Acronis

#CyberFit

Die geheime Abkürzung zur Disaster Recovery

Inhalts-verzeichnis

Einleitung

Wahrscheinlich glauben Sie, Backups allein reichen aus. Wahrscheinlich wissen Sie nicht, wie wertvoll Ihre Daten, Systeme und Anwendungen sind, bis es zur Kompromittierung kommt. Disaster Recovery ist der zusätzliche Schritt, der nötig ist, um nach einem Ausfall schnell wieder auf die Beine zu kommen.
Ja, wir wissen, das wird Ihnen niemals passieren. Es ist nur ein nützliches Extra.

Was ist Disaster Recovery?

Disaster Recovery (DR) funktioniert nicht ohne Backup. DR umfasst aktuelle Kopien der Daten und Verarbeitungsfunktionen auf einer Plattform, die Ihnen die automatische Verfügbarkeit Ihrer wichtigsten Daten, Systeme und Anwendungen ermöglicht.

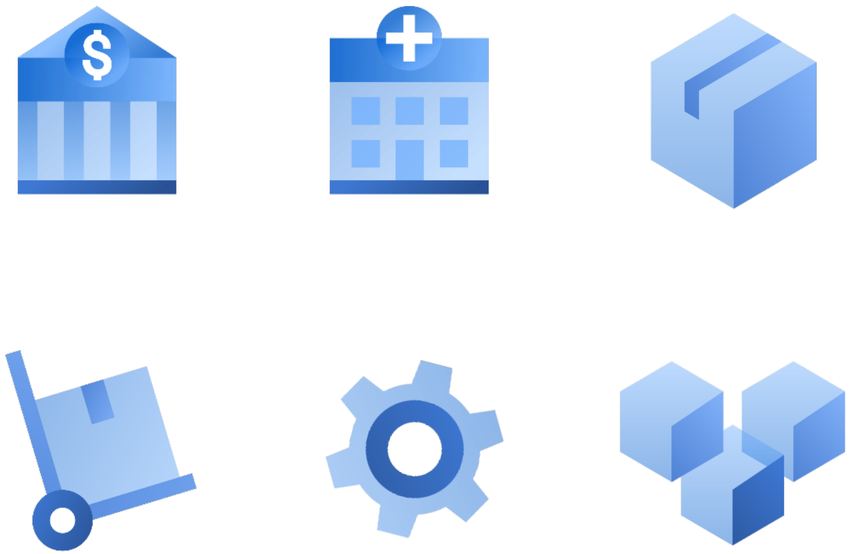
DR sorgt dafür, dass voneinander abhängige Prozesse in der richtigen Reihenfolge, auf dem richtigen Recovery-Punkt und zum richtigen Zeitpunkt wiederhergestellt werden.

Ist Ihr Unternehmen bereit?

Wer benötigt DRaaS? Jeder. Jedes Unternehmen kann einer Katastrophe zum Opfer fallen. Eventuell sind Sie in einer katastrophenanfälligen Region oder verfügen nicht über die technischen Ressourcen oder das nötige Fachwissen, um ein Disaster Recovery-Programm umzusetzen.

Folgende Branchen sind auf geschäftskritische Anwendungen und Daten angewiesen oder müssen bei Verstößen gegen gesetzliche Vorschriften mit hohen Geldstrafen rechnen:

- Finanzdienstleistungen
- Gesundheitswesen
- Rechtsbranche
- Transportbranche
- Telekommunikation
- Fertigungsindustrie
- Baubranche
- Energiebranche
- E-Commerce
- Versorgungsunternehmen
- Lieferketten und Logistik



Nicht nur die IT ist betroffen

Die Wiederherstellung des gewohnten Betriebs ist nicht nur für die IT ein Problem. Wenn auch Abteilungen wie Personal, Finanzen, Recht usw. von Ausfällen betroffen sind, werden sie zu einem unternehmensweiten Problem.

IT

- Backup und Recovery
- Interne und externe SLAs
- Zufriedenheit der Mitarbeiter
- Audits
- Einhaltung gesetzlicher Vorschriften

Führungsebene

- Pläne zur Gewährleistung der Geschäftskontinuität
- Marktwahrnehmung
- Produktivität der Mitarbeiter
- Einhaltung gesetzlicher Vorschriften
- Versicherung

Finanzwesen

- Einhaltung gesetzlicher Vorschriften
- Schutz sensibler Daten
- Aufrechterhaltung des Geschäftsbetriebs
- Markt- und ökonomisches Vertrauen
- Audits

Personal

- Planung für Stellen-besetzung und Belegschaft
- Schulungen
- Produktivität der Mitarbeiter
- Schutz sensibler Daten

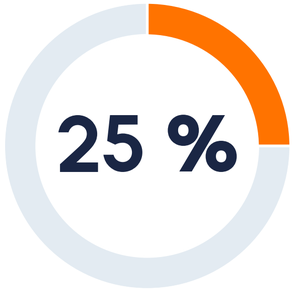
Rechtsbranche

- Einhaltung gesetzlicher Vorschriften
- Schutz sensibler Daten
- Versicherung

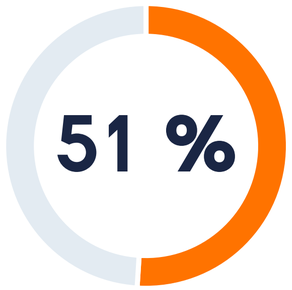
Die Realität

Jederzeit kann eine Katastrophe in unterschiedlichster Form eintreten.

Wir sind da, damit Sie nicht Teil der Statistik werden.



der Datenschutz-verletzungen im Jahr 2019 wurden durch versehentliches Löschen oder Überschreiben von Dateien oder Ordnern verursacht[1]



der Datenschutz-verletzungen im Jahr 2019 wurden durch kriminelle oder böswillige Angriffe verursacht[1]

der Unternehmen werden wahrscheinlich bis 2022 Geschäftsunterbrechungen wegen unbehebbarem Datenverlust erleiden[2]

der Unternehmen haben in den letzten drei Jahren Angriffe erlebt[3]

2,2 Tage

durchschnittliche Ausfalldauer[2]

5.600 $

durchschnittliche Kosten pro Minute[2]

3,92 Mio. $

durchschnittliche Gesamtkosten einer Datenschutzverletzung[2]

1) Ponemon Institute, 2019. 2) Gartner, 2019. 3) IDC, 2019

Die Bedrohungen

Für welche Bedrohungen sollten Sie vorsorgen? Eventuell glauben Sie, dass nur natürliche Desaster zu Unterbrechungen mit Stromausfällen und Hardware-Störungen führen können, doch müssen auch Versagen von Software und Mitarbeitern als Gründe für Ausfälle bedacht werden. Mit der weiteren Entwicklung der Technologie entstehen zudem neue interne und externe Bedrohungen.

Natürliche Desaster

Hurrikane, Tornados und Feuer können schwere Ausfälle verursachen, da sie auch Gebäude und Infrastruktur beeinträchtigen.

Viele Unternehmen verstehen wahrscheinlich nicht, dass nur 6 % der Ausfälle durch natürliche Desaster ausgelöst werden.

Pandemien

Bei dieser Art von Bedrohung sind vor allem die Mitarbeiter eines Unternehmens betroffen. Kommt noch die Arbeit im Home Office hinzu, entsteht eine ganze Reihe an Planungsszenarien, die von der IT bisher noch nicht berücksichtigt wurden.

Das Sicherheitsrisiko steigt, wenn Daten und Geräte permanent außerhalb der regulären IT-Infrastruktur genutzt werden.

Hardware-Fehler und Software-Beschädigungen

Hardware-Fehler können durch einen Stromausfall entstehen. Software kann durch fehlerhafte Updates oder inkorrekte Formatierung von Laufwerken beschädigt werden.

Menschliche Fehler – unabsichtlich oder böswillig

Menschliches Versagen kommt vor. Viele von uns haben schon einmal etwas versehentlich gelöscht oder überschrieben.

Zudem kann auch ein verärgerter Mitarbeiter verheerende Schäden an Daten und Systemen anrichten.

Cyberangriffe

Durch einen einzigen kompromittierten Rechner eines Mitarbeiters können ganze Netzwerke anfällig werden.

Schnell können Angriffe erfolgen, wenn Mitarbeiter schwache Passwörter verwenden, auf Phishing-Betrug hereinfallen oder auf böswillige Links klicken.

Die Entwicklung der Disaster Recovery

1990er

Rechenzentrum oder Colocation-Cage im Unternehmen

- Veraltete Hardware
- Netzwerke
- Lizenzierung
- Replikationsplattformen
- Enorme Speichermengen

2000er

Hybrider Ansatz

- Teure Lizenzierung
- Kompliziert
- Begrenzte Abdeckung

2010er

Moderne hybride und Cloud-basierte DR

- Kostengünstig
- Anwenderfreundlich
- Sofort einsetzbar

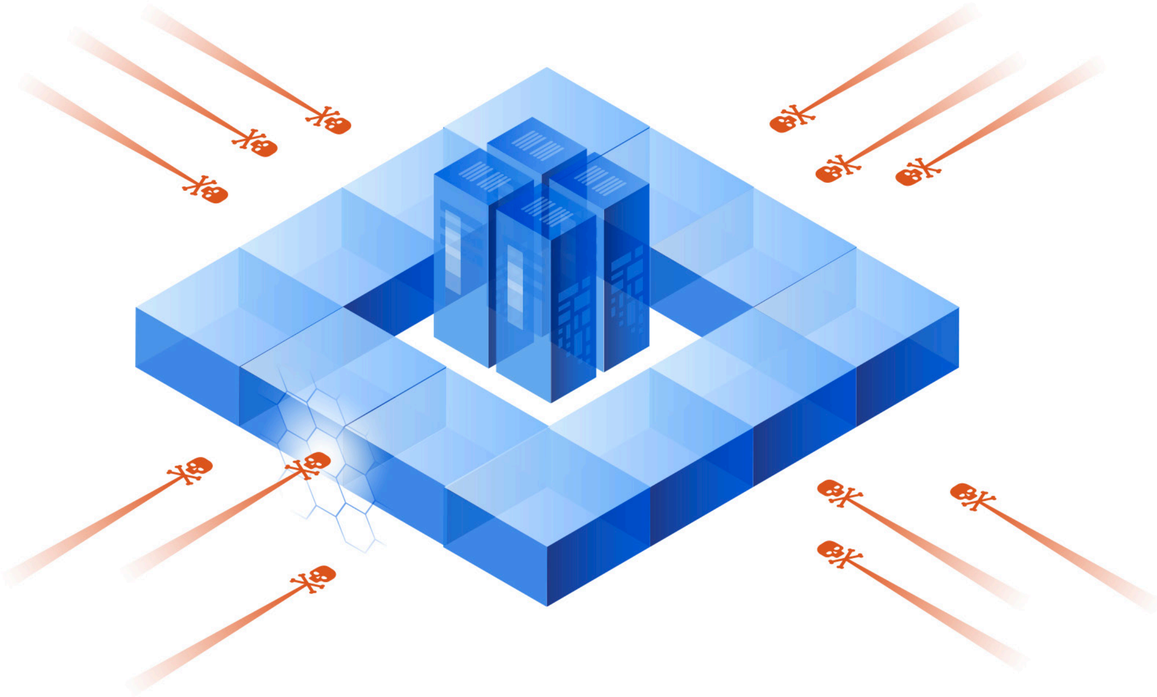
10 Gründe, warum Sie in Disaster Recovery investieren sollten

Es gibt viele Gründe, warum es sich lohnt, über Backups hinaus in Disaster Recovery zu investieren.

- Sehr viel **kostengünstiger** als je zuvor
- **Geringere Auswirkungen** von Katastrophen
- Gewährleistung ununterbrochener **Mitarbeiterproduktivität**
- Einhaltung **gesetzlicher Vorschriften**
- Nutzung **sofortiger Wiederherstellung**
- **Kürzerer Ausfall** des Geschäftsbetriebs
- **Weniger** potenzielle **Finanzverluste**
- **Weniger Risiken** durch Haftungsverpflichtungen
- **Geringeres Risiko** für negative Publicity
- **Optimiertes** Krisenmanagement

Angesichts der Vielzahl von internen und externen Faktoren, die Ihre Systeme und Daten beeinträchtigen können...

stellt sich nicht die Frage, ob Sie Datenverluste erleiden werden, sondern eher wann es passieren wird.



Berechnen Sie die Kosten durch Ausfälle

All diese Faktoren lassen sich auf Ihr Unternehmen anwenden. Um die tatsächlichen Ausfallkosten pro Stunde zu berechnen, werden Zahlen für Aufwand und Kosten aus allen Abteilungen herangezogen. Das Ergebnis: Ausfälle führen zu enormen finanziellen Verlusten.

Verlorener Gewinn + Verlorene Produktivität + Wiederherstellungskosten + Immaterielle Kosten = Ausfallkosten (pro Stunde)

Verlorener Gewinn

Dieser Punkt ist relativ leicht zu verstehen. Steht Ihr Unternehmen still, kann kein Gewinn erwirtschaftet werden. Berechnen Sie anhand des Bruttojahresumsatzes für jeden Geschäftsbereich den verlorenen Gewinn pro Stunde im Falle eines Ausfalls.

Verlorene Produktivität

Die Kosten durch Ausfälle steigen auch, wenn Ihre Mitarbeiter nicht arbeiten können oder dazu gezwungen sind, nicht gewinnbringende Tätigkeiten auszuführen. Gehälter oder Stundenlöhne sind fixe Kosten und müssen unabhängig von der Produktivität der Mitarbeiter gezahlt werden.

Wiederherstellungskosten

Oft werden die Kosten, die durch Wiederherstellung und Wiederaufnahme des regulären Betriebs entstehen, nicht bedacht. Beispiele für anfallende Kosten:

- Zeitaufwand von Dienstleistern und Mitarbeitern für die Wiederherstellung verlorener Daten
- Physische Tools bzw. Geräte, die repariert oder ersetzt werden müssen
- Kosten durch verlorene Daten

Immaterielle Kosten

Reputations- und Markenschäden führen zu finanziellen Verlusten. Der kleinste Ausfall kann zu unwiderruflichen Schäden für Ihr Unternehmen führen. Wie der Ausfall gehandhabt wird, kann zudem entscheidend dazu beitragen, ob Ihr Unternehmen wieder auf die Beine kommt oder untergeht.

Umsetzung eines DR-Programms

Um ein Disaster Recovery-Programm selbst zu verwalten, benötigen Sie Folgendes:

- **Personal für:**
  - Analysen
  - Erstellung
  - Test
  - Implementierung
  - Verwaltung
- **Schulungen**
- **Dokumentation**
- **Berichterstellung**
- **Wiederherstellungs-Infrastruktur**

Wenn Sie sich für einen zertifizierten Acronis Partner entscheiden, steht Ihnen Folgendes zur Verfügung:

- **Unsere jahrelange Erfahrung mit Disaster Recovery**
- **Schnelle und einfache Aktivierung von Disaster Recovery-Services**
- **Kontinuierliches und effizientes Bereitstellungsmodell**
- **Rund-um-die-Uhr-Support (24/7)**
- **Vereinfachte Testfunktionen**
- **Überwachung und Verwaltung**
- **Integrierte Cloud Storage- und Computing-Ressourcen**
- **Kostengünstige Betriebsausgaben**

Geschäftskontinuität wird jetzt noch einfacher

Stellen Sie sich vor, Sie benötigen nur einen Agenten, eine Konsole und eine Cloud.

Data Protection +

Cyber Security +

Disaster Recovery

Backup und Wiederherstellung

Schwerpunkt:

- Verhindern, dass wertvolle Daten verloren gehen
- Daten auf Servern, Workstations und mobilen Geräten

Endpunktverwaltung und Sicherheit

Schwerpunkt:

- Erkennung und Abwehr von Malware-Angriffen
- Schwachstellenbewertung und Konfigurationsverwaltung
- URL-Filter
- Patch-Verwaltung

Disaster Recovery

Schwerpunkt:

- Hochverfügbarkeit wichtiger Anwendungen
- Schnelle Wiederherstellung, um teure Ausfallzeiten zu vermeiden

Acronis

#CyberFit

Vielen Dank für Ihr Interesse!

Kontaktieren Sie uns noch heute, um zu erfahren, wie wir Ihr Unternehmen dabei unterstützen können, sich schneller von einer Katastrophe zu erholen.

www.acronis.com | dr@acronis.com