NOLTING SYSTEMS

Kommunikationstechnik ▪ Computerservice
Smarthome ▪ Beleuchtung ▪ Objektservice

Datensicherung – ein kleiner Leitfaden

Wozu dient eine Datensicherung?

Eine Datensicherung soll Ihre Daten vor Verlust schützen, indem Kopien Ihrer Daten für den Fall des Verlustes vorgehalten werden. „Daten“ sind Ihre persönlichen Ordner und Dateien, wie Dokumente, Bilder, Musik und Videos, aber auch Programme und das Betriebssystem (beispielsweise Windows) und deren Einstellungen.

Wie kommt es zum Verlust von Daten?

- Benutzerfehler

  Beispielsweise löscht ein Nutzer unabsichtlich ein Dokument, bemerkt dies aber erst später, wobei zwischenzeitlich auch der „Papierkorb“[1] geleert wurde, in welchen Dateien beim „Löschen“ in der Regel zunächst verschoben werden.

  Nicht selten wird auch ein Dokument verändert und gespeichert (überschrieben), wobei sich vielleicht später heraus stellt, dass dabei versehentlich Inhalte gelöscht oder unbeabsichtigt verändert wurden und man einfach die vorherige Version gern wieder zur Verfügung hätte.

- Schaden am Gerät

  Der Datenspeicher (Festplatte, SSD) ist defekt (Verschleiß, Fehlspannung, Unfall oder Elementarschaden) und verhindert Zugriff auf alle Daten, oder bestimmte Dateien sind beschädigt.

- Schadprogramme und Fremdzugriff

  Schadprogramme können sich beispielsweise durch das Öffnen von Email-Anhängen auf dem eigenen Computer einnisten. Dabei kann es sich um ausführbare Dateien (.exe, .com), aber auch Dokumente (.doc, .pdf etc.) oder Bilder handeln, in welche schädlicher Programmcode eingebettet ist. Prominentes Beispiel für Schadprogramme ist die so genannte Ransomware. Dabei hat sich ein Schadprogramm beispielsweise auf einem PC eingenistet, das im Hintergrund Ihre Daten verschlüsselt. Ohne den korrekten Schlüssel können die Daten dann nicht mehr genutzt werden. Anschließend wird der Geschädigte meist zu einer Geldzahlung für den Schlüssel erpresst. Es gibt natürlich noch viele weitere Angriffswege und Arten von Schadprogrammen, aber das würde hier den Rahmen sprengen. Auch kann es natürlich durch Diebstahl oder Sabotage zu Datenverlust kommen.

1 Eine Anmerkung zur Nutzung des „Papierkorbs“: Wir empfehlen, den „Papierkorb“ nicht regelmäßig zu leeren und ihn weniger als einen „Papierkorb“ anzusehen, sondern als eine Zwischenablage für versehentliche Löschungen. Einige Kunden verwechseln dies und meinen, sie sollten den „Papierkorb“ (wie einen echten Papierkorb) regelmäßig leeren, damit er nicht zu voll wird oder, damit es ordentlicher aussieht. Tatsächlich ist es nämlich so, dass der „Papierkorb“ ein bestimmtes Kontingent des Datenspeichers zugewiesen bekommt. Ist dieses ausgeschöpft, werden die ältesten Elemente automatisch aus dem „Papierkorb“ entfernt, um Platz für neue zu schaffen.

Strategien zur Prävention von Datenverlust

Zunächst einmal muss man sagen, dass es nicht nur einen richtigen Weg der Datensicherung gibt. Es gibt verschiedene Ansätze, die sich am subjektiven oder objektiven Wert der Daten und der konkreten Situation orientieren. Eine Lösung im geschäftlichen Bereich unterscheidet sich in der Regel stark von einer im privaten Bereich. Kern der Überlegungen ist immer, welche direkten oder indirekten Konsequenzen eines Datenverlusts zu erwarten oder zu befürchten wären. Die Bandbreite reicht da vom Achselzucken bis zum Verlust der geschäftlichen Existenz.

In der Regel möchte man seine Daten nicht verlieren. Im privaten Bereich ist es vielleicht die Fotosammlung, die einen hohen emotionalen Wert besitzt, oder auch eigene Texte, in die viel Arbeit geflossen ist. Im geschäftlichen Bereich kann man es sich meist nicht wirklich aussuchen, da eine Datensicherung vorgeschrieben ist - der Verlust geschäftlicher Daten wäre aber ohnehin oft sehr schmerzhaft. Dennoch ist es nicht selten, dass dieses Thema noch immer unzureichende Aufmerksamkeit bekommt.

Bevor es zu den Strategien geht, soll hier noch kurz der Begriff der *inkrementellen Sicherung* eingeführt werden. Datensicherungsprogramme lassen sich so einrichten, dass nur die seit der letzten Sicherung veränderten Dateien und Ordner gesichert werden und die Sicherungen entsprechend aufeinander aufbauen. Dies spart Zeit und Speicherplatz. Da Speicherplatz nicht unbegrenzt ist, muss man auch schauen, wie häufig gesichert werden soll und wie lange die Sicherungen vorgehalten werden sollen, bis sie ggf. überschrieben werden. Das Sicherungsintervall orientiert sich auch daran, in welchen Abständen neue Daten hinzu kommen und wie viel Arbeit potentiell verloren ginge.

- Gelegentliche, manuelle Kopien

  Auch bereits das manuelle Anlegen gelegentlicher Kopien wichtiger Dokumente auf einem externen Datenträger (USB-Stick, externe Festplatte etc.) kann für Privatleute eine angemessene Form der Datensicherung sein. Hierbei ist zu beachten, dass das verwendete Speichermedium nicht dauerhaft angeschlossen bleibt und nach jeder Kopie an einem angemessen Ort aufbewahrt wird. Bliebe das Speichermedium dauerhaft angeschlossen, bestünde die Gefahr, dass im Falle eines Ransomware-Angriffs auch die Kopien auf dem Speichermedium verschlüsselt werden. *Diese Sicherungsform ist nicht sehr komfortabel und anfällig dafür, vergessen zu werden.*

- Sicherung via Datensicherungsprogramm auf externe Festplatte (meist via USB)

  Hier verhält es sich ähnlich wie bei den manuellen Kopien. Im Unterschied dazu wird ein Programm für die Datensicherung installiert, welches so eingerichtet wird, dass es bestimmte Daten oder meist das komplette System auf Knopfdruck (meist inkrementell) sichert. Das bedeutet, dass der Prozess des Anlegens der Kopien automatisiert ist, aber noch immer manuell in Abständen angestoßen wird. Das Datensicherungs-Programm ließe es zu, einen Zeitplan zu erstellen, wonach die Datensicherung vollautomatisch vorgenommen werden würde. Damit dies wirklich vollautomatisch passieren kann, müsste die Festplatte jedoch dauerhaft angeschlossen bleiben, was aber aus o.g. Gründen (Ransomware) nicht zu empfehlen ist.

- Vollautomatische Sicherung auf einen lokalen Netzwerkdatenspeicher (NAS)

  Hier werden via Datensicherungsprogramm nach Zeitplan im Hintergrund Sicherungen gewünschter Dateien oder meist des kompletten System vorgenommen. Dies ist sehr

komfortabel für den Nutzer und vermeidet, dass Sicherungen vergessen werden. PC und NAS sind über das lokale Netzwerk (Ethernet, Router, Switch etc.) miteinander verbunden und halten die Verbindung. Daher gilt auch hier, dass die Daten vor Ransomware geschützt werden müssen. Um dies zu gewährleisten, wird der Zugriff des Nutzers auf die Datensicherung eingeschränkt, so dass dieser lediglich Lesezugriff auf die Datensicherung bekommt. Das Datensicherungsprogramm nutzt einen diskreten Zugang (eigens dafür am NAS eingerichtete Anmeldedaten), welcher verschlüsselt im Datensicherungsprogramm hinterlegt ist.

Da kein System absolut sicher ist und auch das NAS über verschiedene Wege kompromittiert werden könnte, raten wir dazu, die Sicherungen zusätzlich in Abständen auf eine externe Festplatte zu sichern und diese an einem sicheren Ort aufzubewahren. Optimalerweise ist der Aufbewahrungsort „Off-Site“, also in einem entfernten Gebäude. Beispielsweise nimmt man die externe Festplatte vom Büro mit nach Hause und verwahrt sie dort. Dies erhöht noch einmal den Schutz vor Ransomware, Elementarschäden, Diebstahl oder Sabotage.

- Vollautomatische „Off-Site“-Sicherung auf entferntem Datenspeicher (eigenes NAS oder „Cloud“)

  Dies ist die Sicherungsform, welche wir in unserem Unternehmen einsetzen. Unsere geschäftlichen Daten liegen auf einem NAS, welches diese im lokalen Netzwerk (und auch „remote“ via Internet) bereit stellt. Zudem werden die Systeme der PCs im Büro täglich darauf gesichert, um im Falle eines Ausfalls eines PCs den Arbeitsplatz über Rücksicherung auf ein Ersatzgerät schnell wieder einsatzfähig zu machen.[2] In einem entfernten Gebäude steht ein weiteres NAS zur Datensicherung bereit. Diese verläuft dann im Hintergrund über das Internet verschlüsselt von NAS zu NAS und ist unabhängig davon, ob die PCs im Büro eingeschaltet sind. Mit dem von uns verwendetem Sicherungsprogramm auf den NAS-Geräten lassen sich – verglichen mit üblichen Desktopalternativen – sehr komfortabel, präzise und vor allem Speicherplatz schonend auch sehr lange Vorhaltezeiten einrichten. Unsere Sicherung hält beispielsweise 24 stündliche Versionen, 7 tägliche, 4 wöchentliche, 12 monatliche und 2 jährliche Versionen vor. So erhalten Sie eine langfristige Sicherung, ohne dass Sie schnell immer wieder neue Speichermedien anschaffen oder das Speichervolumen erhöhen müssen.[3] Aus oben beschriebenen Gründen legen wir in Abständen zudem weitere, unabhängige Sicherungen auf einer externen Festplatte an.

2 Noch besser wäre eine Virtualisierung der Arbeitsplätze, was aber erst bei größeren Firmen wirtschaftlich und angemessen ist.

3 Wir möchten hier nicht zu technisch werden, aber hier dennoch auf einen entscheidenden Unterschied zu üblichen Sicherungsprogrammen eingehen, wie sie auf vielen PCs zum Einsatz kommen. Diese nutzen in der Regel inkrementelle Sicherungsketten. Diese Ketten sollten nicht zu lang werden, da dies a) die Geschwindigkeit der Sicherungsläufe stark negativ beeinflussen und b) zu Schwierigkeiten bei der Integrität der gesamten Kette führen kann, wenn „Glieder“ der Kette fehlerhaft sind. Daher werden bei dieser Methode in Abständen Vollsicherungen erstellt, welche entsprechend erheblich mehr Speicherplatz verbrauchen. Alternativ verwendet man auch so genannte differenzielle Sicherungen, bei der keine Ketten entstehen, sondern bei jedem Sicherungslauf die Differenz zur Vollsicherung gesichert wird. Dass dies nicht besonders Speicherplatz schonend ist, kann man sich sicher gut vorstellen.

Im Unterschied dazu nutzt das von uns verwendete Sicherungsprogramm einen gänzlich anderen Ansatz. Daten werden nicht in Containern gesammelt und gesondert abgelegt. Statt dessen werden Dateien und Ordner über ein verändertes Dateisystem markiert. Über Listen wird dann fest gelegt, welche Daten aus dem Datensicherungspool im jeweiligen Sicherungsordner angezeigt werden oder nicht. Dies umgeht das Problem der Versionsketten auf sehr elegante Weise.

Alternativ zum eigenen NAS können die Daten auch auf einem fremden Server („Cloud“) gesichert werden. Auf die Vor- und Nachteile möchten wir an dieser Stelle nicht im Detail eingehen. Besonders wichtig ist bei der Nutzung eines fremden Servers, dass die Datensicherung verschlüsselt wird. Das bedeutet, dass nicht lediglich die Übertragung der Sicherungsdateien verschlüsselt geschieht, sondern dass das Sicherungsprogramm (vor der Übertragung) verschlüsselte Dateien erstellt.

Ein wichtiger Hinweis zur Verwendung von iCloud: Wenn Sie iCloud nutzen, um beispielsweise Ihre Fotos auf Ihren Geräten zu synchronisieren, ist dies noch nicht unbedingt eine Datensicherung. Denn je nach Konfiguration werden Dateien beim Löschen auch auf allen Geräten und in der "Cloud" gelöscht und nicht vorgehalten. Man kann jedoch auch iCloud für eine Datensicherung nutzen. Auch hier gilt (insbesondere bei sensiblen Daten), dass die Datensicherung vor der Übertragung verschlüsselt werden sollte.

Abschließende Bemerkungen und Hinweise

Zum Abschluss möchten wir noch einen Klassiker der Missverständnisse zum Thema Datensicherung ansprechen: RAID ist keine Datensicherung. RAID 1 beispielsweise nutzt zwei Festplatten, wobei - grob gesagt - die eine Festplatte die Spiegelung der anderen ist. Das bedeutet auch, dass beispielsweise beim Löschen von Daten diese auf beiden Festplatten gelöscht werden. Dieses Verfahren erhöht jedoch die Datensicherheit dadurch, dass im Falle eines Ausfalls einer Festplatte die Daten weiterhin verfügbar bleiben und auch weiter damit gearbeitet werden kann. Die ausgefallene Festplatte wird dann zeitnah ersetzt, sodass die Spiegelung im Hintergrund wieder hergestellt werden kann. Wenn es wichtig ist, dass Daten unterbrechungsfrei verfügbar sind, bietet sich ein RAID als relativ kostengünstige Lösung für die notwendige Redundanz an. Ohne eine solche Redundanz müsste im Falle eines Ausfalls ja zunächst eine Wiederherstellung der Daten aus der Datensicherung erfolgen. In dieser Zeit wären die Daten nicht verfügbar, und es könnte entsprechend nicht damit gearbeitet werden. Auch für kleine und kleinste Unternehmen kann daher die Nutzung eines RAIDs nur wärmstens empfohlen werden. Dies gilt auch für Privatanwender, wenn viel mit den eigenen Daten gearbeitet wird. Der Arbeitsaufwand der Wiederherstellung ohne RAID kann recht hoch werden, sodass sich der finanzielle Mehraufwand sehr schnell lohnen kann. Im Privatbereich ist dies aber weit stärker eine Sache subjektiver Bewertung.

Dieser kleine Überblick zum Thema Datensicherung erhebt natürlich keinen Anspruch auf Vollständigkeit. Es gäbe noch viel dazu zu sagen, wobei es jedoch sehr in technische Details gehen würde, die im Zweifel eher den Überblick verringern, statt zu fördern. Bei Interesse informieren wir Sie natürlich gern über weitere Details.