
open-e
MEHR ALS NUR BACKUP:
WIE WIR DATEN ZUKUNFTIG SCHÜTZEN


Betriebliche Kontinuität
Elementare Sicherheit
Notfallwiederherstellung
Grundlegender Datensicherheit
Datenredundanz (RAID)
Hochverfügbarkeits-Cluster
Lokaler Datenschutz (On-Site)
Externer Datenschutz (Off-Site)
Maximale Datensicherheit

Datensicherheit verstehen – im Jahr 2025 und darüber hinaus

In unserer technologiegetriebenen Welt, in der digitale Lösungen jeden Aspekt unseres privaten und beruflichen Alltags durchdringen, sind zuverlässige Backups wichtiger denn je.

Der Begriff „Backup“ stammt vom englischen Verb to back up, was so viel bedeutet wie „unterstützen“ oder „absichern“ – und spiegelt damit seine Bedeutung in unserem Leben treffend wider. Ein Backup ist im Grunde eine Kopie wichtiger Daten, die erstellt wird, um wertvolle Informationen vor unvorhersehbaren Ereignissen zu schützen – etwa technischen Ausfällen, Naturkatastrophen oder anderen Bedrohungen.

Da wir in einer Welt leben, die von Daten geprägt ist, sind Backups längst zu einem unverzichtbaren Bestandteil für alle geworden, die digitale Informationen speichern. Das gilt insbesondere für Unternehmen – denn dort ist effektiver Datenschutz geschäftskritisch.

In diesem Dokument tauchen wir tiefer in die Welt der Datensicherung ein. Los geht's.

*“**In den letzten Jahren stand unsere Welt vor außergewöhnlichen Herausforderungen. Bei Open-E haben wir aus erster Hand erlebt, wie stark unsere Partner und Kunden davon betroffen waren**. Die Storage-Branche musste sich nicht nur auf die Folgen der Pandemie einstellen, sondern auch auf Hardwareengpässe, steigende Inflation, geopolitische Spannungen, Energiekrisen und wirtschaftliche Unsicherheiten. Diese Entwicklungen – fast wie die sprichwörtlichen apokalyptischen Reiter – machen eines deutlich: “**Verlässliche und robuste Backup-Lösungen sind heute wichtiger denn je.**”* **Kristof Franek, CEO von Open-E.**

Backup-Statistiken

- Im Durchschnitt versagen alle Bandlaufwerke irgendwann – das bedeutet, sie bieten keinen zuverlässigen Schutz bei Naturkatastrophen, Bränden oder Terroranschlägen, die das Büro und die gesamte Hardware zerstören. Unternehmer, die z. B. von Hurrikan Katrina betroffen waren, haben schmerzhaft gelernt, wie wichtig externe Sicherungskopien sind. (Quelle: VaultLogix)
- Innerhalb eines Jahres nach einem Datenverlust gehen **93 % der betroffenen Unternehmen**, bei denen die Ausfallzeit zehn Tage oder länger beträgt, in die Insolvenz – **50 % davon sofort**. (Quelle: National Archives & Records Administration, Washington D.C.)
- Alle fünf Jahre sind **20 % der kleinen und mittelständischen Unternehmen** voraussichtlich von einem schweren Vorfall betroffen, der zum Verlust geschäftskritischer Daten führt. (Quelle: Richmond House Group)
- Veraltete Software, Fehlkonfigurationen und mangelhafte Sicherheitsprotokolle ermöglichen es Cyberkriminellen, **93 % der Unternehmensnetzwerke** erfolgreich zu kompromittieren. In **50 % der Fälle** merken Unternehmen nicht einmal, dass sie angegriffen wurden. (Quellen: GartnerGroup & Keepnet)
- Die durchschnittliche Ausfallrate von Festplatten liegt **langfristig bei 100 %** – jede Festplatte hat eine begrenzte Lebensdauer und wird irgendwann ausfallen. (Quelle: VaultLogix)
- Nur **34 % der Unternehmen testen ihre Band-Backups** regelmäßig – und von diesen berichten **77 %** über Fehler bei solchen Tests. (Quelle: VaultLogix)
- Über **50 % der Unternehmen**, die von Datenverlust betroffen sind, müssen ihre Geschäftstätigkeit dauerhaft einstellen. (Quelle: VaultLogix)
- Mehr als **50 % aller kritischen Geschäftsdaten** werden auf Desktop-PCs und Laptops gespeichert, die nicht ausreichend geschützt sind. (Quelle: VaultLogix)
- Hauptursachen für Datenverluste:
  - **78%** Hardwarefehler oder Systemausfall
  - **11%** Menschliches Versagen
  - **7%** Softwarefehler oder Programmstörungen
  - **2%** Computerviren
  - **1%** Naturkatastrophen
  - **1%** Sonstiges

  (Quelle: VaultLogix)
- Rund **30 % der Unternehmen** haben **noch kein Notfallwiederherstellungsprogramm** etabliert. Zwei Drittel von ihnen schätzen ihre bestehenden Backup- und Recovery-Pläne als **anfällig für schwerwiegende Probleme** ein. (Quelle: VaultLogix)
- Die durchschnittlichen Kosten einer Datenschutzverletzung im Jahr 2024 lagen bei **4,88 Mio. US-Dollar.** (Quelle: IBM, Cost of a Data Breach Report)
- Der weltweite Schaden durch Cyberkriminalität wird bis 2025 voraussichtlich **10,5 Billionen US-Dollar** betragen – mit einer jährlichen Wachstumsrate von **15 %**. (Quelle: Secureframe)

Und jetzt?

Warum braucht Ihr Unternehmen ein Backup?

Haben Sie sich schon einmal gefragt, wie oft – und vor allem warum – Sie eigentlich ein Backup erstellen sollten?

Wenn nicht, stellen Sie sich diese eine Frage:
"*Wie viele meiner Arbeitsdaten kann mein Unternehmen sich leisten zu verlieren – und wie schnell brauchen wir sie zurück?*".

Die Antwort liegt auf der Hand.

Backup-Lösungen schützen Ihre Investition in Daten, indem sie mehrere Kopien anlegen. Wenn eine davon beschädigt wird, ist das kein Problem – **solange es ein Backup gibt.** Daten sind wertvoll – und die Wiederherstellung kostet Zeit, Geld und Aufwand. Backups helfen, die Folgen von Datenverlust zu vermeiden.

Folgen von Datenverlust

- **Finanzielle Verluste:** Verlorene Geschäftschancen, hohe Wiederherstellungskosten, mögliche Klagen von Kunden bei Datenverlust oder Datenlecks – sowie Gehaltskosten für Mitarbeitende, die ohne Zugriff auf ihre Daten nicht arbeiten können..
- **Reputationsschäden:** Der Verlust von Daten beeinträchtigt die Glaubwürdigkeit und das Vertrauen von Kunden, Partnern und anderen Stakeholdern – und kann negative öffentliche Aufmerksamkeit erzeugen.
- **Rechtliche und regulatorische Konsequenzen:** Verstöße gegen Datenschutzbestimmungen wie die DSGVO (EU) oder CCPA (USA) können zu hohen Geldstrafen und Klagen führen – etwa durch Personen oder Organisationen, deren sensible Daten verloren gingen oder offengelegt wurden.
- **Verlust von geistigem Eigentum:** Wertvolles Know-how, Geschäftsgeheimnisse oder proprietäre Informationen können unwiederbringlich verloren gehen..
- **Produktivitätseinbußen:** Mitarbeitende können ihre Aufgaben nicht mehr effizient erfüllen, wenn wichtige Informationen fehlen. Oft müssen Daten manuell rekonstruiert werden – das bindet Ressourcen..
- **Nichtverfügbarkeit wichtiger Informationen:** Wenn entscheidungsrelevante Daten fehlen, kann dies Prozesse verzögern, zu Fehlentscheidungen führen oder auf veraltete Informationen zurückgeworfen werden – was Qualität und Genauigkeit mindert.

Das Hauptziel von Backups besteht darin, durch Datensicherheit und Disaster Recovery die Geschäftskontinuität zu gewährleisten.

OPEN-E JOVIANDSS-BASIERTE DATENSPEICHERLÖSUNGEN MIT TOSHIBA-FESTPLATTEN

Die perfekte Lösung für Enterprise-Storage

Die Enterprise-Festplatten von Toshiba und Open-E JovianDSS bieten die ideale Lösung für Unternehmen, die zuverlässigen, leistungsstarken und kosteneffizienten Speicher mit hoher Kapazität benötigen. Mit bis zu **20 TB Kapazität**, einer jährlichen Arbeitslast von bis zu **550 TB** und einer **Ausfallrate von nur 0,35 %** bieten Toshiba-Festplatten eine **überragende Performance und Zuverlässigkeit**. Die Caching-Mechanismen von Open-E JovianDSS beschleunigen Lese- und Schreibvorgänge – gerade in Bezug auf die typischen Schwachstellen von HDDs – und ermöglichen so einen schnellen Zugriff auf große Datenmengen.

Vorteile:

- **Maximale Speicherkapazität zum niedrigsten Preis**
- **Lange Lebensdauer, niedrige Betriebskosten und hohe Nachhaltigkeit**
- **Open-E JovianDSS-Caching für beschleunigte Lese- und Schreibprozesse**
- **Ideal für die Speicherung großer Datenmengen**

Entdecken Sie die ideale Speicherlösung für Ihr Unternehmen – mit Datenspeicher-Appliances auf Basis von Open-E JovianDSS und Toshiba-HDDs.

open-e JovianDSS

TOSHIBA

LESEN SIE DIE BROSCHÜRE – JETZT!

Ebenen der Datensicherheit

Je nach geschäftlichen Anforderungen Ihres Unternehmens können Sie geeignete Maßnahmen zur **Business Continuity** und Ihrer Storage-Infrastruktur definieren. Dabei ist es entscheidend, die potenziellen Risiken zu verstehen und alle Details Ihrer Infrastruktur zu kennen, bevor Sie sich für bestimmte Speicherfunktionen entscheiden. Zuerst sollten Sie analysieren, **wie und warum Sie Daten speichern**. Notieren Sie dazu alle geschäftlichen Prozesse, die mit der Datenspeicherung in Ihrem Unternehmen zusammenhängen. Stellen Sie sich folgende Fragen:

- **Welche Daten sind geschäftskritisch und notwendig, damit Ihr Unternehmen arbeitsfähig bleibt?**
- **Welche Daten sind weniger wichtig, aber für den langfristigen Betrieb dennoch erforderlich?**
- **Welche Daten sind verzichtbar – können also gelöscht oder möglichst kostengünstig archiviert werden?**

Wenn Sie diese Fragen beantworten können, haben Sie bereits begonnen, Ihren Business-Continuity-Plan zu entwickeln. Glückwunsch!

Bevor Sie mit der Umsetzung beginnen, werfen wir einen Blick auf die konkreten Schutzfunktionen für Ihre Daten – und darauf, welches Sicherheitsniveau Sie mit Ihrer Infrastruktur erreichen können.

BRINGEN SIE IHRE SPEICHERLÖSUNG AUF DAS NÄCHSTE LEVEL

mit dem Open-E JovianDSS Setup!

Nutzen Sie die unbegrenzten Möglichkeiten bei der Umsetzung Ihrer Speicherlösung mit **Open-E JovianDSS** – einer auf **ZFS und Linux basierenden, hardwareunabhängigen Data Storage Software**, die sich für eine Vielzahl fortschrittlicher Einsatzszenarien eignet, darunter:

- **Business Continuity & Disaster Recovery**
- **Datenspeicherung**
- **Backups**

Weitere Informationen finden Sie auf unserer Website:
www.open-e.com/r/qvfn

Grundlegender Datenschutz

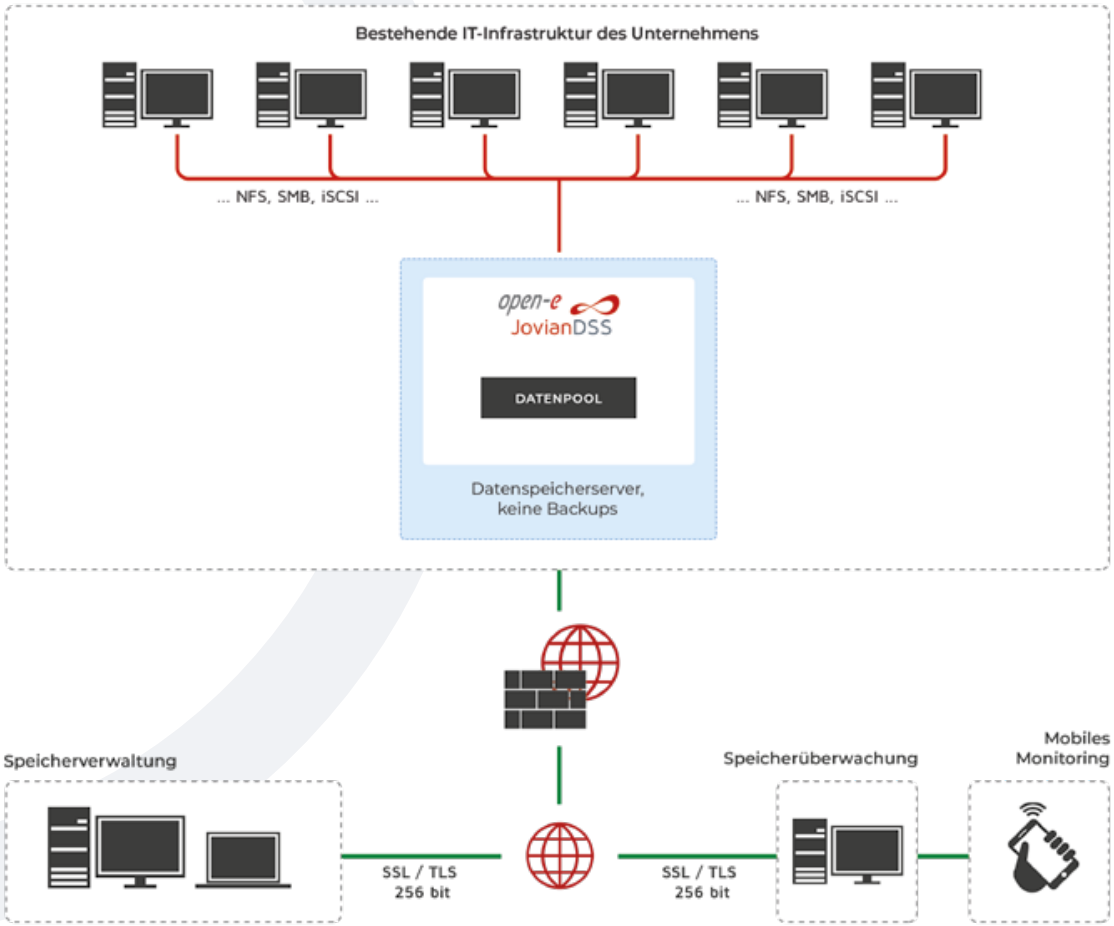
Die wichtigsten Aspekte, auf die Sie sich vorbereiten müssen, sind **stille Datenbeschädigung** (die bei jedem Speichermedium auftreten kann), das **Handeln gegen die Folgen von Virenangriffen** (z. B. Ransomware) und **menschliche Fehler und Handlungen**, die nach wie vor zu den Hauptursachen für die meisten Systemausfälle zählen. Ersteres kann durch eine **Selbstheilungsfunktion** vermieden werden, wie sie von einer ZFS-basierten Software wie Open-E JovianDSS bereitgestellt wird. **Snapshots** hingegen schützen Sie vor den Folgen von Virenangriffen sowie vor menschlichen Fehlern oder anderen Vorfällen, da sie es ermöglichen, den Zustand des Systems auf den Zeitpunkt vor dem Sicherheitsvorfall zurückzusetzen.

Unabhängig davon, wie relevant Ihre Daten sind, müssen Sie sie selbst auf der grundlegendsten Ebene absichern gegen:

- ✓ **stille Datenbeschädigung**
- ✓ **menschliche Fehler (eine der Hauptursachen für Datenverluste über Jahre hinweg), verursacht durch versehentliches Löschen oder absichtliches Handeln von Mitarbeitenden**
- ✓ **die Folgen von Ransomware-Angriffen**

Beides sind **grundlegende, in Open-E JovianDSS integrierte Funktionen**, die für Storage-Systeme mit niedriger Priorität ausreichend sein können. Sie funktionieren auch in sehr einfachen Storage-Setups wie etwa einem Single-Node-Server – es wird nichts weiter benötigt, was die Wartung günstig macht.

Allerdings gibt es auch einige **Nachteile**. Aus Sicht des Dateisystems sind Ihre Daten zwar geschützt. Der Schutz hängt jedoch vollständig von der verwendeten Hardware ab. Sobald diese ausfällt, sind Ihre Daten verloren. Es gibt kein Backup Ihrer Daten. Sie können das System nicht wiederherstellen. Seien Sie sich daher bewusst, dass ein Datenverlust irreversibel sein kann.



+ **Ermöglicht Wiederherstellung mit Snapshots (Zugriff auf zuvor gesicherte Daten)**
+ **Ermöglicht die Wahl der Snapshot-Häufigkeit**
+ **Selbstheilung (Self-Healing)**
+ **Schnelles Zurücksetzen per Snapshot**
+ **Geringe Kosten**
– **Kein Schutz vor Naturkatastrophen**
– **Kein Schutz bei Ausfall der lokalen Speichereinheit**
– **Kein RAID-Wiederherstellung möglich**
– **Verhindert keinen Systemausfall**

WARNUNG: Obwohl es sich um eine kosteneffiziente Lösung handelt, die Daten vor den häufigsten Bedrohungen wie menschlichem Versagen, Ransomware-Angriffen und stiller Datenbeschädigung schützt, stellt die verwendete Hardware einen Single Point of Failure dar – was direkt zu Datenverlust führen kann. **Dies ist kein echtes Backup und bietet keine Disaster-Recovery-Funktion.**

Datenschutz mit grundlegender Datenredundanz

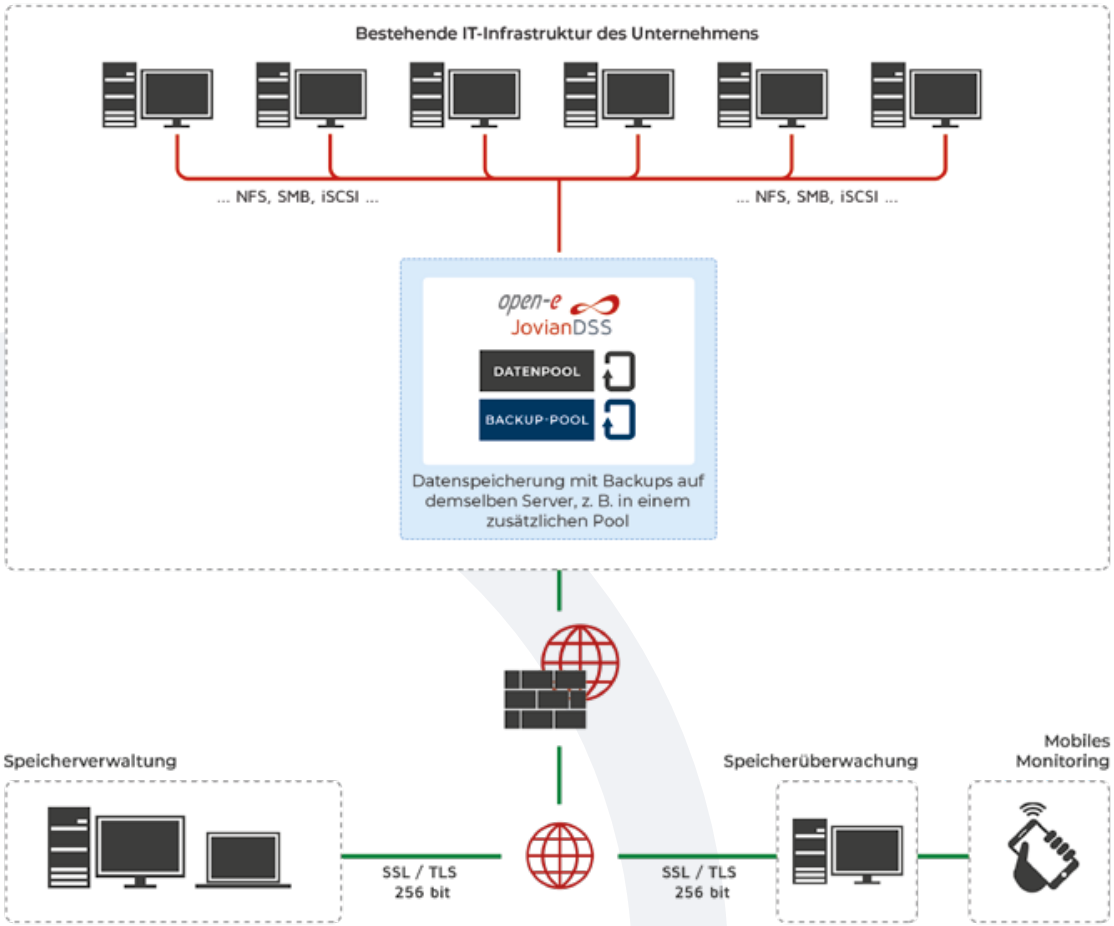
Wenn Sie ein **kleines Unternehmen** betreiben, das darauf **fokussiert ist, die Gesamtkosten der Dateninfrastruktur zu minimieren** und Ihre Transaktionssysteme nicht geschäftskritisch sind, **kann es ausreichen, ein Datenspeichersystem mit grundlegender Redundanz zu verwenden, um sich zu schützen gegen:**

✓ **Ausfälle von Festplatten**

Wie lässt sich das erreichen? Der elementare Datenschutz, bei dem der **Produktivserver mit einem Datenpool auf Basis eines gewählten RAID-Levels** betrieben wird, erscheint in diesem Fall ausreichend. Die Sicherung von Daten **gegen die Folgen eines Ransomware-Angriffs mit Snapshots, Selbstheilung, Schutz vor stiller Datenbeschädigung** funktioniert weiterhin – aber mit RAID erreichen Sie deutlich mehr. RAID schützt vor dem Ausfall einer oder mehrerer Festplatten – je nach Aufbau des Arrays.

Die Möglichkeit, Ihren Datenpool mit RAID aufzubauen, bietet Datenredundanz, sodass Sie im Falle eines Datenverlusts auf einem Laufwerk oder des kompletten Laufwerks immer auf die Paritätsdaten zurückgreifen können, um die Daten wiederherzustellen.

Die Verwendung eines höheren RAID-Levels (z. B.RAID 6) schützt Sie vor dem Verlust mehrerer Festplatten im Pool. Es liegt an Ihnen zu entscheiden, wie wichtig diese Daten sind und wie viel Sie bereit sind, in zusätzliche Laufwerke zu investieren. Sobald das entschieden ist, können Sie die entsprechende RAID-Konfiguration wählen.



+ **schützt mit Snapshots (Zugriff auf zuvor gesicherte Daten)**
+ **ermöglicht die Wahl der Snapshot-Frequenz**
+ **selbstheilend**
+ **Schutz bei Festplattenausfall (RAID)**
+ **RAID-Wiederherstellung**
+ **schnelles Zurücksetzen per Snapshot**
+ **geringe Kosten**
– **kein Schutz vor Naturkatastrophen**
– **kein Schutz bei Ausfall der lokalen Speichereinheit (inkl. Backup-Pool)**
– **verhindert keine Ausfallzeiten**

WARNUNG: Beachten Sie, dass es keinen Schutz gegen Systemausfall oder Standortprobleme gibt (z. B. Stromausfälle, Katastrophen sowie menschliches Versagen oder Fehler, die das gesamte Festplatten-Array betreffen). Wenn Sie Ihr Array verlieren, verlieren Sie auch Ihre Daten und die Möglichkeit, sie wiederherzustellen. Dieses Sicherheitsniveau ist für die meisten realen Geschäftsanwendungen nicht ausreichend. **Dies ist kein echtes Backup, und es wird keine Disaster-Recovery-Funktion bereitgestellt.**

High Availability Cluster

Was ist, wenn Ihr Geschäftsprozess zusätzlich Schutz vor dem Ausfall von mehr Festplatten erfordert, als Ihr RAID-Level unterstützt?
Wenn etwas mit Ihrem Server passiert, der nur aus einem Knoten besteht, verlieren Sie alle dort gespeicherten Daten. Es gibt jedoch eine höhere Sicherheitsstufe – nämlich einen **High Availability Cluster**, der Sie schützt vor:

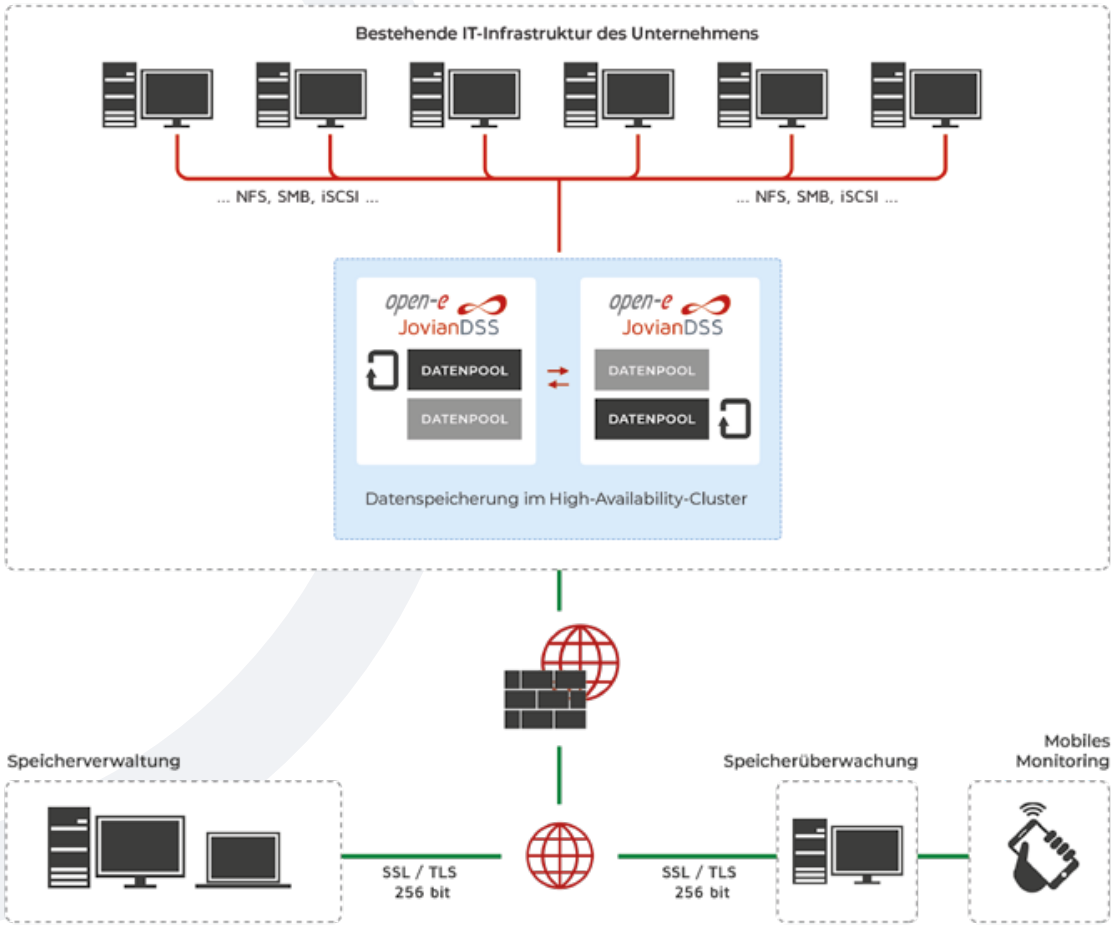
✓ **RAID-Ausfall (am Produktivknoten)**

Ein solcher Cluster besteht aus **zwei Knoten**, die **lokal oder remote verbunden** sind, und verwendet eine Architektur mit gemeinsam genutztem oder getrenntem Speicher. **Einzelhandel, Gastgewerbe** oder allgemein **kleine und mittelständische Unternehmen**, die diese Lösung in ihrer Sicherheitsinfrastruktur einsetzen, stellen so ihre **Business Continuity** sicher – durch unterbrechungsfreien Datenzugriff selbst bei Hardwareausfällen und durch optimale Nutzung von Hardware- und Netzwerkressourcen.

Beachten Sie, dass **dies kein echtes Backup ist**, da Sie Ihre Daten nicht an einem anderen Ort aufbewahren. **Ein Verlust des Clusters führt zu einem unwiederbringlichen Datenverlust**. Die Hardware ist zudem **anfällig für Katastrophen oder vorsätzliche schädliche Handlungen** (z. B. Diebstahl), die den gesamten Cluster außer Betrieb setzen können – insbesondere wenn dieser sich am Unternehmensstandort befindet.

Es gibt jedoch eine **Lösung von Open-E JovianDSS**, die dies umgeht: ein „**Non-Shared Storage Stretched Cluster**".

Dabei wird der zweite Knoten **an einem anderen** Ort installiert – mit einer maximalen Entfernung von **80 km** (bei Glasfaser-Punkt-zu-Punkt-Verbindung), um die Daten zwischen den Knoten zu spiegeln. Tatsächlich kann die Entfernung noch größer sein, wenn ein zusätzlicher Switch verwendet wird und die Netzwerklatenz unter 5 ms bleibt. Da sich der zweite Knoten **an einem anderen Standort befindet, müssen Sie sich auch im Brand- oder Katastrophenfall keine Sorgen um die Datenverfügbarkeit machen.**



+ **schützt mit Snapshots (Zugriff auf zuvor gesicherte Daten)**
+ **ermöglicht die Wahl der Snapshot-Frequenz**
+ **selbstheilend**
+ **Schutz bei Festplattenausfall (RAID)**
+ **RAID-Wiederherstellung**
+ **schnelles Zurücksetzen per Snapshot**
+ **automatisches Umschalten bei Systemausfall (Failover)**
+ **kann Ausfallzeiten verhindern**
− **kein Schutz vor Naturkatastrophen**
− **kein Schutz bei Ausfall der lokalen Speichereinheit**

WARNUNG: Wenn Sie diese Lösung für Ihre Datensicherheit einsetzen, können die Funktionen des Produktivservers durch den zweiten Knoten übernommen werden, während der erste wiederhergestellt wird. Das ist möglich, weil synchrone Kopien der Daten auf beiden Knoten vorhanden sind - daher der höhere Schutzgrad. Es ist der erste Schritt hin zu maximaler Datensicherheit. Allerdings muss diese Lösung **mit einem On- oder Off-Site-Datenschutz** kombiniert werden, um Ihre Infrastruktur mit einem **echten Backup** abzusichern. **Denken Sie daran: Auch wenn ein Non-Shared Storage Stretched Cluster verwendet wird – es handelt sich immer noch nicht um ein echtes Backup.**
Disaster Recovery ist ebenfalls nicht enthalten – aber keine Sorge, genau dazu kommen wir gleich.

Business Continuity vs. Disaster Recovery

Im vorherigen Abschnitt lag der Fokus auf den **Business-Continuity-Maßnahmen** für Ihre Speicherinfrastruktur – also auf den Risiken, die Sie berücksichtigen sollten, und den Schutzfunktionen, die bei der Wahl Ihres Speicherkonzepts eine Rolle spielen. Aber selbst die besten Sicherheitsmaßnahmen können nicht zu 100 % garantieren, dass kein **Desaster oder unvorhergesehenes Ereignis** eintritt.

Das kann dazu führen, dass eine Situation entsteht, in der **Disaster Recovery** notwendig wird, um den Geschäftsbetrieb so schnell wie möglich wiederherzustellen. Wie stellen Sie also sicher, dass Sie auf den Ernstfall vorbereitet sind? Schauen wir uns das nun genauer an.

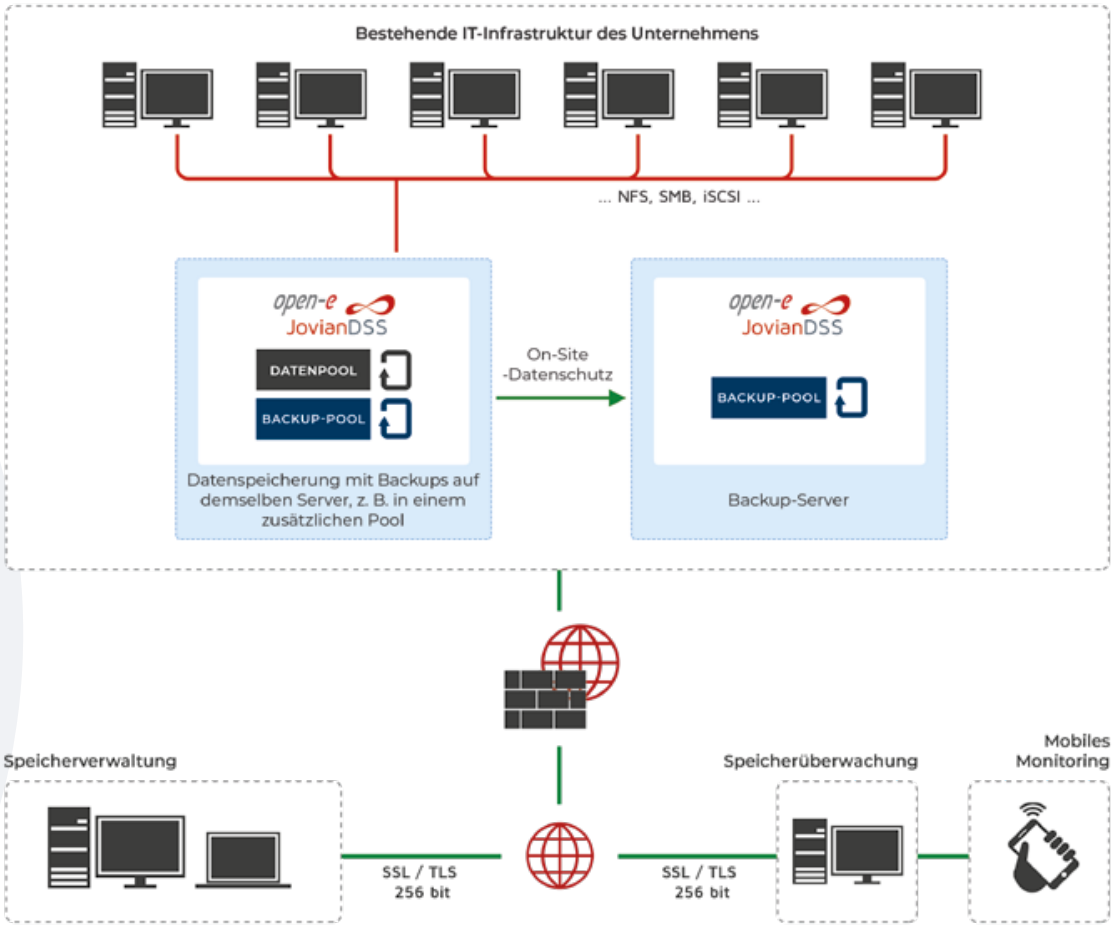
On-site Data Protection mit einem Backup Pool

Sie fragen sich vielleicht, wie Sie Ihr Unternehmen vor den Folgen eines Ausfalls des High-Availability-Clusters schützen können. Das kann z. B. durch Hardwareprobleme oder unbeabsichtigte menschliche Fehler passieren, die zu einem Totalausfall führen. Fällt die gesamte Einheit aus, können Geschäftsprozesse nicht mehr ausgeführt oder verwaltet werden. Die eindeutige Antwort darauf lautet: **On-Site Data Protection**, die Sie schützt vor:

✓ **Cluster-Ausfall**

On-site-Protection ermöglicht es, Backups an Ihrem Standort auf einem zusätzlichen lokalen System auf Basis von Open-E JovianDSS zu speichern. Somit sichern Sie die Datenspeicherung auf dem produktiven HA-Cluster mit einem Backup auf einem zweiten lokalen Server ab.

Wer profitiert davon? Gesundheitseinrichtungen, um Patientendaten zu schützen, **Finanzdienstleister**, um Kundendaten zu schützen, **Behörden**, um sensible Informationen zu sichern und regulatorischen Vorgaben zu entsprechen, sowie **Industrie und Logistik**, um Betriebs- und Kundendaten zu schützen. Außerdem erfüllen alle genannten Bereiche mit dieser Lösung die gesetzlichen Anforderungen.



+ schützt mit Snapshots (Zugriff auf zuvor gespeicherte Daten)
+ ermöglicht die Wahl der Snapshot-Frequenz
+ selbstheilend
+ Schutz bei Festplattenausfall (RAID)
+ RAID-Wiederherstellung
+ schnelles Zurücksetzen
+ automatisches Umschalten bei Systemausfall
− kein Schutz vor Naturkatastrophen
− kein Schutz bei Ausfall der lokalen Speichereinheit
− verhindert keine Ausfallzeiten

WARNUNG: Durch einen zweiten Server am Standort ist die Wiederherstellung von Daten in der Regel einfacher und schneller als bei einem Off-Site-Backup, wenn der Hauptserver ausfällt. Daher eignet sich diese Lösung ideal für Hot-Data-Backups, die aus der Sicherungskopie wiederhergestellt werden können. Beachten Sie, dass **kein Schutz vor Naturkatastrophen, Ausfall der lokalen Speichergeräte oder Downtime** besteht. **Es handelt sich nur um ein lokales Backup – aber Disaster Recovery im Falle eines Cluster-Ausfalls ist enthalten.**

Off-Site-Datenschutz

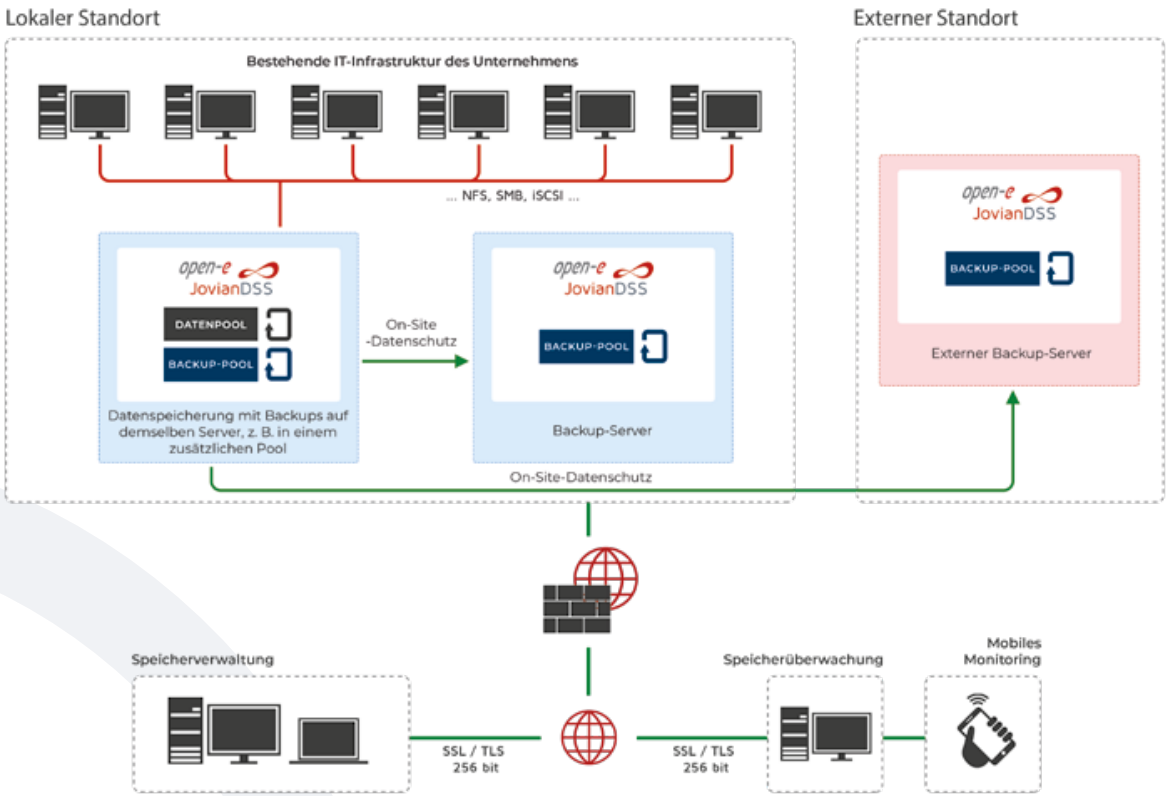
Wie wir alle wissen, steht im Hintergrund jeder geschäftlichen Tätigkeit ein ewiger Konflikt – **Mensch gegen Natur**. In extremen Fällen verlieren wir – und mit uns unsere Unternehmen. **Überschwemmung, Feuer, Erdbeben usw.** – egal, wie wichtig unsere Daten sind, wenn so etwas passiert, **kann zum vollständigen Bankrott führen**, weil die gesamte Hardware und alles, was darauf gespeichert ist, verloren geht. Gibt es etwas Schlimmeres? Wir bezweifeln es. Besonders dann, wenn Ihr Unternehmen auf Archivierung und langfristige Datensicherung angewiesen ist. Wenn genau das Ihre Sorge ist, dann ist **Off-Site Data Protection** die Lösung – sie bietet:

- ✓ **Schutz vor Naturkatastrophen**
- ✓ **Hervorragende Archivierungsmöglichkeiten mit langfristigen Backups**

Neben allen zuvor genannten Funktionen wie Snapshots, RAIDs, Hochverfügbarkeit und lokalen Backup-Servern verwenden sie **einen zusätzlichen externen Server,** mit dem Sie von allen Vorteilen externer Datensicherung profitieren. Dazu gehören: **Schutz vor Naturkatastrophen sowie vorsätzlichen oder böswilligen menschlichen Handlungen** (z. B. Diebstahl), die sowohl das Produktionssystem als auch den lokalen Backup-Server zerstören oder beschädigen können.

Es ist eine ausgezeichnete Lösung für **große Unternehmen, die kritische Anwendungen und Kerndaten verarbeiten**. Sie findet breite Anwendung in **Verteidigung und nationaler Sicherheit**, in Abteilungen mit streng vertraulichen Informationen. Auch Unternehmen aus den Bereichen **Technologie, Software, Energie und Versorgungswirtschaft** können sich darauf verlassen.

Es gibt jedoch auch Nachteile. **Sie verhindert Ausfallzeiten nicht vollständig**, sodass die Business Continuity davon abhängt, wie schnell vollständig wiederhergestellt werden kann und wie hoch die Übertragungsleistung ist. Je nach Datenmenge und Management kann die Wiederherstellung viel Zeit in Anspruch nehmen – und **die Kosten sind in einem solchen Fall deutlich höher**, da eine separate Backup-Einheit erforderlich ist.



+ schützt mit Snapshots (Zugriff auf zuvor gespeicherte Daten)
+ ermöglicht die Wahl der Snapshot-Frequenz
+ selbstheilend
+ Schutz bei Festplattenausfall (RAID)
+ RAID-Wiederherstellung
+ schnelles Zurücksetzen
+ automatisches Umschalten bei Systemausfall
+ schützt vor Naturkatastrophen
+ schützt bei Ausfall der lokalen Speichereinheit durch Backup-Server
+ ermöglicht den Einsatz des Backup-Servers als Produktivsystem
+ keine Notwendigkeit für Backup-Systeme von Drittanbietern
− verhindert keine Ausfallzeiten
− hohe Kosten
− lange Wiederherstellungszeit (bei Ausfall anderer Sicherheitsmechanismen)

WARNUNG: Off-Site-Datenschutz ermöglicht es, alle Ihre Daten auf einem entfernten Server an einem anderen Standort zu sichern. Gehen die Daten des Produktionsservers verloren, können sie vom externen Backup-System wiederhergestellt werden. Dies kann – je nach Anzahl und Größe der Dateien – etwas Zeit in Anspruch nehmen. Unternehmen, die Archive verwalten oder langfristige Backups nutzen, bei denen kein sofortiger Zugriff nötig ist, können besonders vom Einsatz eines externen Backup-Servers profitieren – mit anschließender Wiederherstellung oder Rückübertragung der Daten an den Hauptstandort. **Dies ist ein echtes Backup – und Disaster Recovery ist inbegriffen.**

Maximale Datensicherheit

Wenn Ihr oberstes Ziel darin besteht, das **höchstmögliche Sicherheitsniveau für Ihre Daten** zu gewährleisten und Geld dabei keine Rolle spielt – Ausfallzeiten aber schon –, dann können Sie mit Open-E JovianDSS die Datensicherheit maximieren. Dies gelingt, indem Sie alle zuvor genannten Methoden kombinieren und gemeinsam einsetzen. **Die Kombination aus On- und Off-Site-Backup mit einem zusätzlichen High-Availability-Cluster** ermöglicht **volle Business Continuity ohne Ausfallzeiten.**

Die Kosten mögen auf den ersten Blick als Nachteil erscheinen, doch vergleichen Sie diese mit den potenziellen Kosten eines Datenverlusts – niemand kann es sich leisten, Daten zu verlieren. Außerdem ist es nicht erforderlich, auf besonders teure Hardware zu setzen – die **zusätzlichen Komponenten reichen aus**, um Ihre Daten effektiv zu schützen. Diese Lösung ist vor allem in **Software-, Technologie- und Finanzbranchen** verbreitet, ebenso wie in **Behörden der nationalen Sicherheit**. Wenn man sich für diese Variante entscheidet, bedeutet das in der Regel, dass **keine Downtime erlaubt ist**, was **vollständige Business Continuity** zur Pflicht macht. Außerdem eignet sich die Lösung für große Mengen an **sensiblen, geschützten und geschäftskritischen Informationen**. Allerdings kann die **Wiederherstellungszeit bei Rücksicherung von einem entfernten Standort länger sein**, wenn alle anderen Schutzmechanismen ausfallen.

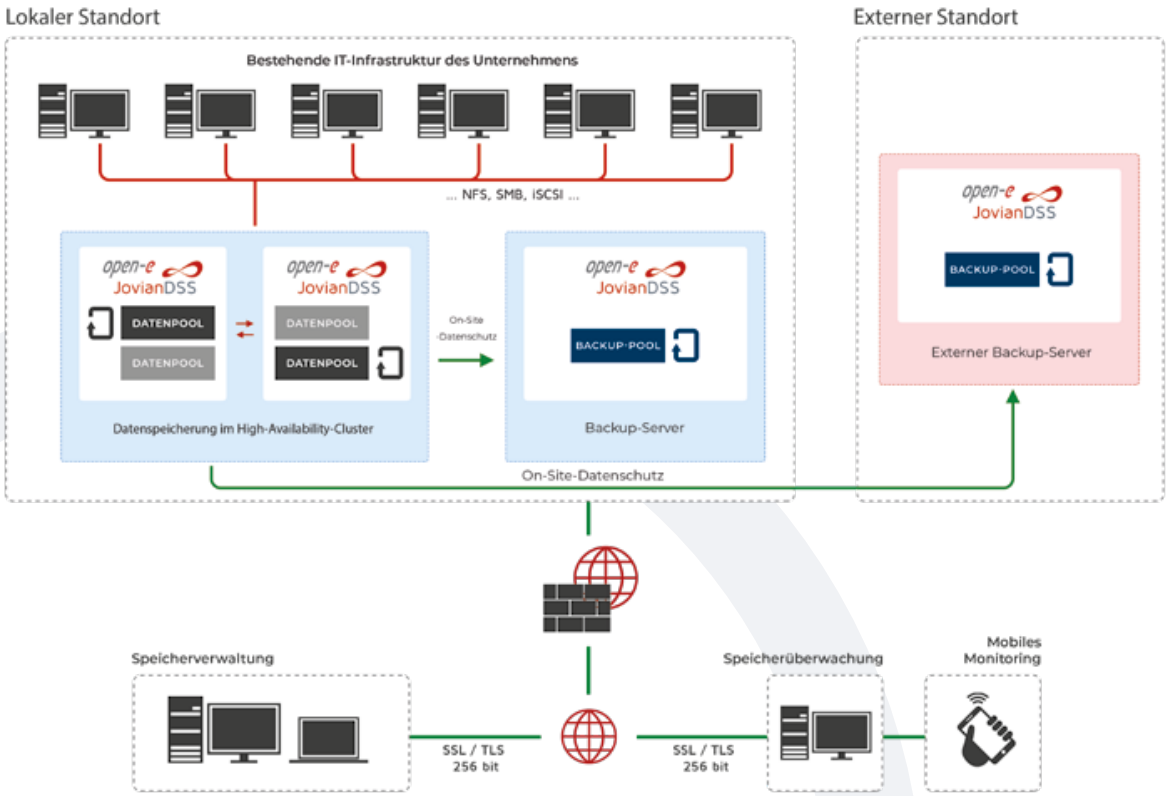
High Availability

+

On- & Off-Site Data Protection

=

Maximaler Datenschutz



+ **schützt mit Snapshots (Zugriff auf zuvor gespeicherte Daten)**
+ **ermöglicht die Wahl der Snapshot-Frequenz**
+ **selbstheilend**
+ **Schutz bei Festplattenausfall (RAID)**
+ **RAID-Wiederherstellung**
+ **schnelles Zurücksetzen**
+ **automatisches Umschalten bei Systemausfall**
+ **Schutz vor Naturkatastrophen**
+ **Schutz bei Ausfall der lokalen Speichereinheit (Backup-Pool) durch Backup-Server**
+ **ermöglicht die Nutzung des Backup-Servers als Produktivsystem**
+ **keine Ausfallzeiten während der Wiederherstellung**
+ **vollständige Disaster Recovery (HA)**
− **hohe Kosten**
− **lange Wiederherstellungszeit (bei Versagen der übrigen Schutzmechanismen)**

WARNUNG: Dieses Modell deckt alle potenziellen Szenarien ab, die sich negativ auf Ihre Geschäftsprozesse auswirken könnten. Archive und langfristige Speicherungen sind sicher, wenn sie auf dem **Remote-Backup** abgelegt werden. Der **On-Site-Backup-Server** enthält die Daten, die im Ernstfall sofort wiederhergestellt werden müssen. **RAIDs und Snapshots** sorgen für Parität und Selbstheilung.
All das kann über **Open-E JovianDSS** verwaltet werden und bietet schnellen, effizienten Zugriff. **Es handelt sich um ein echtes Backup – Disaster Recovery ist enthalten.**

Entdecken Sie die neuesten Broschüren von Open-E

Ein großer Schritt für Ihre Datenspeicherung – und ein noch größerer für Ihr Budget!

ZEIT IST GELD – UND DATEN SIND ES AUCH: Business Continuity & Disaster Recovery

Wie bereits festgestellt, sollte sich Ihre Datensicherheitsstrategie darauf konzentrieren, die Kontinuität Ihres Geschäftsbetriebs sicherzustellen – und im Fall eines unvorhergesehenen Ereignisses die Wiederherstellung nach einem Desaster. Warum?

Damit das Geschäft so schnell wie möglich wieder in Gang kommt. Werfen wir noch einmal einen Blick auf die drei entscheidenden Fragen, um herauszufinden, welchen Weg der Datensicherung Sie wählen sollten:

- **Welche Daten sind geschäftskritisch und halten Ihr Unternehmen am Laufen?**
- **Welche Daten sind weniger wichtig, aber dennoch notwendig für den langfristigen Betrieb?**
- **Welche Daten sind entbehrlich – also solche, die Sie löschen oder möglichst kostengünstig speichern können?**

Wenn Sie diese Fragen ehrlich beantwortet und bereits die passende Methode für die Sicherheit Ihres Unternehmens gewählt haben, haben wir nun noch ein paar Tipps für Sie: Es ist sinnvoll, den Betrieb **mit möglichst wenigen Unterbrechungen fortzusetzen** und **die passenden Kennzahlen für einen Disaster-Recovery-Plan** zu definieren, um die Ausfallzeiten zu minimieren. **Disaster Recovery ist Teil der Business Continuity,** zusammen mit allen Prozessen, die eingebunden werden sollten, um die bestmögliche Methode zur Verkürzung der Ausfallzeit und zur schnellen Rückkehr in den Normalbetrieb zu finden. Ein **durchdachter Retention-Plan** mit den beiden Hauptzielen – **Zeitraum und Intervall** – kann dabei helfen, einen sinnvollen Backup-Prozess zu gestalten, der Ihren Möglichkeiten und Anforderungen entspricht.

Merken Sie sich - **ZEIT IST GELD – UND DATEN SIND ES AUCH!**

EUROstor

Hochredundanter ZFS-Speicher für Big Data von EUROstor mit Open-E JovianDSS

Der shared Storage Cluster ES-8700JDSS von EUROstor mit Open-E JovianDSS kombiniert die Vorteile des selbstheilenden ZFS-Dateisystems mit einer intuitiven Benutzeroberfläche im Browser sowie der Flexibilität beim Design von Datenpools, die über FC oder Ethernet an Kunden bereitgestellt werden. In dieser Konfiguration wird die Datenverteilung gleichmäßig auf 4 JBODs mit insgesamt 44 Festplatten aufgeteilt. Dadurch entsteht eine Redundanz über das gesamte Chassis mit einer nutzbaren Nettokapazität von 75 % der Gesamtkapazität. Bei voller Bestückung mit den derzeit größten verfügbaren 22-TB-Festplatten ergibt sich eine nutzbare Gesamtkapazität von 1,3 PiB.

EUROstor GmbH
Deutschland

Business Continuity

Business Continuity ist eine Art Plan im Bereich Risikomanagement, der Ihnen hilft, die wichtigsten organisatorischen Funktionen zu verstehen, die Gründe für deren Absicherung zu erkennen – und Ihre Daten in jedem erdenklichen Szenario wiederherstellen zu können. Die grundlegenden Funktionen **verhindern Datenverlust**, etwa durch stille Datenbeschädigung, oder schützen Ihre Unternehmensdaten mit geeigneter Redundanz, indem Paritätsdaten in der Speicherstruktur abgelegt werden.

Dazu gehört ein **High-Availability-Cluster** mit einer zusätzlichen Produktions- und Backup-Umgebung, die einspringt, sobald das primäre System ausfällt. Außerdem kommt die On- und Off-site Data Protection **mit Open-E JovianDSS** zum Einsatz, um Hot-Data-Backups vor Ort oder Cold Data, also z. B. **ausgelagerte Archive,** zu sichern. Diese Maßnahmen gehören zu den ersten Schritten, um Verfahren zur Disaster Recovery zu aktivieren – auf die wir später noch eingehen. Ein solcher Plan vermittelt Ihnen einen vollständigen Überblick über potenzielle Notfallszenarien, damit Sie in der Lage sind, den Betrieb im Ernstfall zumindest auf Basisniveau aufrechtzuerhalten.

Wenn Sie wissen, was Business Continuity bedeutet, können wir uns nun auf die entscheidenden Erfolgsfaktoren und Tipps konzentrieren, **um sie möglichst effizient umzusetzen**.

Stellen Sie Widerstandsfähigkeit ganz oben auf Ihre Prioritätenliste. Sie hilft dabei, Schwachstellen im System aufzudecken und sich auf mögliche Desaster vorzubereiten. Im Rahmen dieser Strategie sollten Sie das organisatorische Umfeld analysieren, um nachfolgende Maßnahmen sinnvoll zu priorisieren – sowohl lokal als auch remote. Dabei müssen alle potenziellen Backup-Szenarien bewertet werden.

Hier sind die wichtigsten Tipps zur Sicherstellung der Business Continuity:

- Ermitteln Sie, welche Funktionen für den Betrieb Ihres Unternehmens essentiell sind, und priorisieren Sie deren Aufrechterhaltung im Störungsfall.
- Implementieren Sie Backup-Systeme und Redundanzen, um sicherzustellen, dass kritische Infrastruktur und Technologie im Störungsfall wiederhergestellt werden können.
- Schulen Sie Ihre Mitarbeitenden und stellen Sie sicher, dass Sie den Business Continuity Plan sowie die Notfallverfahren kennen.
  Merken Sie sich: Menschliches Versagen ist weiterhin die Hauptursache für Datenverlust.
- Nutzen Sie Off-Site-Standorte, um sicherzustellen, dass kritische Daten im Ernstfall wiederhergestellt werden können.
- Entwickeln Sie einen Krisenkommunikationsplan und stellen Sie sicher, dass alle Mitarbeitenden damit vertraut sind – für eine effektive Kommunikation im Störungsfall.
- Setzen Sie auf redundante Stromversorgung und Notstromaggregate, um kritische Infrastruktur bei Ausfällen mit Energie zu versorgen.
- Etablieren Sie Kommunikationsprotokolle mit Mitarbeitenden, Kunden, Partnern und weiteren Stakeholdern während einer Störung.

DISASTER RECOVERY

Einigen wir uns darauf: **Kein Backup zu haben bedeutet, ein zu großes Risiko** für ein erfolgreiches Business-Management einzugehen. Niemand möchte die Konsequenzen eines Datenverlusts – sei es bei sich selbst oder bei Kund:innen – tragen müssen. **Reputationsverlust, rechtliche Konsequenzen oder finanzielle Schäden** sind oft weitaus schwieriger zu bewältigen als eine frühzeitige Investition in geeignete Disaster-Recovery-Lösungen. **Wie bereits gesagt: Zeit ist Geld – und Daten sind es auch!** Ein passender Backup-Plan, abgestimmt auf Ihr Geschäftsmodell, sorgt für Sicherheit und stärkt das Vertrauen in den Markt. Er verschafft Ihnen **einen Wettbewerbsvorteil**, indem er eine smarte Disaster-Recovery-Strategie gewährleistet – damit Sie **nicht abgehängt werden**, wenn etwas schiefläuft.

Hier sind die wichtigsten Tipps für eine erfolgreiche Disaster Recovery:

- Erstellen Sie regelmäßig Sicherungskopien aller geschäftskritischen Daten an einem sicheren Ort.
- Lagern Sie Backups an einen geschützten externen Standort aus, um sie bei physischen Schäden wiederherstellen zu können.
- Verwenden Sie Virtualisierungstechnologien für eine schnelle und flexible Disaster Recovery.
- Nutzen Sie mehrere Netzwerkpfade zur Sicherstellung der Netzwerkverfügbarkeit.
- Bestimmen Sie, welche Systeme und Daten für den Geschäftsbetrieb unerlässlich sind, und priorisieren Sie deren Backup und Wiederherstellung.
- Etablieren Sie Kommunikationsprozesse mit allen relevanten Stakeholdern im Katastrophenfall.

Zwei zentrale Kennzahlen helfen Ihnen, das System optimal wiederherzustellen und den Verlust von Daten, Zeit – und damit Geld – zu vermeiden: **Recovery Point Objective** und **Recovery Time Objective**. Sie gelten als Schlüsselindikatoren für die Systemverfügbarkeit.

Recovery Point Objective (RPO)

RPO beschreibt, wie viele Daten ein Unternehmen im schlimmsten Fall verlieren kann, und hilft dabei, Häufigkeit und Art der Backups zu bestimmen, um das gewünschte RPO zu erreichen.

- **Infrastruktur bewerten** – analysieren Sie die Hardware-, Software- und Netzwerkkomponenten Ihres Backup- und Wiederherstellungsprozesses, um potenzielle Engpässe oder Einschränkungen zu identifizieren.
- **Mehrere Backup-Methoden verwenden** – setzen Sie auf eine mehrstufige Backup-Strategie mit einer Kombination aus lokalen, externen und Cloud-Backups.
- **Backup- und Wiederherstellungsprozesse automatisieren** – stellen Sie sicher, dass Backups konsistent und regelmäßig durchgeführt werden, um menschliche Fehler zu minimieren.
- **Backup- und Wiederherstellungsprozesse regelmäßig testen** – durch Tests wird sichergestellt, dass der Prozess wie vorgesehen funktioniert und Daten im Ernstfall schnell und zuverlässig wiederhergestellt werden können.

Recovery Time Objective (RTO)

RTO ist eine Kennzahl im Bereich Disaster Recovery und Business Continuity. Sie gibt an, wie viel Zeit maximal zur Verfügung steht, um eine geschäftskritische Funktion nach einem Ausfall wiederherzustellen. Der RTO-Wert ist entscheidend für die Wahl der passenden Ressourcen und Strategien im Notfallplan.

- **Risikobewertung durchführen** – identifizieren Sie kritische Geschäftsprozesse und analysieren Sie die potenziellen Auswirkungen eines Ausfalls.
- **Disaster-Recovery-Plan erstellen** – basierend auf der Risikobewertung, mit einem detaillierten Plan zur Wiederherstellung geschäftskritischer Funktionen.
- **Technologien wählen, die den RTO optimal unterstützen** – z. B. geeignete Backup- und Wiederherstellungslösungen, Hardware und Cloud-Dienste.
- **Disaster-Recovery-Plan umsetzen** – inklusive der Entwicklung entsprechender Abläufe und Protokolle.

Resilienz gehört ganz nach oben auf die Agenda

Die **Reaktion** ist ein wesentlicher Bestandteil der Business Continuity, da sie einen Notfallplan vorgibt, wie jede Abteilung im Falle eines unerwarteten Ereignisses handeln soll. Diese Strategie sollte auch Anweisungen enthalten, wie bei routinemäßiger Wartung der IT-Infrastruktur vorzugehen ist:

- **Verhaltenskodex für alle Mitarbeitenden mit Anweisungen, wie sie bei Datenverlusten und Notfällen reagieren sollen**
- **Aktuelle Kontaktdaten der Mitarbeitenden und externen Partner, die im Falle eines Datenverlusts verantwortlich sind**
- **Kommunikationskanäle, die im Falle eines Datenverlusts definiert und etabliert sind**
- **RPO und RTO klar im SLA definiert**
- **„Safety Drills" sowohl für Business Continuity als auch für Disaster-Recovery-Pläne**

Recovery dagegen hilft, einen konkreten Plan oder ein Szenario zu entwickeln, um nach einem Notfall oder unerwarteten Ereignis wieder zur vollständigen Betriebsfähigkeit zurückzukehren. Die Wiederherstellungsstrategie kann – je nach Art und Größe des Unternehmens – unterschiedliche Wege umfassen:

- **Nutzung von Backup-Infrastrukturen, Geräten oder Einrichtungen**
- **Wiederaufnahme des Regelbetriebs mit internen oder externen Ressourcen**

Just Technology GROUP

Just Technology Group Data Storage Services

Just Technology Group ist ein Managed Service Provider, der Hunderte von Kunden betreut. Mit Open-E JovianDSS können wir virtuelle Maschinen erstellen, verwalten und wiederherstellen – genau auf die Bedürfnisse unserer Kunden abgestimmt.
Als Partner von Open-E seit 5 Jahren haben wir zahlreiche Kunden dabei unterstützt, Remote-Backups und Disaster-Recovery-Pläne umzusetzen. Dank Rollback-Funktionen und Cloning-Tools lassen sich verlorene Daten und Infrastrukturen innerhalb weniger Minuten wiederherstellen – und Ausfallzeiten effektiv vermeiden.
Snapshots alle 5 Minuten ermöglichen es, Systeme bei Bedarf auf einen früheren Zustand zurückzusetzen – etwa bei Problemen oder Sicherheitsvorfällen.

Just Technology Group
Vereinigtes Königreich

Zusammengefasst: Dies sind die Schlüsselfaktoren für die Sicherstellung von Business Continuity und Datenschutz. Nachfolgend haben wir einige der wichtigsten Punkte zusammengefasst:

→ Backup- und Disaster-Recovery-Plan:

Einer der wichtigsten Aspekte von Disaster Recovery im Bereich Datenspeicherung ist eine umfassende Backup- und Recovery-Strategie. Diese umfasst regelmäßige Datensicherungen, das Speichern von Backups an externen Standorten und das Testen des Wiederherstellungsprozesses, um sicherzustellen, dass Daten im Katastrophenfall schnell wiederhergestellt werden können – gemäß Ihrem Disaster-Recovery-Plan.

→ Redundanz:

Redundanz ist ein entscheidender Aspekt der Disaster Recovery im Storage-Bereich, da sie sicherstellt, dass Daten und Systeme auch dann verfügbar bleiben, wenn eine Komponente ausfällt. Dazu zählen redundante Storage-Systeme, Backup-Generatoren und redundante Netzwerkverbindungen..

→ Skalierbarkeit:

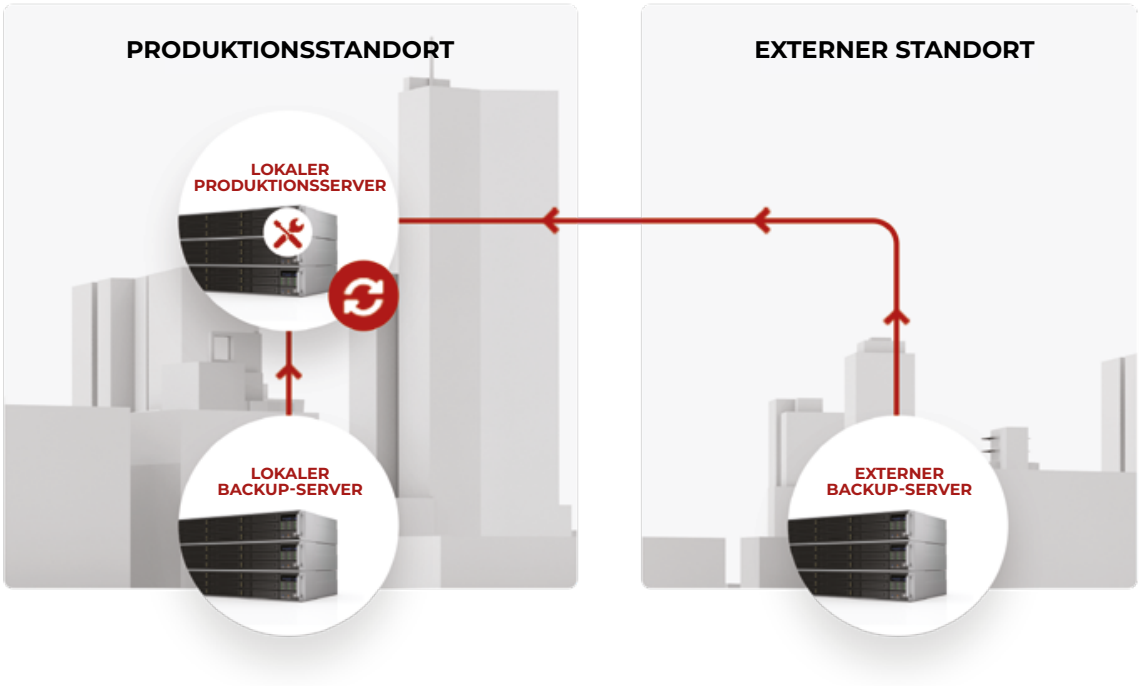
Disaster-Recovery-Pläne müssen skalierbar sein, um mit dem Wachstum und den sich verändernden Anforderungen eines Unternehmens Schritt zu halten. Das bedeutet, dass ausreichend Speicherkapazität für zukünftiges Wachstum verfügbar sein muss – und dass der Disaster-Recovery-Plan problemlos an neue geschäftliche Anforderungen angepasst werden kann.

Sobald ein umfassender Disaster-Recovery-Plan erstellt und Business Continuity sichergestellt wurde, sollten Backup, Recovery, Redundanz und Skalierbarkeit als essenzielle Bestandteile für Speicherlösungen integriert sein. Ziel ist es, die Auswirkungen von Ausfällen auf den Geschäftsbetrieb zu minimieren und wertvolle Daten zu schützen.

ON- UND OFF-SITE DATA PROTECTION für Disaster Recovery

mit Open-E JovianDSS

Die **On- und Off-site Data Protection**-Funktion der Open-E JovianDSS Data Storage Software ermöglicht es, wichtige Unternehmensdaten im Falle eines unerwarteten Ereignisses zu sichern und wiederherzustellen – durch die Kombination mehrerer Technologien. Diese Funktion erlaubt die Erstellung konsistenter Snapshots sowie die asynchrone Snapshot-Replikation an lokale und/oder entfernte Standorte. Die Replikationsaufgaben können je nach spezifischen Anforderungen dank fortschrittlicher Aufbewahrungspläne konfiguriert werden.



Die **On- und Off-site Data Protection** ist äußerst flexibel, da sie eine breite Palette an Disaster-Recovery-Plänen abdeckt – ohne zusätzliche Drittanbieter-Tools. Ein Aspekt wird dabei jedoch oft unterschätzt: Das extern gespeicherte Backup ist wesentlich zuverlässiger und sicherer und kann in unternehmenskritischen Situationen eingesetzt werden. On-site-Backup ist natürlich ebenfalls nützlich, bietet aber keinen vollständigen Schutz. Unerwartete Ereignisse oder andere Ausfälle können zu einem vollständigen Hardwareschaden führen.

Wenn das passiert, verlieren Sie alle Daten – und müssen mit den Folgen leben, die deutlich schwerwiegender sein können als die Investition in ein Off-site-Backup. Bewerten Sie das, während Sie sich mit **Aufbewahrungsplänen** beschäftigen, die auf **Snapshot-Backups** basieren.

Gegründet im Jahr 1998 ist Open-E ein etablierter Entwickler von IP-basierter Speicherverwaltungssoftware. Das Flaggschiffprodukt, **Open-E JovianDSS**, ist eine leistungsstarke, preisgekrönte Speicherlösung, die mit gängigen Industriestandards hervorragend kompatibel ist.

Sie ist zudem besonders benutzerfreundlich und einfach zu verwalten. Darüber hinaus zählt sie zu den stabilsten Lösungen am Markt und gilt als unangefochtener Preis-Leistungs-Sieger.

Dank seines hervorragenden Rufs, seiner langjährigen Erfahrung und seiner unternehmerischen Verlässlichkeit ist Open-E heute der bevorzugte Technologiepartner führender IT-Unternehmen. Weltweit wurden bereits über 38.000 Installationen mit Open-E realisiert.

+40.000 Software-Installationen

+100 Länder weltweit

+25 Jahre Erfahrung

+800 zertifizierte Vertriebs- und Technikexperten

Scan to learn more

Open-E, Inc. | +1 (678) 666 2880 (USA) | +49 (89) 800777 0 (Europa) | info@open-e.com