte Arbeit

Notfallpläne werden häufig falsch angegangen. Eingekaufte Konzepte von der Stange sind im besten Fall eine Gedankenstütze. Selbst entwickelte Pläne bleiben oft unvollständig, weil sie von einem Idealzustand ausgehen, der in der Realität praktisch nie eintrifft.

„ Business Continuity beginnt nicht im Rechenzentrum, sondern im Business.

Wirklich belastbare Notfallpläne entstehen nur durch eines: den vollständigen, echten Durchlauf eines Restores oder Failovers – Schritt für Schritt, mit allen Stolpersteinen. Typische blinde Flecken, die erst im Ernstfall sichtbar werden:

- Wo liegen Zugangsdaten und Secrets – und sind diese im Ernstfall erreichbar?
- Sind Installationsdateien und Lizenzen offline verfügbar?
- In welcher Reihenfolge müssen Systeme neu aufgebaut werden?
- Wer ist im Ernstfall zuständig – und wer ist der Stellvertreter?
- Liegt der Notfallplan ausgedruckt vor – oder liegt er auf dem Server, der gerade nicht erreichbar ist?

Diese Fragen klingen banal. In der Praxis sind sie es, die den Unterschied zwischen einem schnellen Restore und einem wochenlangen Ausfall ausmachen.



Schritt 5: Awareness – der Faktor Mensch

Technologie schützt, aber der Mensch entscheidet.
Eine BC-Strategie, die nur in der IT-Abteilung verankert ist, ist keine nachhaltige Strategie. Folgendes zeigt sich in der Praxis immer wieder:

- **Awareness auf Führungsebene:** Wenn die Geschäftsleitung das Thema nicht als Priorität behandelt, wird kein Budget freigegeben – egal wie gut der IT-Verantwortliche argumentiert.
- **Mitarbeiterschulung:** Ransomware beginnt oft mit einem einzigen Klick. Jede Mitarbeiterin und jeder Mitarbeiter ist potenzielle Einfallstürze und gleichzeitig Schutzwall.
- **Regelmässige Übungen:** Nicht nur Backups, auch Notfallpläne müssen getestet werden. Wer seinen Disaster-Recovery-Plan noch nie in einer realen Umgebung durchgespielt hat, wird im Ernstfall scheitern.

Resilienz beginnt in der Infrastruktur.

Wo Sonio im Ernstfall den Unterschied macht.

Business Continuity ist ein breites Thema, welches von Facility Management über OT-Systeme bis hin zu Applikationen und Prozessen reicht. Sonio ist kein Generaldienstleister für alle Schichten, sondern

unser Fokus liegt klar im Bereich der IT-Infrastruktur. Hier können wir mit fundiertem Fachwissen und Erfahrung aus Dutzenden von Projekten einen echten Unterschied machen.

Was zur IT-Infrastruktur-Schicht gehört:

BEREICH	KONKRETE MASSNAHMEN & LÖSUNGEN
Backup & Datenschutz	Robuste Backup-Architekturen, BaaS (Backup as a Service), Immutable Storage, 3-2-1-1-0-Strategie.
Disaster Recovery	Standortgetrennte DR-Umgebungen, DRaaS (Disaster Recovery as a Service), Failover-Architekturen, RTO/RPO-Einhaltung.
Cyber Recovery	Isolierte Cyber Recovery Vaults, saubere Wiederherstellungsumgebungen, getrennt vom Produktivbetrieb.
Netzwerk & Redundanz	Redundante Netzwerkkomponenten, standortübergreifende Konnektivität, sichere Zugangskontrolle.
Cloud & Hybrid	Hybride Backup-Strategien, Cloud-integriertes DR, sichere Cloud-Workload-Sicherung.
Security-Integration	Minimale Zugriffsrechte, Verschlüsselung, Monitoring und Alerting im Backup-Bereich.
Notfallplanung	Praktische DR-Dokumentation, Restore-Tests, Recovery-Playbooks auf Infrastrukturebene.



Was wir nicht adressieren – und warum das Klarheit schafft

Sonio adressiert bewusst nicht die Applikationsschicht oder das vollständige Business Continuity Management auf Organisationsebene. Nicht weil diese Bereiche unwichtig sind – im Gegenteil. Aber Expertise bedeutet, zu wissen, wo man wirklich stark ist und wo ein anderer Partner mehr Wert schaffen kann.

„Eine robuste Infrastruktur ist dann gut, wenn sie auch unter Druck noch funktioniert.“

Dieses Fokusprinzip schützt unsere Kunden vor einer häufigen Falle: Lösungen zu kaufen, die technisch vorhanden sind, aber nicht zur tatsächlichen Anforderung passen. Wir vermitteln lieber an die richtigen Spezialisten, als eine Pseudolösung anzubieten.

Die Verbindung zu Data Management

Business Continuity im Infrastrukturbereich lässt sich nicht isoliert von der breiteren Datenstrategie betrachten. Wer seine Daten nicht kennt – welche

kritisch sind, wo sie liegen, wie sie abhängig sind – kann sie auch nicht schützen. Aus der Welt des modernen Data Managements sind dabei folgende Disziplinen besonders relevant:

- Data Security, Privacy, Protection and Resilience: Backup, Restore, Immutability, Disaster Recovery und Cyber Recovery als integrierter Teil einer kohärenten Datenschutzstrategie.
- Data Architecture: Wer weiss, wie Daten strukturiert und abhängig sind, kann Recovery-Pläne präziser gestalten.
- Governance & Compliance: Regulatorische Anforderungen wie Retentionspflichten und Datenschutzbestimmungen müssen in die Backup- und Archivierungsstrategie integriert sein.

Der Ernstfall kennt keine Theorie.

Wie unterschätzte Risiken Unternehmen plötzlich handlungsunfähig machen.

Theorie ist hilfreich. Aber die überzeugendsten Argumente für eine robuste Business-Continuity-Strategie kommen aus der Realität und Momenten, in denen man gedacht hat, man sei vorbereitet.

Wenn grüne Backup-Jobs in die Irre führen

Über sechs Monate wurde ein Unternehmen ausgespioniert, ohne dass es irgendjemand gemerkt hat. Die Angreifer hatten nur ein Ziel: sicherstellen, dass im entscheidenden Moment kein Entkommen möglich ist.

„ Die gefährlichsten Schwachstellen sind oft jene, die im Alltag unsichtbar bleiben.

In dieser Zeit haben sie die Treiber der Tape-Drives umgeschrieben. Das Ergebnis war perfide einfach: Die Laufwerke schrieben von da an nur noch Datenmüll auf die Bänder. Alle Backup-Jobs liefen weiterhin durch. Alles zeigte grün. Alles wirkte erfolgreich.

Als das Unternehmen schliesslich verschlüsselt wurde, wähnte es sich in Sicherheit. Die Tapes lagen

ausgelagert, sie waren nicht betroffen. So die Überzeugung. In dem Moment, als der Restore versucht wurde, zeigte sich die bittere Wahrheit: Die Backups bestanden aus reinem Datenmüll. Das Unternehmen hatte keine Wahl mehr und musste zahlen.

Was man aus diesem Fall mitnehmen muss: Ein grüner Backup-Job ist kein Beweis für ein funktionierendes Backup. Regelmässige, echte Restore-Tests – nicht nur automatische Prüfungen, sondern vollständige Wiederherstellungsübungen – sind keine



optionale Massnahme. Sie sind das Einzige, was im Ernstfall den Unterschied macht.

Der Cyberangriff während des DR-Projekts

Mitten in der Phase, in der die Risiken noch diskutiert werden, wird das Unternehmen tatsächlich gehackt. Plötzlich sind alle Rechenzentren nicht mehr erreichbar. Die forensische Aufarbeitung blockiert die Infrastruktur tagelang. Das Fazit der Beteiligten war ernüchternd: «Wir haben gewusst, dass es

„ Im Ernstfall zeigt sich nicht, wie modern eine Infrastruktur ist – sondern wie vorbereitet ein Unternehmen wirklich war.

passieren könnte – aber wir haben die Wahrscheinlichkeit zu tief eingeschätzt. Und dann war plötzlich unendlich viel Geld verfügbar.» Prävention wäre ein Bruchteil davon gewesen.

Millionen für die falsche Lösung

Ein grösseres Unternehmen führt eine Ausschreibung durch und entscheidet sich für eine aufwendige

Infrastrukturlösung mit eigener Secondary Site. Über fünf Jahre gebundene Kosten in Millionenhöhe.

Das Problem: Die Lösung wurde rein aus Infrastrukturperspektive gedacht. Das Business – die Applikationen, die eigentlichen Betriebsprozesse, die Datenflüsse – war nicht in die Entscheidung einbezogen. Im Ernstfall hätte die Infrastruktur zwar funktioniert, aber die darauf aufbauenden Systeme wären nicht wiederherstellbar gewesen. Millionen für eine Lösung, die an der tatsächlichen Anforderung vorbeizieht. Das ist das Ergebnis von Technologie ohne Strategie.



Von der Erkenntnis zur Umsetzung.

Wie Unternehmen Business Continuity Schritt für Schritt aufbauen.

Wie geht man konkret vor, wenn das Management erkannt hat: «Wir müssen dieses Thema ernstnehmen»? Aus unserer Erfahrung hat sich ein mehrstufiges Vorgehen bewährt, das sowohl Schnelligkeit als auch Nachhaltigkeit ermöglicht.

Das 5-Phasen-Modell für Business Continuity im Infrastrukturbereich:

PHASE 1 – SENSIBILISIERUNG

Was kostet uns ein Ausfall? Gemeinsame Erarbeitung eines Business-Impact-Verständnisses auf Management- und IT-Ebene. Konkretisierung von Risiken anhand realer Szenarien.

PHASE 2 – ANALYSE

Was haben wir heute? Inventarisierung aller kritischen Systeme und Daten, Erhebung bestehender Backup- und DR-Massnahmen, Bewertung gegen definierte RTO/RPO-Anforderungen.

PHASE 3 – DESIGN

Was brauchen wir? Architekturentwurf für eine robuste BC-Infrastruktur inklusive Backup, DR-Site, Cyber Recovery Vault und Notfallplanung. Abstimmung mit Business-Anforderungen.

PHASE 4 – UMSETZUNG

Schrittweiser Aufbau der Infrastruktur und der Notfallpläne – durch vollständige, echte Restore-Tests dokumentiert.

PHASE 5 – BETRIEB & KONTINUITÄT

Regelmässige Tests, Updates der Notfallpläne, Awareness-Schulungen, Monitoring und Reporting.

Der richtige Gesprächseinstieg

Ein Gespräch über Business Continuity sollte definitiv nicht mit einem Produktportfolio beginnen. Es sollte mit drei ehrlichen Fragen beginnen:

- Was kostet Sie ein Tag Ausfall Ihrer wichtigsten Systeme?
- Haben Sie das schon einmal wirklich durchgespielt – mit einem echten Restore?
- Wissen Ihre Mitarbeitenden, was sie im Ernstfall zu tun haben – und wer zuständig ist?

„ Resilienz ist kein Zustand, den man kauft – sondern eine Fähigkeit, die kontinuierlich aufgebaut wird.

Wer diese Fragen beantworten kann, ist vorbereitet.
Wer stockt, hat seinen Handlungsbedarf gefunden.



Partner für echte Resilienz.

Sonio begleitet Unternehmen mit Praxis und Verantwortung.

Sonio versteht sich nicht als Softwarelieferant. Wir sind ein Infrastruktur- und Architekturpartner mit tiefem Fachwissen in genau den Bereichen, die für eine funktionierende BC-Strategie auf der technischen Ebene entscheidend sind.

Was das konkret bedeutet

Wir helfen Unternehmen dabei:

- die Verbindung zwischen Business-Anforderungen und technischer Infrastruktur herzustellen – nicht als Berater auf der grünen Wiese, sondern als Praktiker mit Umsetzungserfahrung.
- eine Backup- und Recovery-Architektur aufzubauen, die wirklich funktioniert – inklusive Immutability, Isolation und regelmässiger Validierung.
- Cyber Recovery Vaults und isolierte Wiederherstellungsumgebungen zu konzipieren und zu betreiben.
- Notfallpläne zu erstellen, die auf echten Restore-Tests basieren und nicht auf theoretischen Annahmen.
- Cloud- und hybride Umgebungen in die BC-Strategie zu integrieren.

- Awareness auf der richtigen Ebene zu schaffen – gemeinsam mit IT-Verantwortlichen und Führungskräften.

„Technologie ist eine Karte. Strategie gewinnt das Spiel.“

Unser Verständnis von Partnerschaft

Im Jass reicht es nicht, gute Karten zu haben. Man muss sie lesen, einschätzen und im richtigen Moment spielen. Und vor allem: Jassen gewinnt man nicht alleine.

Genauso sehen wir unsere Rolle. Technologie ist eine Karte. Strategie gewinnt das Spiel. Wir verbinden führende Lösungen mit Architekturkompetenz, getesteten Szenarien, klarer Governance und operativer Verantwortung und wir betreiben alles in der Schweiz. Wer einen Partner am Tisch hat, der weiss, was auf dem Spiel steht, spielt anders.

Handeln, bevor der Ernstfall entscheidet.

Wer Resilienz als Führungsaufgabe versteht, bleibt auch dann handlungsfähig, wenn nichts mehr läuft.

Business Continuity ist kein Thema, das man «irgendwann» angehen kann. Es ist ein Thema, das man heute angehen muss, bevor der Ernstfall erzwingt, was man hätte steuern können.

Die gute Nachricht: Es ist keine Raketenwissenschaft. Es braucht keine unbeschränkten Mittel und keine monatelangen Projekte. Es braucht Klarheit

über die eigenen Anforderungen, über die bestehende Infrastruktur, über die kritischen Lücken. Und es braucht den Willen, konsequent zu handeln.

Wer diese Prinzipien in eine kohärente Strategie überführt, spielt im Ernstfall nicht auf gut Glück. Wer ein gutes Blatt hat, kann gelassen bleiben, selbst wenn der Raum sich verdunkelt und alles stillsteht.

Die zentralen Erkenntnisse aus diesem White Paper:

1. Backup ist der Anfang – nicht das Ende.

Wer glaubt, mit einer Backup-Lösung ausreichend vorbereitet zu sein, unterschätzt das Risiko fundamental.

2. Business Continuity ist eine Führungsaufgabe.

Wenn das Management das Thema nicht trägt, wird kein Budget freigegeben – egal wie gut die IT argumentiert.

3. RTO und RPO müssen mit dem Business definiert werden.

Nicht von der IT allein – sondern im Dialog mit den Verantwortlichen der Geschäftsprozesse.

4. Notfallpläne müssen getestet sein.

Ein grüner Backup-Job ist kein Beweis. Erst der echte Restore zeigt, wo die blinden Flecken liegen.

5. Awareness ist genauso wichtig wie Technologie.

Die beste Infrastruktur nützt nichts, wenn Mitarbeitende nicht wissen, was sie tun müssen – und wer zuständig ist.

6. Fokus schlägt Komplexität.

Sonio konzentriert sich auf das, was wir wirklich können: Infrastruktur-Resilienz auf höchstem Niveau.

Jetzt anfangen – nicht irgendwann.

Mit konkreten Sofortmassnahmen und einem klaren 90-Tage-Plan zur handlungsfähigen BC-Strategie.

Viele Unternehmen wissen nach der Lektüre dieses White Papers, dass sie handeln müssen. Allerdings scheitert der erste Schritt oft an der Frage: Wo fange ich eigentlich an?

Hier ist eine klare Antwort darauf.

Sofortmassnahmen – diese Woche

1. Kosten eines Ausfalls beziffern: Setzen Sie sich mit Ihrer Geschäftsleitung zusammen und berechnen Sie, was ein Tag Ausfall Ihrer wichtigsten Systeme konkret kostet. Wenn Sie diese Zahl nicht kennen, ist das Ihr erster Handlungsbedarf.

2. Backup-Status ehrlich prüfen: Wann wurde das letzte Mal ein vollständiger Restore durchgeführt – nicht nur ein automatischer Test, sondern eine echte Wiederherstellung? Wenn die Antwort «weiss ich nicht» oder «noch nie» lautet, wissen Sie, was zu tun ist.

3. Verantwortlichkeiten klären: Wer ist im Unternehmen verantwortlich für Business Continuity? Wer ist der Stellvertreter? Liegen diese Informationen offline und zugänglich vor?

Mittelfristig – in den nächsten 90 Tagen

1. Business Impact Analysis durchführen: Inventarisieren Sie alle kritischen Systeme mit ihren Abhängigkeiten und definieren Sie RTO und RPO gemeinsam mit dem Business.

2. Lückenanalyse: Vergleichen Sie Ihre bestehende Infrastruktur mit den definierten Anforderungen. Wo sind die grössten Lücken – bei Backup, Disaster Recovery oder Cyber Resilience?

3. Erstes Beratungsgespräch: Sprechen Sie mit einem Partner, der nicht nur Produkte verkauft, sondern die Situation analysiert und einen ehrlichen Bericht liefert.

Strategisch – Ihre BC-Roadmap

Business Continuity ist kein einmaliges Projekt. Es ist eine kontinuierliche Fähigkeit. Setzen Sie sich das Ziel, innerhalb von zwölf Monaten:

- eine vollständige Backup- und Recovery-Architektur nach 3-2-1-1-0 zu betreiben
- mindestens einen vollständigen DR-Test durchgeführt zu haben
- Notfallpläne zu besitzen, die auf echten Restore-Erfahrungen basieren
- und Awareness auf Management- und Mitarbeiterebene verankert zu haben

Das ist kein unerreichbares Ideal. Das ist erreichbar – mit dem richtigen Partner.

BEREIT FÜR DEN NÄCHSTEN SCHRITT?

Wir bieten ein kostenloses, unverbindliches Erstgespräch an.
Keinen Sales-Pitch, sondern eine strukturierte Analyse
Ihrer aktuellen Situation.

Was Sie nach dem Gespräch wissen:

- ✓ Wo Ihre grössten Lücken liegen
- ✓ Welche Massnahmen sofort Wirkung zeigen
- ✓ Was eine vollständige BC-Lösung für Ihr Unternehmen bedeutet

Vereinbaren Sie jetzt ein persönliches Beratungsgespräch:

www.sonio.com/business-continuity

Quellen: Dieses White Paper basiert auf folgenden Grundlagen: Internes Stakeholder-Gespräch: Sasa Gržinić, Lars Kündig, Markus Fischer, Mario Stich – April 2026. Blogartikel: Lars Kündig, «Business Continuity: Die richtigen Trümpfe für den IT-Notfall», April 2026, Sonio AG. White Paper: Ralph Budil, «Geschäftserfolg durch modernes Data Management mit SONIO», April 2026, Sonio AG. BACS (Bundesamt für Cybersicherheit), Jahresberichte Ransomware, Schweiz. Inside IT: «Hochwasser legte Server von 30 Gemeinden lahm», Juli 2024. DAMA DMBOK – Data Management Body of Knowledge. NIST Cybersecurity Framework 2.0; NIST AI Risk Management Framework. Gartner, aktuelle Analystensichten zu Data Protection und Resilience, 2025/2026. Sonio AG, Landing Page Business Continuity, www.sonio.com/business-continuity

sonio.



Kontaktieren
Sie uns für ein
unverbindliches
Gespräch:

info@sonio.com
www.sonio.com