



GESTALTEN > DIGITALISIERUNG > DATENSICHERHEIT UND DATENSCHUTZ AN SCHULEN

Datensicherung

Stand: 04.06.2024



Inhaltsverzeichnis

Datensicherung	3
Datensicherung im Kontext Schule	3
Vorgehensweise für die Erstellung eines Backup-Plans	4
FAQs Datensicherung	5
Downloads	7

Datensicherung



Durch Backups die Verfügbarkeit von Daten erhöhen ©Rachata - stock.adobe.com

Datensicherung im Kontext Schule

Eine Datensicherung, auch als Backup bezeichnet, stellt eine Schutzmaßnahme dar, um die Verfügbarkeit und die Integrität von einzelnen Daten oder ganzen IT-Systemen zu gewährleisten. In der Regel hängt die Auswahl geeigneter Methoden von verschiedenen Faktoren ab. Neben den Vor- und Nachteilen der verschiedenen Methoden, stellt diese Seite auch einen exemplarischen [Backup-Plan](#) zur Verfügung.

Notwendigkeit

Daten können verloren gehen. Dies muss nicht unbedingt der altersbedingte Crash einer Festplatte oder mutwillige Sabotage sein, auch ein versehentliches Löschen oder höhere Gewalt wie ein Blitzschlag oder eine Überschwemmung kann zu dem Verlust von Daten führen. Oft können diese entweder nur mit viel Mühe wiederhergestellt werden oder gar nicht mehr beschafft werden. Einige Daten sind für den reibungslosen Alltagsbetrieb einer Schule jedoch unentbehrlich und müssen im Notfall schnell wieder vorhanden sein. Bei zentral gespeicherten Daten gilt zudem noch zu berücksichtigen, dass eine automatische Synchronisierung zwischen Client und Server nicht die Funktionalität einer Datensicherung erfüllt, insbesondere dann, wenn die Daten von unterschiedlichen Geräten bzw. Benutzern

kollaborativ bearbeitet werden. Die Synchronisierung sowie die Verwendung eines zentralen Speicherortes ersetzen demnach kein Backup!

Vorgehensweise für die Erstellung eines Backup-Plans

Zielgruppe: pädagogischer Systembetreuer, Schulleitung

Bei der Übertragung von Daten auf ein Sicherungsmedium unterscheidet man zwischen einem Vollbackup, einem differentiellen Backup und einem inkrementellen Backup. Die Verfahren unterscheiden sich in der Menge der regelmäßig zu sichernden Daten, dem anfallenden Speicherplatzbedarf, abhängig von der Vorhaltdauer und der Anzahl der Sicherungen zu unterschiedlichen Zeitpunkten (Generationen):

Bewertung/Art	Beschreibung	Vorteile	Nachteile
Kopie	Eine Kopie ist jedes Mal ein vollständiges Backup, das alle ausgewählten Dateien sichert. U. U. werden die Daten noch gepackt. Das Mitsichern der Dateirechte muss u.U. beachtet werden	<ul style="list-style-type: none">· Einfache Handhabung bei der Erstellung und Wiederherstellung· Übersichtlich auch für Laien· Sehr einfaches Wiederherstellen von einzelnen Dateien	<ul style="list-style-type: none">· Großer Speicherplatzbedarf· Lange Sicherungsdauer
Synchronisieren	Beim Synchronisieren werden zwei Datenbestände abgeglichen. Es wird lediglich kopiert oder erstellt (Dateien oder Sektoren), was sich verändert hat.	<ul style="list-style-type: none">· Einfache Handhabung bei der Erstellung und Wiederherstellung· Sehr kurze Sicherungsdauer· Sehr geringer Speicherplatzbedarf· Sehr einfaches Wiederherstellen von einzelnen Dateien	<ul style="list-style-type: none">· Fehlerhafte oder von Schadsoftware befallene Dateien werden mitgesichert· Keine verschiedenen Datenstände

Inkrementelles Backup	Ein inkrementelles Backup erstellt zunächst ein vollständiges Backup und sichert dann immer nur die Daten, die sich seit dem letzten Backup verändert haben.	<ul style="list-style-type: none"> · Per se verschiedene Datenstände · kurze Sicherungsdauer · Geringer Speicherplatzbedarf 	<ul style="list-style-type: none"> · Langdauernde Wiederherstellung – alle Sicherungsstände werden benötigt · Häufig abhängig vom Sicherungsprogramm
Differenzielles Backup	Ein differenzielles Backup erstellt zunächst ein vollständiges Backup und sichert dann immer die Daten, die sich seit dem letzten Voll-Backup verändert haben	<ul style="list-style-type: none"> · Per se verschiedene Datenstände · Keine lange Sicherungsdauer · relativ geringer Speicherplatzbedarf 	<ul style="list-style-type: none"> · Etwas aufwändige Wiederherstellung · Häufig abhängig vom Sicherungsprogramm

Vollbackups und inkrementelle Sicherungen lassen sich häufig mit Boardmitteln der Betriebssysteme wiederherstellen, während die Wiederherstellung differenziellen Sicherungen meist die Software nötig ist, mit der die Sicherung erstellt wurde. Die Funktionsweise des Backups, insbesondere der Wiederherstellung soll regelmäßig geprüft werden.

FAQs Datensicherung

Wie häufig müssen welche Daten gesichert werden?

Sicherungen sollten regelmäßig, bestenfalls automatisiert und unter Verwendung einer geeigneten und verlässlichen Software durchgeführt werden.

Die Art und Häufigkeit der Sicherung hängt im Wesentlichen davon ab, aus welchem Grund die Daten gesichert werden, wie häufig sie sich verändern und wie zeitkritisch eine Wiederherstellung ist.

Je häufiger Daten geändert werden, desto kürzer sollten die Sicherungsintervalle festgelegt

werden. Beispielsweise können sich bei Daten der ASV oder Leistungsbewertungen von Schülern nahezu täglich die Bearbeitungszustände ändern. Dem entsprechend erscheint auch eine tägliche Sicherung hier als sinnvoll.

Wie viele Generationen sollen vorgehalten werden?

Unter Generationen versteht man, die Speicherstände zu verschiedenen Sicherungszeitpunkten in der Vergangenheit. So kann es bei der Wiederherstellung von Daten ein bestimmter Zeitpunkt wichtig sein. Um den Speicherplatzbedarf zu optimieren können z. B. könnte man die letzten 10 Speicherzustände erhalten oder man behält eine festgelegte Anzahl an täglichen, wöchentlichen, monatlichen oder gar jährlichen Backups im System. Die Organisation dieses Verfahrens ist eine zentrale Funktionsweise diverser Backup-Lösungen.

Auf welches Speichermedium soll gesichert werden?

Bei dem Sicherungsmedium gibt es eine große Vielfalt, die von mobilen USB-Festplatten, über NAS-Boxen bis hin zu Ende-zu-Ende-verschlüsselten Speicherdiensten im Internet reicht.

Wo werden Backups verortet?

Um äußerliche Gefahren, wie Überspannung, Feuer, Hochwasser etc. vorzubeugen, sollte man die Sicherung zugriffsgeschützt an einem anderen Ort (anderer Brandabschnitt, weiteres schuleigenes Gebäude, SAT oder Cloudspeicherdienst) sichern bzw. aufbewahren.

Wie kann man Datensicherungen vor Ransomware-Angriffen schützen?

Vorbeugende Maßnahme zu den Gefahren, die von einem erfolgreichen Angriff von Ransomware ausgehen, nehmen eine Sonderrolle bei der Datensicherung ein. Der Grund liegt darin, dass bei den herkömmlichen Verfahren, bei denen Daten auf eine Sicherungsmedium geschoben werden (Push-Verfahren), die Sicherungen ebenfalls von der Schadsoftware unbrauchbar gemacht werden. Eine zusätzliche Sicherungsinstanz, das aktiv und regelmäßig eine zusätzliche Sicherung auf ein weiteres Medium zieht (Pull-Verfahren) kann hierbei Abhilfe schaffen. Es muss sichergestellt werden, dass es auf die gesicherten Daten keinerlei

schreibenden Zugriff von außen gibt - zur Administrierung ist eine Zwei-Faktoren-Authentifizierung unabdingbar.

Eine externe Festplatte, die nur zu den regelmäßigen Sicherungen eingesteckt und danach z. B. im Tresor aufbewahrt wird, erfüllt diesen Zweck auf niederschwellige Art.

Wer ist für die Verlässlichkeit des Backups verantwortlich und wer hat Zugriff auf die gesicherten Daten?

Die Verantwortung für die verlässliche Durchführung liegt bei der technischen IT-Administration (Schulaufwandsträger). Ein Zugriff auf die Daten muss nach festgelegten Regeln der Schulleitung erfolgen.

Downloads

[Beispiel eines Backup-Plans](https://www.km.bayern.de/download/4-24-04/Beispiel_Backupplan.pdf)

https://www.km.bayern.de/download/4-24-04/Beispiel_Backupplan.pdf

[Vorlage Backup-Plan](https://www.km.bayern.de/download/4-24-04/Muster_Backupplan.docx)

https://www.km.bayern.de/download/4-24-04/Muster_Backupplan.docx