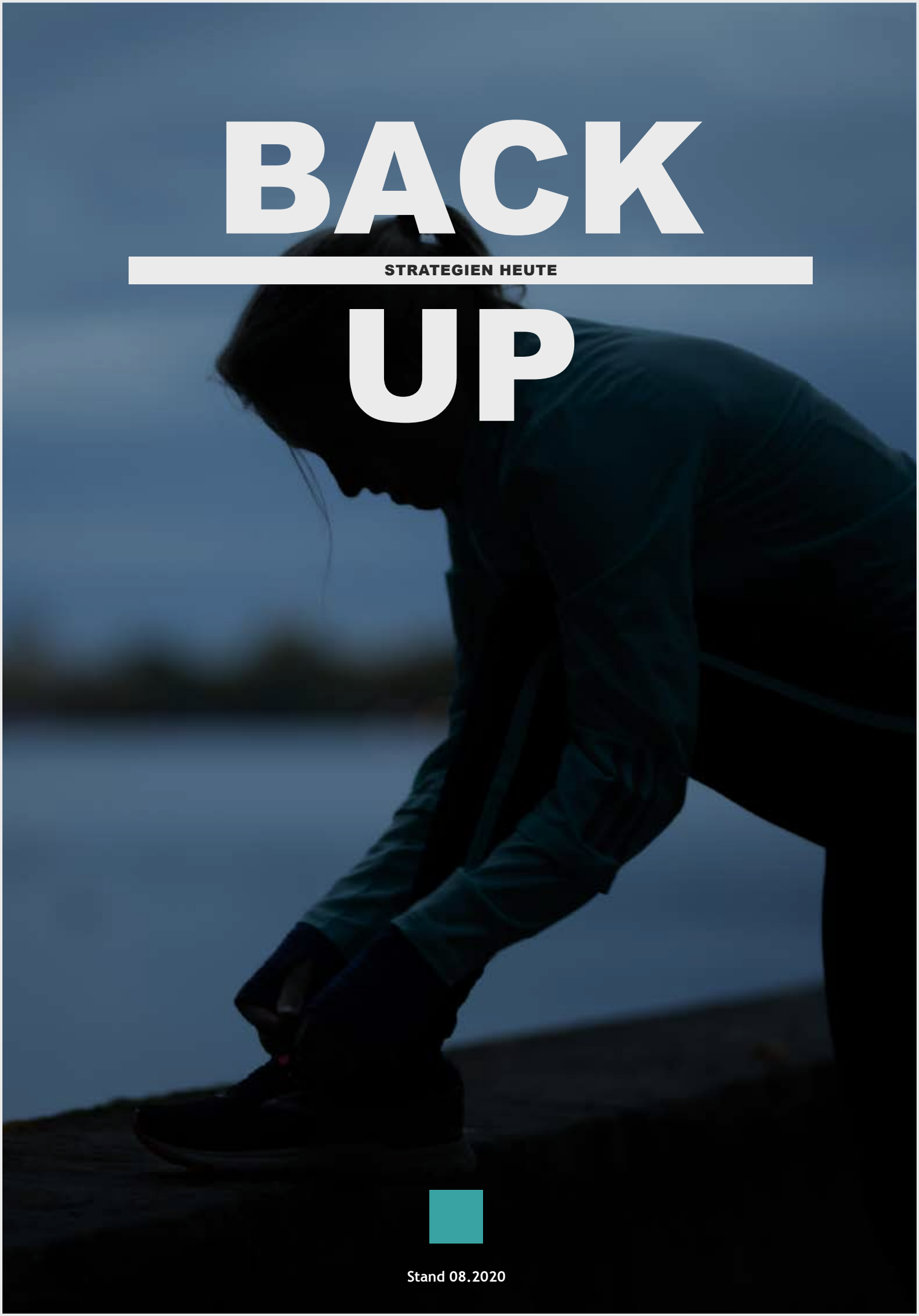

BACK UP

STRATEGIEN HEUTE

Stand 08.2020

WELCHE DATEN WANN UND WO-HIN SICHERN?

Neben der Erfüllung von möglichen gesetzlichen Bestimmungen dienen Backups hauptsächlich dazu, im Fall der Fälle (z.B. Hardware-Defekt, Feuer im Rechenzentrum, Diebstahl von mobilen Geräten, versehentliches Löschen von Daten) den Zustand vor dem Ausfall wiederherstellen zu können (Recovery).

Dies muss nicht zwingend eine Vollsicherung aller Dateien erfordern. Insbesondere bei Servern kann die Wiederherstellung aus zwei Schritten bestehen: automatisierte Neuinstallation von Betriebssystem und Anwendungsprogrammen und anschließend Wiedereinspielen der Nutzdaten aus dem Backup.

Backups von Servern und Clients

Zu unterscheiden sind Backups von Servern und Clients. Warum ist dies ein Unterschied? Auf Servern liegt aus Administrator-Sicht meist eine homogenere Situation vor, da Installationen hier in der Regel auch von Administratoren nach definierten Regeln vorgenommen wurden. Auf Clients dagegen haben es Administratoren in der Regel mit deutlich inhomogeneren Installationen zu tun, da die Nutzer der Clients hier individuelle Eingriffe vornehmen werden, z.B. Installationen von zusätzlicher Software oder individuelle Ablagestrukturen in den lokalen Datei-Verzeichnissen. Die beschriebene Recovery-Strategie „Automatisierte Erstellung der Umgebung mit anschließender Übernahme der Nutzdaten aus dem Backup“ ist daher auf Servern häufiger anwendbar und führt dort zu einem geringeren Umfang von zu sichernden Daten.

Bei der Sicherung von Datenbanken ist eine Besonderheit zu beachten: Datenbanken bestehen nicht nur aus den in ihnen abgelegten Nutzdaten (die wiederum irgendwo in Betriebssystemdateien gespeichert sind), sondern auch aus einer Vielzahl von Prozessen zur Datenverwaltung (z.B. Transaktionshandling). Aus diesem Grund ist es in den meisten Fällen empfehlenswert, die Datenbank-eigenen Backup-Tools zu verwenden, da diese in die Datenbank-Prozessverwaltung eingebunden sind. Ansonsten droht die Gefahr, dass man inkonsistente Daten sichert, wenn man unglücklicherweise genau zu dem Zeitpunkt eine (externe) Sicherung gestartet hat, als die Transaktionsverwaltung aktiv war.

Beim Backup einer Datenbank ist zu unterscheiden zwischen den folgenden Alternativen:

- Offline-Backup bestehend aus „Stoppen der Datenbank, Sicherung der relevanten Dateien und Wiederhochfahren der Datenbank“. In vielen Produktionsdatenbanken, die im 24*7-Betrieb betrieben werden, wird diese Variante nicht angewendet werden können.

- Online-Backup: Hier erfolgt die Datensicherung im laufenden Betrieb, in der Regel über spezielle Hersteller-Tools, z.B. bei Oracle im speziellen ARCHIVELOG-Modus.

- Logische Sicherung: Innerhalb der Datenbank wird eine Sicherung der Nutzdaten gestartet. Hierbei werden die Daten aus der Datenbank ausgelesen und dann in einer externen Datei in einem herstellerspezifischen Format abgelegt. Im Recovery-Fall kann der Datenbankzustand zum Zeitpunkt der logischen Sicherung dann innerhalb der Datenbank wiederhergestellt werden.

Bei der Sicherung von Clients – insbesondere von mobilen Clients – sind einige Besonderheiten zu beachten. Neben der Tatsache, dass Daten auf mobilen Endgeräten häufig verschlüsselt gespeichert sind, gilt es bei der Backup-Planung vor allem zu beachten, dass mobile Clients nicht immer vor Ort im Unternehmen sind. In die Backup-Strategie muss daher einfließen, dass eine Sicherung über das Netzwerk möglicherweise an fehlenden Netzressourcen (z.B. aus dem Homeoffice heraus) scheitern kann. Eine Alternative ist dann die Übertragung der Verantwortung für das Backup an den Nutzer des mobilen Endgerätes, der das Backup dann lokal durchführen muss.

Viele Unternehmen lagern ihre Datenhaltung in die Cloud aus. Auch von diesen Daten muss es ein Backup geben, denn Rechenzentren von Cloud-Anbietern können genauso von Ereignissen wie Feuer, Überschwemmung usw. betroffen sein. Wenn man entschieden hat, die Unternehmensdaten in einer Cloud abzulegen, dann kann man natürlich auch beim Thema Backup die gesamte Arbeit (und Verantwortung) an einen Cloud-Dienstleister übergeben. Möglicherweise bleiben aber auch dann noch Backup-Arbeiten übrig, nämlich die dauerhafte Sicherung von Daten, die nur temporär in der aktuellen Cloud-Arbeitsumgebung liegen dürfen, ab einem bestimmten Zeitpunkt aber zur Archivierung irgendwo anders gesichert werden müssen. Womit wir bei der Frage angekommen sind, wo die Daten eines Backups abgelegt werden sollen.

Wohin die Daten sichern?

Die Alternativen lauten hier „Cloud“ oder „On Premise“ (lokal). Wer sich schon einmal Gedanken um ein Backup seines privaten Rechners gemacht hat, der stand vor derselben Frage. Die Vor- und Nachteile der beiden Alternativen sind für eine betriebliche Backup-Strategie übertragbar. Im privaten Bereich hat man die Alternativen „Automatisierte Sicherung in Cloud-Umgebungen“ oder „Manuelle Sicherung von kritischen Daten auf USB-Stick / externer Festplatte“ (On-Premise). Die lokale Sicherung hat den Vorteil, dass man die Daten weiterhin Inhouse hat, was aber gleichzeitig ein Nachteil sein kann, da man das Backup-Speichermedium im Falle eines Feuers oder eines Einbruchs auch verlieren kann. Außerdem muss man regelmäßig an das Backup denken. Die Cloud-Lösung lässt sich einfacher automatisieren und bietet den Vorteil der (geografisch) getrennten Ablage des Backups. Gut überlegen muss man sich aber die Auswahl des Cloud-Anbieters für die Ablage des Backups. Neben den finanziellen Konditionen (bezahlt werden muss neben dem benötigten Speicherplatz häufig auch der Netzwerkverkehr zur Übertragung der Backup-Daten) spielt dabei auch eine Rolle, ob man dem Anbieter die möglicherweise sensiblen Daten anvertrauen will bzw. darf. Im betrieblichen Bereich kommen hier auch gesetzliche Bestimmungen ins Spiel, die z.B. eine Ablage der Daten auf Servern in bestimmten Ländern ausschließt.

Was gehört zu einer guten Backup-Strategie?

Mit der Festlegung, welche Daten wohin gesichert werden, ist eine Backup-Strategie aber noch nicht vollständig. Auch um Themen wie Dokumentation und Recovery-Test („Test des Ernstfalls“) sollte man sich frühzeitig kümmern.
Aus welchen Schritten besteht nun die Erstellung, Durchführung und Überwachung einer unternehmensweiten Backup-Strategie?
Die folgende Checkliste zeigt die wichtigsten Schritte:

- Welche Daten müssen gesichert werden? Die Notwendigkeit zur Sicherung kann sowohl aus gesetzlichen Notwendigkeiten bestehen (z.B. buchhalterische Fristen, DSGVO-Vorgaben zur verschlüsselten Archivierung) als auch das Ergebnis von Umfragen unter den für die unternehmenskritischen Systeme verantwortlichen Mitarbeitern sein („Welche Eurer Daten sind für Euch unverzichtbar?“).

- Wohin sollen Daten gesichert werden? Die beiden Alternativen „Cloud“ und „On-Premise“ wurden oben bereits erläutert.

- Wie häufig muss gesichert werden? Die Antwort auf diese Frage hängt davon ab, welcher Umfang eines möglichen Datenverlustes wegen zu seltener Sicherung maximal noch verkraftbar wäre. Einen 100%-igen Schutz gegen Datenverlust wird es nicht geben, denn Datenänderungen zwischen der letzten Sicherung und dem Zeitpunkt eines Blitzeinschlages in die Hardware sind verloren.

- Ist alles ausreichend dokumentiert? Festgelegt werden muss neben technischen Informationen zu den für Backup und Recovery benötigten Tools auch die Zuständigkeit für die Durchführung und Überwachung des Backups. Und auch die Verantwortlichkeit sowie das Vorgehen im Recovery-Fall sollten klar beschrieben und schnell wiederauffindbar sein. Im Ernstfall ist schnelles Handeln erforderlich.

- Ist das gesamte Backup- und Recovery-Szenario auch einmal durchgängig getestet worden?

Mit der richtigen Strategie kann man einem möglichen Ernstfall entspannter entgegensehen.

ÜBER DEN AUTOR

Rudolf Jansen ist Diplom-Informatiker aus Aachen und arbeitet als freiberuflicher Softwareentwickler und Autor. Er schreibt über alle IT-Themen und unterstützt seine Kunden bei Projekteinsätzen als Business Analyst und Requirements Engineer.