Datensicherung im KMU-Umfeld

Die schnelle und möglichst vollständige Wiederherstellung von Unternehmensdaten bei Verlusten durch böswillige, versehentliche oder zufällige Szenarien gehört zum unabdingbaren Grundschutz eines KMU. Dazu bedarf es der Implementierung eines ausgeklügelten Datensicherungsprozesses.

Wichtigste Merkpunkte für Unternehmen:

- Erstellen Sie ein Inventar Ihrer IT-Systeme und Daten und bestimmen Sie dafür jeweils den maximal tolerierbaren Ausfall resp. Verlust.
- Bilden Sie darauf basierend Schutzklassen von Objekten mit gleichem Risiko und definieren Sie für jede Schutzklasse das jeweilige Datensicherungskonzept.
- Definieren und implementieren Sie in Ihrem KMU einen Datensicherungsprozess.
- Prüfen Sie regelmässig die korrekte Datensicherung gemäss Datensicherungskonzept und die Wiederherstellbarkeit der Daten.

Der Datensicherungsprozess

Mit fortschreitender Digitalisierung nimmt auch in KMU die Zahl der eingesetzten IT-Systeme und die Menge an verarbeiteten Daten stetig zu. Damit steigt die Abhängigkeit der KMU von der uneingeschränkten Verfügbarkeit dieser IT-Systeme und Daten.

Umfangreiche Datenverluste, wie sie etwa durch böswillige Cyberangriffe, technische Defekte, Elementarschäden oder auch bloss durch versehentliche Löschungen entstehen, können für KMU eine existentielle Bedrohung darstellen. Die Fähigkeit einer schnellen und möglichst vollständigen Wiederherstellung von Unternehmensdaten aus einer Datensicherung gehört daher zum unabdingbaren Grundschutz.

Hierfür ist ein Datensicherungsprozess zu etablieren, der die ordnungsgemässe Durchführung der Datensicherung gemäss Datensicherungskonzept gewährleistet. Ebenso wichtig ist, dass in diesem Prozess auch regelmässig das Funktionieren der Datenwiederherstellung überprüft wird.

Die Schutzklassen

Nicht jedes IT-System einer KMU ist gleich kritisch für den Geschäftsprozess. Es braucht daher eine differenzierte Beurteilung des Schutzbedürfnisses von IT-Systemen und Daten. Ein umfassendes und aktuelles Inventar sämtlicher IT-Systeme und Daten bildet die Grundlage, um sich einen Überblick zu verschaffen und die darin geführten Objekte jeweils einer angemessenen Schutzklasse zuzuordnen.

Beispiel einer Schutzklassenzuordnung aufgrund von Kriterien

SK	Bezeichnung	Risiko	Max. tolerierbarer Ausfall/Verlust	Wiederherstellungszeit	Aufbewahrungsfristen
I	Normaler Schutzbedarf	Klein	> 1 Tag	1 Woche	
II	Hoher Schutzbedarf	Mittel	1 Tag	1 Tag	> 1 Monat

III	Sehr hoher Schutzbedarf	Hoch	1 Jahr

Neben der Gefährdung durch die genannten schädlichen Einflüsse sind weitere Kriterien in die Betrachtung einzubeziehen. Dazu zählen einerseits die Einschätzung des jeweils maximal tolerierbaren zeitlichen Ausfalls von IT-Systemen resp. des quantitativen Verlusts von Daten und andererseits die erforderlichen Aufbewahrungsfristen.

Mittels einer solchen Beurteilung lassen sich IT-Systeme und Daten mit ähnlichem Schutzbedürfnis zu Schutzklassen zusammenfassen. Für jede Schutzklasse werden daraufhin die Anforderungen an ein angemessenes Datensicherungskonzept definiert.

Das Datensicherungskonzept

Das Datensicherungskonzept legt für jede Schutzklasse die organisatorischen und technischen Details der Datensicherung fest. Zu den organisatorischen Details gehören dabei insbesondere:

1. Umfang der Datensicherung (Scope)
2. Periodizität der Datensicherung (täglich, wöchentlich, monatlich, ...)
3. Zeitpunkt der Datensicherung (Tagesende, Wochenende, Monatsende, ...)
4. Aufbewahrungsfristen der Datensicherungsstände (Generationenprinzip)
5. Geforderte Wiederherstellungszeiten (maximal tolerierbarer Ausfall)

Daraus leiten sich wiederum die technischen Details der Umsetzung ab, insbesondere:

1. Datensicherungsverfahren (voll, differentiell, inkrementell)
2. Datensicherungsmedium (Festplatte, Tape, ...)
3. Aufbewahrung der Datensicherungsmedien (on premise, physisch ausgelagert, Cloud, ...)

Umfangreiche Datenverluste – etwa durch böswillige Cyberangriffe, technische Defekte, Elementarschäden oder versehentliche Löschungen – können für KMU eine existentielle Bedrohung darstellen.

Mittels eines cleveren Datensicherungskonzepts kann das Risiko solcher Szenarien minimiert werden, indem eine schnelle und möglichst vollständige Wiederherstellung der verlorenen Daten erzielt wird.

Weiterführende Informationen

Mit dem **Umfang der Datensicherung** (Scope) wird festgelegt, welche Daten(-quellen) tatsächlich in der Datensicherung aufgenommen werden. Eine wohl überlegte und gut strukturierte Datenablage kann stark dazu beitragen, dass keine wichtigen Daten übersehen werden. Zudem ist zu prüfen, ob die zu sichernden Daten(-quellen) zum Zeitpunkt der Datensicherung auch tatsächlich verfügbar sind (z. B. ausgeschaltete Geräte am Wochenende).

Eine kurze **Periodizität der Datensicherungen** gewährleistet einerseits kleinere Datenausfälle, treibt im Gegenzug jedoch den Aufwand für die Datensicherung in die Höhe. Insbesondere kann es zu Engpässen im Netzwerk kommen, wenn täglich grosse Datenmengen gesichert werden sollen. Ein sorgfältiges Abwägen nach Schutzbedürfnissen ist hier angezeigt.

Der **Zeitpunkt der Datensicherung** richtet sich nach den Geschäftsabläufen. Dabei sollte der Risikoverlauf hinsichtlich eines Datenverlusts in der Zeitspanne zwischen den einzelnen Datensicherungen beurteilt werden. Häufig werden daher Tagesend-Sicherungen durchgeführt, um den Tagesbetrieb nicht zu stören und die freibleibenden Ressourcen in der Nacht für die Datensicherung zu nutzen.

Üblicherweise wird bei einem Datenausfall der Stand der letzten verfügbaren Datensicherung wiederhergestellt. Es kann aus unterschiedlichen Gründen manchmal aber auch erforderlich sein, weiter zurückliegende, historische Daten wiederherstellen zu können. Für solche Daten sind **Aufbewahrungsfristen der Datensicherungsstände** festzulegen. Mittels eines überlegten, an den Datenmengen und Schutzbedürfnisse des KMU orientierten Rotationsschemas (Generationen-Prinzip) können diese Aufbewahrungsfristen mit einem Minimum an Datensicherungsmedien gewährleistet werden. Z. B. können bei täglicher Datensicherung (Mo – Fr) mit nur 20 Datensicherungsmedien die Stände der letzten vier Wochentage (Mo – Do), der letzten 13 Wochenenden (Fr), der letzten beiden Monatsenden, sowie des letzten Jahresendes wiederhergestellt werden.

Mit den **geforderten Wiederherstellungszeiten** ist die Zeitspanne zwischen dem Feststellen des Datenausfalls bis zum Zeitpunkt des wiederhergestellten Zugriffs gemeint. Je kürzer dieser maximal tolerierbare Ausfall angesetzt wird, desto höher sind die organisatorischen und technischen Anforderungen an die Datensicherung. In Betracht zu ziehen sind hierbei die erforderlichen Zeiten für die Identifikation der wiederherzustellenden Daten, die Lokalisierung dieser Daten auf den jeweiligen Datensicherungen, den Zugriff auf die benötigten Datensicherungsmedien, sowie das eigentliche Zurückspielen der Daten.

Manchmal reicht die zur Verfügung stehende Zeit (z. B. Nachtstunden) nicht aus, um die Daten einer bestimmten Schutzklasse in der geforderten Periodizität vollständig zu sichern. Dieses Problem kann mit der Wahl des **Datensicherungsverfahrens** (voll, differentiell, inkrementell) gemindert werden. Bei der **vollen** Datensicherung (Vollbackup) wird eine vollständige Kopie sämtlicher Daten im Scope auf dem Datensicherungsmedium erstellt. Dieses Verfahren verursacht den grössten Platzbedarf auf dem Datensicherungsmedium und erfordert am meisten Zeit. Beim **differentiellen** Verfahren werden hingegen nur die seit der letzten vollen Datensicherung geänderten Daten gesichert (Differenz zum letzten Vollbackup). Das reduziert das Datenvolumen erheblich, da insbesondere unveränderliche Daten nur einmal gesichert werden müssen. Das Wiederherstellen eines Datensicherungsstands ist bei diesem Verfahren zweistufig: Es erfordert zunächst das Zurückspielen der letzten vorgängigen vollen Datensicherung und anschliessend das Zurückspielen der gewünschten differentiellen Datensicherung. Das **inkrementelle** Verfahren minimiert das zu sichernde Datenvolumen noch weiter. Hierbei werden nur die Änderungen zur letzten Datensicherung (egal nach welchem Verfahren) gesichert. Im Falle einer Wiederherstellung müssen daher die letzte volle Datensicherung, die letzte differentielle Datensicherung, sowie sämtliche anschliessenden inkrementellen Datensicherungen zurückgespielt werden.

Mit dem **Datensicherungsmedium** ist das Behältnis gemeint, das einen bestimmten Datensicherungsstand aufnimmt. Dabei kann es sich im einfachsten Fall um eine blosse Datei mit einem speziellen Dateiformat handeln oder aber auch einem physischen Datenträger (Festplatte, optisches Medium, Magnetband, ...) in einem dedizierten Backupsystem. Die Wahl des geeigneten Datensicherungsmediums richtet sich primär nach den organisatorischen Anforderungen (Umfang, Periodizität, Aufbewahrungsfristen und Wiederherstellungszeiten). Insbesondere für die langfristige Aufbewahrung (Archivierung) grosser Datenmengen haben sich Magnetbänder etabliert.

Datensicherungsmedien und deren **Aufbewahrung** sind für den gesamten Datensicherungsprozess geradezu von zentraler Bedeutung. In einer Risikoabschätzung sind Faktoren wie physischer Schutz, Lagerungsbedingungen, Verfügbarkeit, Zugänglichkeit usw. einzubeziehen. Generell sollten Datensicherungen von externen Einflüssen maximal isoliert sein. So ist z. B. in Zusammenhang mit Ransomware darauf zu achten, dass Datensicherungen für diese unerreichbar, also unbedingt offline aufbewahrt werden.