

LEARNING NUGGET DIGITALE SOUVERÄNITÄT 1. OKTOBER 2026

Nur in der Cloud heisst nicht gesichert

Warum Synchronisation kein Backup ist, wie die 3-2-1-Regel des Bundesamts für Cybersicherheit funktioniert und welche zwei Punkte bei der Datensicherung oft vergessen gehen.

Von Rico Eberle, E-Learning-Experte für Weiterbildung und Gemeinderat in Dübendorf



Video zum Beitrag

Dieses Learning Nugget gibt es als Video mit Transkript (1:02 Min.). QR-Code scannen oder Link öffnen:

ricoeberle.ch/blog/backup-ist-souveraenitaet/

Viele Menschen, Vereine und kleine Organisationen haben ihre Dateien heute in der Cloud. Das fühlt sich sicher an: Die Daten liegen ja beim Anbieter, auf mehreren Geräten, jederzeit erreichbar. Nur ist das noch keine Datensicherung.

Synchronisation ist kein Backup

Ein Synchronisationsdienst hat eine klare Aufgabe: Er hält alle Geräte auf demselben Stand. Genau das wird zum Problem, wenn etwas schiefgeht. Wird eine Datei auf dem Laptop gelöscht oder von Schadsoftware verschlüsselt, kann die Synchronisation diesen Zustand in die Cloud und auf alle anderen Geräte übertragen.



Eine Synchronisation überträgt auch Löschungen und Verschlüsselungen in die Cloud.

Das Bundesamt für Cybersicherheit BACS hält fest, dass Cloud-Dienste nur bedingt vor Angriffen mit Verschlüsselungsschadsoftware, also Ransomware, schützen. Dasselbe gilt für Speichermedien, die dauerhaft angeschlossen sind: Sie können mitverschlüsselt werden.

Zur Einordnung: Viele Dienste bieten eine Versionierung, mit der sich ältere Stände zurückholen lassen. Darum heisst es im Video «kann» und nicht «wird». Eine eigenständige Sicherung ersetzt das aber nicht.

Die 3-2-1-Regel

Das BACS empfiehlt eine einfache Faustregel:

- **3 Kopien** deiner Daten: das Original und zwei Sicherungskopien.
- **2 unterschiedliche Speichermedien**, zum Beispiel eine externe Festplatte und eine Cloud.

- **1 Kopie** ausserhalb des eigenen Geräts an einem externen Ort.



Die 3-2-1-Regel: drei Kopien, zwei Speichermedien, eine Kopie ausser Haus.

Für diese externe Kopie empfiehlt das BACS, sie offline auf einem externen Medium aufzubewahren und das Medium nach dem Backup wieder zu trennen. Was nicht angeschlossen ist, kann eine Schadsoftware nicht erreichen.

Zwei Punkte, die oft vergessen gehen

Die Wiederherstellung üben. Das BACS rät ausdrücklich, das Einspielen von Sicherungskopien zu üben, bevor man im Ernstfall darauf angewiesen ist. Erst beim Zurückholen zeigt sich, ob die Sicherung vollständig ist, ob du das Passwort noch kennst und wie lange es dauert.

Oft vergessen

1 Wiederherstellung üben, bevor der Ernstfall kommt

Ein ungetestetes Backup ist eine Hoffnung.

2 In offenen Formaten sichern, lesbar auch ohne Anbieter



Zwei Punkte, die bei Backups oft fehlen: die Wiederherstellung üben und offene Formate.

In offenen Formaten sichern. Das ist meine Empfehlung, keine Vorgabe des BACS: Eine Sicherung nützt wenig, wenn sich die Dateien nur mit der Software eines bestimmten Anbieters öffnen lassen. Offene Formate machen dich unabhängiger, falls du den Anbieter wechselst oder es ihn nicht mehr gibt.

Mein Vorschlag: eine Wiederherstellungsprobe

Plane in den nächsten Tagen eine kleine Probe ein:

1. Wähle eine Datei, die dir wichtig ist, und einen Ordner, den du oft brauchst.
2. Hol beide aus deiner Sicherung zurück, und zwar an einen neuen Ort, damit du nichts überschreibst.
3. Öffne die Dateien auf einem anderen Gerät oder mit einem anderen Programm.
4. Notiere, was gefehlt hat oder unklar war, und wann du die Probe wiederholst.

Für Vereine und Teams lohnt sich eine zusätzliche Frage: Wer ausser dir weiss, wo die Sicherung liegt und wie man sie einspielt?

Meine Sicht

Ein Backup, das nie getestet wurde, ist eine Hoffnung, keine Sicherung. Und Souveränität beginnt für mich genau dort, wo du deine Daten selbst zurückholen kannst, ohne auf einen Anbieter angewiesen zu sein.

Und bei dir?

Wann hast du dein Backup zuletzt getestet?

Häufige Fragen

Ist die Cloud ein Backup?

Nicht automatisch. Ein Synchronisationsdienst hält alle Geräte auf demselben Stand und kann so auch eine gelöschte oder verschlüsselte Datei auf alle Geräte übertragen. Das Bundesamt für Cybersicherheit BACS hält fest, dass Cloud-Dienste nur bedingt vor Ransomware schützen.

Was ist die 3-2-1-Regel?

Eine Faustregel des BACS für die Datensicherung: drei Kopien der Daten, auf zwei unterschiedlichen Speichermedien, davon eine an einem externen Ort. Für die externe Kopie empfiehlt das BACS, sie offline aufzubewahren und das Medium nach dem Backup wieder zu trennen.

Wie prüfe ich, ob mein Backup funktioniert?

Indem du die Wiederherstellung übst, wie es das BACS empfiehlt. Erst beim Zurückholen zeigt sich, ob die Sicherung vollständig ist, ob du das Passwort noch kennst und wie lange es dauert.

Quellen

1. Bundesamt für Cybersicherheit BACS: Datensicherung
<https://www.bacs.admin.ch/de/datensicherung>



ÜBER DEN AUTOR

Rico Eberle

Rico Eberle ist E-Learning-Experte, Betriebsökonom FH und Gemeinderat in Dübendorf. Er präsidiert den Stiftungsrat der Stiftung Weiterbildungskurse Dübendorf (WBK). In den Learning Nuggets erklärt er Forschung zu Lernen, KI und digitaler Souveränität kurz und mit Quellen.

Kontakt: ricoeberle.ch · LinkedIn: [linkedin.com/in/rico-eberle](https://www.linkedin.com/in/rico-eberle)

LIZENZ

Text, Transkript und Video von Rico Eberle stehen unter der Lizenz CC BY 4.0 (ausgenommen Musik und Soundeffekte des Videos). Du darfst die Inhalte teilen und bearbeiten, auch im Unterricht, wenn du die Quelle nennst.
creativecommons.org/licenses/by/4.0/deed.de

ZITIERVORSCHLAG

«Nur in der Cloud heisst nicht gesichert», Rico Eberle, ricoeberle.ch, 2026, <https://ricoeberle.ch/blog/backup-ist-souveraenitaet/>, CC BY 4.0