N-ABLE in Kooperation mit INFINIGATE

Gerüstet für den Ernstfall: Der Disaster-Recovery-Plan

Eine umfassende und qualitativ hochwertige IT-Betreuung besteht aus vielen, meist beweglichen Elementen: performante Monitoring- & Management-Systeme, eine ausführliche vertragliche Basis, effizientes Service Management und weiterem. Viele dieser Elemente zielen auf das reibungslose Management der IT-Infrastruktur des Kunden sowie die Vermeidung von Risiken ab. Letztere sind im IT-Umfeld sehr vielfältig und einem stetigen Wandel unterworfen. Für Managed Services Provider (MSPs) bedeutet das sowohl eine ständige Iteration der eigenen Prozesse als auch der eingesetzten Software-Lösungen.

Das übergeordnete Ziel ist dabei immer gleich: die Arbeitsfähigkeit des Kunden aufrecht zu erhalten. Um dies sicherzustellen, ist weitaus mehr als nur Software oder andere Lösungen notwendig. Umfassende Managed-Security-Konzepte bestehen aus einem vielschichtigen Netz von Anwendung, die ineinandergreifen und dienen dazu, ein möglichst großes Spektrum von Bedrohungen zu vermeiden. Eines haben diese teils sehr komplexen IT-Sicherheits-Strategien gemeinsam: Wenn alle genutzten Systeme nicht greifen und das Risiko zur Wirklichkeit wird, existiert eine regelmäßige und nachvollziehbare Daten- und Systemsicherung in Form von Backups.

Aber wie zuverlässig ist eine solche Sicherung tatsächlich? Wie gut ist ein Backup überhaupt, von dem man nicht weiß, ob man es wiederherstellen kann? Wie lange dauert eine Wiederherstellung im Zweifelsfall, wer ist verantwortlich und wie geht es nach einem Komplettausfall weiter?
Damit MSPs ihre Kunden für den Ernstfall rüsten, empfiehlt es sich einen Disaster-Recovery-Plan zu erstellen und ihren Kunden im Rahmen ihrer Managed Backup Services als Leistung anzubieten.

Backups als last line of defence – und profitable Dienstleistung

Ein großer Vorteil für IT-Dienstleister ist, dass Bedrohungen der IT-Sicherheit dank Verschlüsselungstrojanern, Hacker-Angriffen und Sicherheitslücken in moderner Hardware mittlerweile bei jedem Entscheider präsent sind. Somit ist wenig Überzeugungsarbeit notwendig, um Security- und passende Backup-Konzepte erfolgreich beim Kunden zu platzieren. Sollten dennoch Einwände vorhanden sein, empfiehlt es sich, gemeinsam mit dem Entscheider zu ermitteln, welchen Stellenwert die Unternehmensdaten haben, ob auf deren Zugriff verzichtet werden kann und wie lange das Unternehmen ohne funktionierende IT auskommt.

Zusätzlich profitieren Systemhäuser davon, dass viele Unternehmen ihr Budget für IT-Ausgaben deutlich erhöhen[1]. Das Thema Storage und Backup nimmt bereits jetzt zehn Prozent der IT-Ausgaben eines Unternehmens ein.

Diese hohen Werte begründen sich in den Kosten, die im Falle eines Datenverlustes entstehen: Laut IBM[2] lassen sich die durchschnittlichen Ausgaben im Falle einer Datenpanne auf 4,2 Millionen Euro beziffern. Auch die Allianz stellt fest, dass Unterbrechungen des Geschäftsbetriebes im Jahr 2020 das größte Risiko darstellen. beziffern. Auch die Allianz stellt fest, dass Unterbrechungen des Geschäftsbetriebes im Jahr 2020 das größte Risiko darstellen.

„Every business today not only needs to find answers to the question of how best to prevent business interruptions, but also how to best reduce their impact if they do happen“[3]

Für Unternehmen ist es also unabdingbar sich vor einem Datenverlust zu schützen, da Summen in dieser Größenordnung im schlechtesten Falle eine Insolvenz bedeuten. Laut einer Studie von Dell und Vanson Bourne[4] hatten 48 Prozent der befragten Unternehmen in Deutschland in den letzten zwölf Monaten bereits mit ungeplanten Systemausfallzeiten zu kämpfen, 32 Prozent erlitten sogar einen Datenverlust. Zwei Drittel der Befragten gehen zusätzlich davon aus, dass Service Level Agreements (SLAs) nicht eingehalten werden können und beinahe alle Teilnehmer gaben an, dass die von ihnen genutzten Backup-Lösungen nicht im Einklang mit ihren geschäftlichen Herausforderungen stehen.

[1] Etwa 44 Prozent der von Spiceworks befragten Unternehmen planen ihr Budget für IT-Ausgaben 2020 um 18 Prozent zu erhöhen. Vgl. https://www.spiceworks.com/marketing/state-of-it/report/
[2] vgl. https://www.ibm.com/security/data-breach
[3] vgl. https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html
[4] vgl. https://www.delltechnologies.com/de-de/data-protection/gdpi/index.htm

„Maintaining secure backups can also limit the damage from [cyber incidents]. Business resilience and business continuity planning are also key to reducing the impact of a cyber incident, although response plans need to be tested, practiced and regularly reviewed."[5]

Deutlich wird: Für IT-Systemhäuser besitzt die erfolgreiche Daten- und Systemsicherung ihrer Kunden eine besonders hohe Relevanz. Ein Verlust oder eine langfristige Störung dieser ist existenzbedrohend – eine schnelle Wiederherstellung der Arbeitsfähigkeit ist daher unerlässlich. Zu beachten ist hierbei jedoch ebenfalls, dass kaum ein Unternehmen seiner eingesetzten Lösung hinsichtlich einer reibungslosen Wiederherstellung der Daten traut. Dieser Mangel an Vertrauen ist zumeist dadurch begründet, dass die Sicherungsprozesse oftmals intransparent sind. Berichte, E-Mails und Checklisten geben zwar Auskunft über die Durchführung der Backups, aber Konsistenz und Wiederherstellbarkeit der Unternehmensdaten bleiben unklar.

Für IT-Dienstleister gilt es folglich, durch umfassende Disaster-Recovery-Pläne sowie zugehörige Prozessplanung und Wiederherstellungstests Risiken zu minimieren – und dadurch Vertrauen beim Kunden zu schaffen.

Transparenz und Vertrauen als Schlüssel zu erhöter Kundenbindung

Die folgenden vier Schritte bieten Systemhäuser hierbei Orientierung:

1. Stellenwert der Unternehmensdaten vermitteln
2. Vertrauen in die IT-Infrastruktur schaffen
3. Modernere Datensicherheitssysteme einsetzen
4. Minimierung von Wiederherstellungs-Zeiten

Eine strukturierte Herangehensweise zur Umsetzung dieser Punkte ist die Erstellung des bereits erwähnten Disaster-Recovery-Plans. Dieser ermöglicht es IT-Dienstleistern, effiziente Prozesse und Lösungen zur Wiederherstellung von Daten- und Systemen nach einem Sicherheitsvorfall zu definieren. Kunden schöpfen hierdurch Vertrauen, da das Vorliegen eines solchen Plans inklusive strukturierter Prozesse Professionalität ausstrahlt. Für Systemhäuser resultiert der Vorteil, dass sie eingesetzte Technikerzeit im Ernstfall minimieren.

Doch was bedeutet Disaster Recovery genau?

Synonym zu Disaster Recovery steht die Notfallwiederherstellung. Das heißt, dass es sich um eine Wiederherstellung des IT-Betriebes nach einer Störung oder einem Sicherheitsvorfall handelt. Dies bezieht sich nicht nur auf die Daten eines Betriebes, sondern auch deren Systeme, Anlagen oder Netzwerke.

Dabei sollte das Disaster Recovery nicht mit Business Continuity verwechselt werden. Ein angewandtes Risikomanagement durch einen umfangreichen Disaster-Recovery-Plan ist zwar Teil einer Business-Continuity-Strategie, diese bezieht sich jedoch über die IT-Infrastruktur hinaus auf die Aufrechterhaltung der Geschäftstätigkeit eines Unternehmens im Allgemeinen.

Es handelt es sich daher vor allem um eine technische Dienstleistung, dessen effektive Anwendung ein schriftliches Konzept für die eingesetzten Prozesse und Tätigkeiten bedarf. Hat man sich vor einem Datenverlust bereits über Abläufe, Tätigkeiten und Verantwortlichkeiten Gedanken gemacht, dann spart dies sowohl Zeit als auch Geld – und bietet Kunden die benötigte Transparenz, um Vertrauen zu schaffen.

[5] vgl. https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

Erstellung eines Disaster-Recovery-Plans

Primäres Ziel bei der Erstellung eines Disaster-Recovery-Plans ist es, Maßnahmen zu definieren, die die Herstellung der Arbeitsfähigkeit eines Unternehmens nach einem Ausfall und/oder Datenverlust zeitnah ermöglichen. Daher umfasst dieser sowohl Informationen zur technischen Struktur der Firma und verantwortlichen Personen (inklusive Vertretungen) als auch Handlungsanweisungen und Ablaufplänen für den Ernstfall. An dieser Stelle ähnelt er stark einem allgemeinen IT-Notfallplan oder Business-Continuity-Plan. Im Gegensatz dazu enthält der Disaster-Recovery-Plan jedoch ausschließlich Aktivitäten bezüglich der Datensicherung und stellt dadurch ein spezialisiertes Werkzeug für IT-Dienstleister und Endkunden dar.

Inhalt und Aufbau sollten seitens des Systemhauses standardisiert werden, damit der Plan effizient auf einen Großteil der Kunden übertragen und modular angepasst werden kann. Folgende Informationen sind zentraler Bestandteil des Disaster-Recovery-Plans und werden über IT-Infrastrukturanalysen, Checklisten, Audits und Vor-Ort-Termine beim Kunden eruiert:

- Welche Backup-Strategie oder-Konzept wird angewendet?
- Welche Systeme sind für den Erhalt der Arbeitsfähigkeit relevant, welchen Stellenwert haben diese für eine Priorisierung?
- Mit welchen Risiken ist zu rechnen? Wie wahrscheinlich sind diese Risiken?
- Ab welcher Abweichung vom SOLL-Stand wird die Meldestelle kontaktiert?
- Welche Abläufe sind notwendig, um dem SOLL-Stand wiederherzustellen? Wie lange darf dies dauern?
- Wann und in welchen Abständen werden diese Prozesse evaluiert, überprüft und testweise durchgeführt?
- Welche Personen inklusive Vertretungen sind für welche Prozesse oder Systeme verantwortlich und wie erreicht man sie? Welche Kommunikationswege werden für eine Benachrichtigung im Disaster-Fall gewählt?

Die Definition zentraler Fragestellungen ermöglicht es sowohl dem MSP als auch dem Kunden, komplexe Themen nachzuvollziehen – und so Bewusstsein und Vertrauen zu schaffen. Zur Beantwortung dieser empfiehlt sich ein strukturiertes Vorgehen, das wie folgt aussehen kann:

- **Identifikation kritischer Systeme**
  Genau notieren, welche Prozesse auf welchen IT-Systemen durchgeführt werden und welchen Stellenwert diese im Tagesgeschäft des Kunden haben.

  Diesen Schritt kann man aus einer IT-Infrastrukturanalyse ableiten, da dort bereits eine genaue Aufstellung der verwendeten IT-Systeme zur Verfügung steht. Existiert diese noch nicht, dann sollte die Erstellung dieser nachgeholt werden. Eine detaillierte Kenntnis des IST-Standes ist zwingend notwendig für die nachfolgenden Service-Prozesse.

- **Definition möglicher Ausfallzeiten**
  Wie lange kann tatsächlich ohne Zugriff auf die oben genannten Systeme produktiv gearbeitet werden und nach welchen Zeiträumen muss das Thema weiter eskaliert werden?

  Diese Information ist stark von der Arbeitsweise und -tätigkeit des Unternehmens abhängig. Hier kann genau festgelegt werden, wann welche Handlungen notwendig sind, um die Arbeitsfähigkeit wiederherzustellen. Daraus lässt sich ganz einfach sowohl

  - RTO (Recovery Time Objective: Wie lange darf ein System ausfallen?)

    als auch

  - RPO (Recovery Point Objective: Wie viel Zeit darf zwischen einzelnen Datensicherungen liegen? Welcher Datenverlust ist hinnehmbar?)

  ableiten. Mit diesen Informationen kann das eventuell noch zu definierende Datensicherungs-Konzept angereichert werden.

» **Erstellung eines Datensicherungs-Konzepts**
Was wird benötigt, um die definierten Wiederherstellungszeiten technisch einzuhalten?

Hier wird genau festgelegt, welche Daten und Systeme gesichert werden. Es empfiehlt sich eine detaillierte Dokumentation des Datensicherungsbetriebes (der Konfiguration des Backups inklusive Angaben über Sicherungspläne, Datenquellen, Ausschlüsse etc.) zu erstellen und separat auszuliefern. Dies kann auf Grundlage einer standardisierten Vorlage erfolgen, welche vom Service-Techniker während oder nach der Installation ausgefüllt wird.

Innerhalb des Datensicherungs-Konzepts sollte zentral definiert werden

- welche Systeme gesichert werden sollen,
- wie häufig Backup-Prozesse durchgeführt werden,
- wie lange Datensicherungen vorgehalten werden,
- an welchen Orten die Datensicherungen verbleiben,
- wer Zugriff auf die Datensicherung hat und erhält.

» **Schaffung von Redundanzen**
Gibt es einen Ausweichplan, um die Geschäftsbereitschaft bei voraussichtlich mittelfristig- oder längerem Ausfall der IT wiederherzustellen?

Abhängig von der vorherigen Definition kritischer Systeme und Ausfallzeiten sollte ein Alternativ-Plan dokumentiert werden, über den zumindest bis zur finalen Lösung des Sicherheitsvorfalls produktiv weitergearbeitet werden kann. Es wird definiert mit welchen Einschränkungen zu rechnen ist und auf welcher Grundlage die Redundanz des Produktivsystems zur Verfügung gestellt werden kann.
Denkbar ist hier die Spiegelung des Server-Systems auf mit der letzten Datensicherung auf einen Leih-Server oder auf einen entsprechenden Hyper-Visor, welche auch nicht unbedingt in der Kundenumgebung stehen muss (SaaS).

Deutlich wird: Die Klärung der Fragestellungen zur Erstellung eines Disaster-Recovery-Plans für kleine und mittelständische Unternehmen (KMU) zu umfangreich, komplex und vor allem zeitaufwändig. Für Systemhäuser entsteht folglich die Chance, Ihre Kunden durch einen erprobten, strukturierten und standardisierten Ablauf zu unterstützen. Ähnlich der IT-Infrastrukturanalyse kann ein Disaster-Recovery-Plan zentral vorbereitet und als Standard in Kundengesprächen genutzt werden. An dieser Stelle ist es zusätzlich wichtig, dass IT-Dienstleister den Wert ihrer Unterstützung aufzuzeigen. Denn sie sind als Experten für die IT-Infrastruktur ihrer Kunden die richtige Anlaufstelle, wenn es darum geht, einen reibungslosen Betrieb der IT-Infrastruktur zu ermöglichen – insbesondere im Notfall.

Erstellung eines Disaster-Recovery-Plans

Die Umsetzung der zuvor genannten Punkte stellt IT-Dienstleister teilweise vor Herausforderungen, da die sich daraus ergebenden Anforderungen technisch anspruchsvoll sind.

Um die Prozesse möglichst nachvollziehbar zu gestalten, bieten sich Lösungen an, die viele der im Disaster-Recovery-Plan definierten Anforderungen konsolidieren. Am Beispiel von N-able Backup begegnen IT-Dienstleister diesen Herausforderungen wie folgt:

Herausforderung	Umsetzung mit N-able Backup
Auslagerung – Sicherungsdaten sind den gleichen Risiken wie den Live-Systemen ausgesetzt, wenn sie innerhalb des Unternehmens aufbewahrt werden.	» Primäres Sicherungsziel sind zertifizierte Rechenzentren » Als sekundäres Ziel können lokale Medien im Unternehmen genutzt werden » Primäres und sekundäres Sicherungsziel synchronisieren sich automatisch untereinander » Zusätzlich können unendlich viele weitere hot- oder cold-standby Restores/Systeme eingerichtet werden
Prüfung – Backups müssen regelmäßig verifiziert werden, um im Disaster Fall wiederherstellbare Daten & Systeme zu erhalten.	» Prüfung der Sicherungsprozesse über zentrale Oberfläche » Individuelle Berichte für unterschiedliche Fehler und Ausfälle » Eigene Ansichten und Dashboards um Zeit/Aufwand für Monitoring zu minimieren » Integration in Monitoring-Systeme möglich
Verifikation – Wiederherstellbarkeit muss gewährleistet und regelmäßig überprüft werden.	» Automatische Test-Rücksicherungen der letzten erfolgreichen Sicherung ohne Hardware-Aufwand » Spiegelung von Systemen oder Daten in anderem Brandabschnitt/außerhalb der Kundenumgebung
Automatisierung – Wiederkehrende Prozesse müssen ohne Eingriff des Dienstleisters erfolgen können.	» Sicherungsdaten werden automatisiert außerhalb der Kundenumgebung gesichert » Schnittstellen für Branchen-Software und Eigenentwicklungen verfügbar
Compliance – Eingesetzte Lösungen müssen mit EU-DSGVO, GOBD und übrigen rechtlichen Maßstäben entsprechen.	» Hersteller, Lösung und Hersteller sind EU-DSGVO/GOBD-konform und ISO-zertifiziert » Vorlage zur Vereinbarung von AVV » Audit auf Geräte-Ebene um Änderungen/Anpassungen langfristig nachvollziehen zu können
Skalierbarkeit – Backups müssen „mitwachsen“, wenn sich Systeme vergrößern, ohne dass zusätzlicher Aufwand/Kosten für Dienstleister entstehen.	» Keine Begrenzung der verwendeten Rechenzentrums-Kapazitäten » Kalkulation basiert auf vom Dienstleister einfach zu beeinflussenden/anpassbaren Werten. Eingekaufte Pauschalen können einfach weiterverkauft werden.

Disaster-Recovery-Plan als Must-have

Aufgrund der aktuellen Bedrohungslage durch Cyber-Kriminalität ist es sowohl für Unternehmen als auch IT-Systemhäuser unabdingbar, sich mit der Thematik Disaster Recovery auseinanderzusetzen.

Insbesondere KMUs sind jedoch an dieser Stelle überfordert und benötigen die Mithilfe ihres IT-Dienstleisters. Für Systemhäuser entsteht folglich die Chance, Ihre Kunden zu unterstützen und ihnen langfristig durch standardisierte Abläufe und Vorlagen optimale Backup-Dienstleistungen anzubieten – und zusätzliche monatliche Roherträge zu erwirtschaften. Ein gutes „Disaster Recovery-as-a-Service" ist somit die logische Erweiterung eines jeden Managed-Services-Konzepts.

Darüber hinaus setzen sich MSPs bei der Erstellung eines Disaster-Recovery-Plans intensiv mit den Geschäftsprozessen und zugehöriger IT-Infrastruktur des jeweiligen Kunden auseinander – und erhöhen somit dessen Bindung an seinen IT-Dienstleister. Zudem schafft ein solcher Plan die notwendige Transparenz, sodass das Vertrauen des Kunden in seinen IT-Dienstleister deutlich gesteigert wird.

Doch sollte man sich stets vor Augen führen, dass die reine Erstellung eines Disaster-Recovery-Plans nicht ausreicht. In der technischen Umsetzung steht das Systemhaus in der Pflicht, seine Kunden vor Datenverlusten zu schützen und im Notfall seine Arbeitsfähigkeit zeitnah wiederherzustellen. Regelmäßige Testrücksicherungen sind folglich ein **Muss** und kein **Kann**.

Autoren:
Florian Zeiter, Infinigate Deutschland GmbH
Hannah Strobel, Infinigate Deutschland GmbH

Sie möchten eine Live-Demo zu Virtual Disaster Recovery und Bare-Metal Restore mit N-able Backup erhalten?

» Schauen Sie sich das passende Video in unserer Infothek an: https://www.acmeo.eu/acmeothek/503

Sie möchten Sicherungen von Daten und Systemen Ihrer Kunden erfolgreich durchführen?

» Schauen Sie sich unsere Checkliste und das Video zu den zehn Schritten einer Systemsicherung mit N-able Backup in der Infothek an:
  » Checkliste: https://www.acmeo.eu/acmeothek/396
  » Video: https://www.acmeo.eu/acmeothek/397

Sie möchten N-able Backup testen?

» Starten Sie Ihre 30-tägige Teststellung unter: https://www.acmeo.eu/produkte/msp-backup-recovery

Sie benötigen Unterstützung dabei, Ihren Kunden Disaster Recovery als Dienstleistung anzubieten und diese effizient umzusetzen? Kommen Sie auf uns zu – wir beraten Sie gerne!

+49 511 515151-96

managed-services@infinigate.de