

Krywerk – Bedienungsanleitung

Diese Anleitung richtet sich an alle, die mit Krywerk arbeiten – Lehrkräfte, Verwaltung und alle, die vertrauliche Dateien in OneDrive oder einem anderen Speicher ablegen. Technikwissen ist nicht nötig. Wer Team-Ordner für andere verwaltet, findet in Kapitel 5 zusätzliche Hinweise.

Die Anleitung beschreibt Krywerk unter Windows. Unter macOS und Linux ist alles gleich, nur heißt der Infobereich unter macOS Menüleiste, und Laufwerke erscheinen im Finder bzw. Dateimanager unter `~/Krywerk` statt mit eigenem Buchstaben im Explorer. Das Kontextmenü heißt unter macOS „Schnellaktionen“, unter Linux erscheint es in Dolphin unter „Aktionen“ und in Nautilus unter „Skripte“.

Zum Ausdrucken: Bedienungsanleitung als PDF.

Inhalt

1. Was ist Krywerk?
2. Installieren und einrichten
3. Persönlicher Tresor
4. Team-Ordner nutzen
5. Team-Ordner verwalten (für Verantwortliche)
6. Umstieg von Boxcryptor
7. Häufige Fragen und Probleme
8. Begriffe

Das Wichtigste in Kürze

- Krywerk zeigt verschlüsselte Ordner als **Laufwerk** an. Was Sie dort ablegen, wird automatisch verschlüsselt, bevor es in OneDrive & Co. landet.
- Es gibt drei Arten von Laufwerken: **persönliche Tresore** (eigenes Passwort), **Team-Ordner** (Zugriff über Ihr Organisationskonto, ohne gemeinsames Passwort) und **Boxcryptor (alt)** für den Umstieg.
- Drei Dinge müssen Sie sicher aufbewahren, je nachdem, was Sie nutzen: das **Tresor-Passwort**, Ihren **Freischaltcode** und – wenn Sie Team-Ordner verwalten – deren **Wiederherstellungsschlüssel**. Krywerk kann keines davon wiederherstellen.

1. Was ist Krywerk?

Krywerk verschlüsselt Ordner und zeigt sie entschlüsselt als Laufwerk an – unter Windows mit eigenem Buchstaben im Explorer, zum Beispiel **Z:**. Sie arbeiten darin wie in jedem anderen Ordner: Dateien öffnen, speichern, kopieren, umbenennen. Im Hintergrund legt Krywerk alles verschlüsselt in einem normalen Ordner ab.

Dieser Ordner kann überall liegen, wo Ordner synchronisiert oder geteilt werden: in **OneDrive**, Google Drive, Dropbox, Nextcloud oder iCloud Drive, auf einem **Netzlaufwerk** (SMB, NFS) oder auf einem **USB-Stick**. Der Speicheranbieter sieht nur verschlüsselte Daten.

Was bleibt sichtbar, was nicht?

	Für den Speicheranbieter sichtbar?
Inhalt der Dateien	Nein
Datei- und Ordernamen	Nein (bei Boxcryptor (alt) nur, wenn die Namensverschlüsselung an ist)
Wie viele Dateien es gibt und wie groß sie ungefähr sind	Ja
Wann Dateien geändert wurden	Ja

Drei Arten von Laufwerken

	Persönlicher Tresor	Team-Ordner	Boxcryptor (alt)
Wofür?	Eigene vertrauliche Dateien	Zusammenarbeit (Fachgruppe, Gremium, Verwaltung)	Vorhandene Boxcryptor-Daten weiter nutzen
Wie entsperrt?	Mit dem Tresor-Passwort	Mit Ihrem Organisationskonto (z. B. Microsoft 365), ohne gemeinsames Passwort	Mit Boxcryptor-Schlüsseldatei und -Passwort
Wer hat Zugriff?	Wer das Passwort kennt	Nur Personen und Gruppen, denen Zugriff gewährt wurde	Wer Schlüsseldatei und Passwort hat
Auf dem Handy?	Ja, mit der Cryptomator-App	Noch nicht	Nein
Kennzeichnung in Krywerk	„Persönlich (Passwort)“	„Team“	„Boxcryptor (alt)“

Persönliche Tresore verwenden das offene Cryptomator-Format. Sie lassen sich deshalb auch mit den Cryptomator-Apps für Android, iOS und Linux öffnen.

Team-Ordner brauchen einen Schlüsselservers Ihrer Organisation – den **Krywerk Server** oder einen Cryptomator Hub. Der Server verwaltet, wer einen Team-Ordner öffnen darf; die Dateien selbst kann er nicht lesen. Die Adresse erhalten Sie von Ihrer IT-Administration.

Boxcryptor (alt) ist nur für den Übergang gedacht. Das Verfahren ist älter und schützt nicht gegen gezielte Veränderung der verschlüsselten Dateien. Stellen Sie solche Ordner deshalb nach und nach um (Kapitel 6).

Wie Krywerk aussieht

- **Übersicht:** Oben stehen Statusanzeigen, zum Beispiel „Organisationskonto: Ihr Name“. Darunter folgen Hinweise, wenn etwas ansteht, und die Liste „**Meine Laufwerke**“ mit allen Laufwerken und Team-Ordnern.
- **Einstellungen:** über „ **Einstellungen**“ oben rechts oder per Rechtsklick auf das Krywerk-Symbol im Infobereich. Dort gibt es die Bereiche *Allgemein*, *Organisationskonto*, *Boxcryptor (alt)* (nur wenn Sie Boxcryptor-Ordner nutzen) und *Über Krywerk*.
- **Infobereich:** Krywerk läuft im Hintergrund weiter, wenn Sie das Fenster schließen. Das Symbol finden Sie unten rechts in der Taskleiste, eventuell hinter dem Pfeil „^“. **Beenden** über einen Rechtsklick auf das Symbol – dabei werden alle Laufwerke ausgehängt.

2. Installieren und einrichten

Voraussetzungen

Krywerk gibt es für Windows, macOS und Linux. Wenn Ihre IT Krywerk verteilt, ist das meiste schon erledigt – fragen Sie dort nach. Die Pakete zum Herunterladen finden Sie unter <https://krywerk.eu/download/>.

Windows 10 oder 11:

1. **Krywerk** installieren: `Krywerk_..._x64-setup.exe` ausführen und die Rückfrage nach Administratorrechten bestätigen. Der Installer richtet alles Nötige mit ein – auch **WinFsp**, die Komponente, mit der Krywerk Laufwerke bereitstellt, und unter Windows 10 bei Bedarf *WebView2* für das Fenster.
2. Meldet Windows „Der Computer wurde durch Windows geschützt“, liegt das daran, dass die Vorabversion noch nicht signiert ist: **„Weitere Informationen“** › **„Trotzdem ausführen“**.

macOS:

1. **FUSE-T** installieren (<https://www.fuse-t.org/>), z. B. mit `brew install macos-fuse-t/homebrew-cask/fuse-t`.
2. **Krywerk.app** aus dem heruntergeladenen ZIP in den Programme-Ordner ziehen.
3. Beim ersten Öffnen meldet macOS, dass die App nicht überprüft werden kann (die Vorabversion ist noch nicht notariert): **Rechtsklick auf Krywerk.app** › **„Öffnen“** › **„Öffnen“**. Unter neueren macOS-Versionen stattdessen *Systemeinstellungen* › *Datenschutz & Sicherheit* › *„Trotzdem öffnen“*.

Linux:

1. **Debian, Ubuntu, Linux Mint:** das Paket `Krywerk_..._amd64.deb` installieren, z. B. per Doppelklick oder mit `sudo apt install ./Krywerk_..._amd64.deb`. Benötigte Komponenten (FUSE, WebKitGTK) kommen automatisch mit.
2. **Andere Distributionen:** die Datei `Krywerk_..._amd64.AppImage` ausführbar machen und starten. Das Paket `fuse3` der Distribution muss installiert sein.
3. Für **„Passwort merken“** braucht Ihre Sitzung einen Schlüsselbund (KDE: KWallet, GNOME: Schlüsselbund – meist vorhanden). Unter GNOME erscheint das Krywerk-Symbol oben in der Leiste nur mit der Erweiterung *AppIndicator and KStatusNotifierItem Support*.

Laufwerke erscheinen unter Windows mit eigenem Laufwerksbuchstaben, unter macOS und Linux im Ordner `Krywerk` Ihres Benutzerordners (z. B. `~/Krywerk/Vertraulich`) und in der Seitenleiste des Finders bzw. Dateimanagers.

Erster Start

Nach dem Start erscheint das Krywerk-Fenster und das Krywerk-Symbol im Infobereich (unten rechts in der Taskleiste, eventuell hinter dem Pfeil „^“). Die Liste „Meine Laufwerke“ ist zunächst leer.

Wie es weitergeht, hängt davon ab, was Sie nutzen möchten:

- eigene vertrauliche Dateien → [Kapitel 3: Persönlicher Tresor](#)
- Team-Ordner Ihrer Organisation → [Kapitel 4: Team-Ordner nutzen](#)
- vorhandene Boxcryptor-Daten → [Kapitel 6: Umstieg von Boxcryptor](#)

Automatisch starten

Unter  **Einstellungen** › **Allgemein** können Sie „**Beim Anmelden am Computer automatisch starten**“ einschalten. Krywerk startet dann ohne Fenster, nur mit dem Symbol im Infobereich. Laufwerke, bei denen „Automatisch einhängen“ eingeschaltet und das Passwort gemerkt ist, stehen gleich zur Verfügung. Team-Ordner öffnen Sie nach der Anmeldung beim Organisationskonto.

Fenster schließen und Krywerk beenden

- **Fenster schließen oder minimieren:** Krywerk läuft im Infobereich weiter, Ihre Laufwerke bleiben verfügbar. Ein Klick auf das Symbol holt das Fenster zurück.
- **Beenden:** Rechtsklick auf das Symbol › **Beenden**. Dabei werden alle Laufwerke ausgehängt. Speichern Sie vorher offene Dateien.

Zwischenspeicher (nur bei Problemen ändern)

Unter  **Einstellungen** › **Allgemein** › **Erweitert** ist „**Zwischenspeicher verwenden (empfohlen)**“ eingeschaltet. Er macht die Laufwerke schneller. Schalten Sie ihn nur aus, wenn Änderungen, die OneDrive oder ein anderer Speicher von anderen Geräten holt, im Laufwerk nicht oder erst verspätet erscheinen. Die Änderung gilt beim nächsten Einhängen.

3. Persönlicher Tresor

Ein persönlicher Tresor ist ein verschlüsselter Ordner mit **eigenem Passwort**. Er eignet sich für Ihre eigenen vertraulichen Dateien – zum Beispiel Notenlisten, Gutachten oder Personalunterlagen.

Tresor anlegen

1. Auf der Übersicht bei „Meine Laufwerke“ auf „**+ Hinzufügen**“ klicken. Ist ein Organisationskonto verbunden, erscheint eine Auswahl – dort „**Persönlichen Tresor oder vorhandenen Ordner ...**“ wählen.
2. Als Format „**Modern (empfohlen)**“ lassen.
3. Bei „**Ordner für den Tresor**“ auf „**Durchsuchen ...**“ klicken und einen **leeren Ordner** wählen, zum Beispiel einen neuen Ordner `Vertraulich` in Ihrem OneDrive. Krywerk legt den Tresor darin an.
4. Ein **Tresor-Passwort** mit mindestens 8 Zeichen eingeben und wiederholen.
5. Optional „**Passwort merken**“ ankreuzen. Das Passwort wird dann mit Ihrem Windows-Benutzerkonto geschützt auf diesem Computer gespeichert, und Sie müssen es beim Einhängen nicht eingeben.
6. Optional einen **Namen** (erscheint im Explorer) und einen **Laufwerksbuchstaben** wählen. „Automatisch“ nimmt den nächsten freien Buchstaben ab `Z` : .
7. „**Speichern**“ klicken.

Wichtig: Ohne das Tresor-Passwort sind die Daten nicht wiederherstellbar – auch nicht durch die IT oder durch Krywerk. Bewahren Sie es sicher auf, zum Beispiel in einem Passwortmanager.

Vorhandenen Tresor einbinden

Haben Sie schon einen Tresor – zum Beispiel mit der Cryptomator-App angelegt oder auf einem anderen Computer mit Krywerk –, gehen Sie genauso vor, wählen in Schritt 3 aber den Ordner des Tresors (den Ordner, in dem die Datei `vault.cryptomator` liegt) und geben dessen Passwort ein.

Einhängen und arbeiten

- **Einhängen:** In der Zeile des Tresors das Passwort eingeben (falls nicht gemerkt) und auf „**Einhängen**“ klicken. Danach steht dort „Eingehängt als Z:“.
- **Öffnen:** Klick auf „**Öffnen**“ zeigt das Laufwerk im Explorer. Sie können es auch direkt im Explorer unter „Dieser PC“ öffnen.
- **Aushängen:** Klick auf „**Aushängen**“, wenn Sie fertig sind. Beim Beenden von Krywerk werden alle Laufwerke automatisch ausgehängt.

Mit „**Automatisch einhängen**“ (unter „**Bearbeiten**“) hängt Krywerk den Tresor beim Start selbst ein, sofern das Passwort gemerkt ist.

Tresor bearbeiten oder entfernen

Unter „**Bearbeiten**“ (nur bei ausgehängtem Tresor) ändern Sie Namen, Laufwerksbuchstaben, „Automatisch einhängen“ und „Nur lesend“. Außerdem gibt es dort:

- „**Gemerkttes Tresor-Passwort löschen**“ – Krywerk fragt beim nächsten Einhängen wieder nach dem Passwort.
- „**Entfernen**“ – nimmt den Tresor aus der Liste von Krywerk und vergisst das gemerkte Passwort. **Die verschlüsselten Dateien bleiben erhalten**; Sie können den Tresor jederzeit wieder einbinden.

Auf dem Handy öffnen

Persönliche Tresore verwenden das Cryptomator-Format. So öffnen Sie sie unterwegs:

1. Die **Cryptomator-App** für Android oder iOS installieren (im jeweiligen App-Store).
2. In der App einen **vorhandenen Tresor hinzufügen** und OneDrive (bzw. Ihren Speicher) verbinden.
3. Den Ordner des Tresors wählen (darin liegt `vault.cryptomator`) und das Tresor-Passwort eingeben.

Änderungen auf dem Handy erscheinen auf dem Computer, sobald OneDrive sie synchronisiert hat – und umgekehrt.

4. Team-Ordner nutzen

Ein Team-Ordner ist ein verschlüsselter Ordner für mehrere Personen – zum Beispiel für eine Fachgruppe, ein Gremium oder die Verwaltung. Es gibt **kein gemeinsames Passwort**: Wer Zugriff hat, öffnet den Team-Ordner mit dem eigenen Organisationskonto (zum Beispiel dem Microsoft-365-Konto der Schule). Den Schlüssel verwaltet der Schlüsselservers Ihrer Organisation; die Dateien selbst kann der Server nicht lesen.

Einmalig: Organisationskonto verbinden

1.  **Einstellungen > Organisationskonto** öffnen.
2. Bei „**Adresse des Schlüsselservers**“ die Adresse eintragen, die Sie von Ihrer IT bekommen haben, zum Beispiel `https://schluessel.schule.example`.
3. „**Mit Organisationskonto verbinden**“ klicken.
4. Krywerk fragt einmalig nach: „**Schlüsselserver bestätigen**“. Bestätigen Sie mit „**Vertrauen und fortfahren**“, wenn die Adresse die ist, die Ihre Organisation genannt hat. Die zweite angezeigte Adresse gehört zum Anmeldedienst (zum Beispiel Microsoft).
5. Krywerk öffnet **einen neuen Tab in Ihrem Standardbrowser** mit der Anmeldeseite. Melden Sie sich dort mit Ihrem Organisationskonto an. Danach zeigt der Browser „Anmeldung erfolgreich“; den Tab können Sie schließen.
6. Oben im Krywerk-Fenster steht jetzt grün „**Organisationskonto: Ihr Name**“.

Beim ersten Mal: Konto einrichten und Freischaltcode aufbewahren

Nutzen Sie Team-Ordner zum ersten Mal, zeigt Krywerk „**Konto einrichten ...**“. Klicken Sie darauf. Krywerk zeigt dann **Ihren Freischaltcode** an – **nur dieses eine Mal**.

- Bewahren Sie den Freischaltcode sicher auf: „**Kopieren**“ in einen Passwortmanager oder „**Als Datei speichern ...**“ an einem sicheren Ort (nicht im Team-Ordner selbst).
- Kreuzen Sie „**Ich habe den Freischaltcode sicher aufbewahrt.**“ an und klicken Sie auf „**Fertig**“.

Diesen Computer hat Krywerk dabei bereits freigeschaltet. Den Freischaltcode brauchen Sie für **jeden weiteren Computer** – ohne ihn können Sie dort keine Team-Ordner öffnen.

Weiteren Computer freischalten

Auf einem weiteren Computer verbinden Sie das Organisationskonto wie oben. Krywerk zeigt dann „**Gerät freischalten ...**“ (oder fragt beim ersten Öffnen eines Team-Ordners danach). Geben Sie Ihren Freischaltcode ein – Leerzeichen, Bindestriche und Groß-/Kleinschreibung spielen keine Rolle.

Anmelden nach einem Neustart

Krywerk merkt sich die Anmeldung, bis Sie Krywerk beenden. Nach einem Neustart steht oben gelb **„Organisationskonto: nicht angemeldet – Anmelden“**. Ein Klick darauf (oder auf **„Jetzt anmelden“**) öffnet wieder die Anmeldung im Browser.

Einen geteilten Team-Ordner öffnen

Damit Sie einen Team-Ordner öffnen können, braucht es **zwei Freigaben**:

1. **Die Dateien:** Der Ordner muss auf Ihrem Computer ankommen – meist teilt ihn die verantwortliche Person in **OneDrive** mit Ihnen (in OneDrive: „Geteilt“ > Ordner > „Verknüpfung zu Meine Dateien hinzufügen“, damit er synchronisiert wird).
2. **Der Schlüssel:** Die verantwortliche Person nimmt Sie in Krywerk auf und gewährt Ihnen Zugriff.

Sobald beides da ist, erscheint der Team-Ordner in „Meine Laufwerke“ mit der Kennzeichnung „Team“. Krywerk sucht den Ordner selbst in OneDrive und anderen Cloud-Ordnern.

- **„Öffnen“** hängt den Team-Ordner als Laufwerk ein. **„Im Explorer zeigen“** öffnet ihn, **„Schließen“** hängt ihn aus.
- Steht dort **„Ordner auf diesem Gerät nicht gefunden“**, ist der Ordner (noch) nicht synchronisiert. Prüfen Sie die OneDrive-Freigabe – oder wählen Sie den Ordner mit **„Ordner suchen ...“** selbst aus.
- Meldet Krywerk beim Öffnen, dass der Zugriff noch nicht gewährt ist, bitten Sie die verantwortliche Person, in Krywerk bei diesem Team-Ordner auf **„Verwalten“ > „Zugriff gewähren“** zu klicken.

Selbst einen Team-Ordner anlegen und teilen

1. Auf der Übersicht **„+ Hinzufügen“ > „Team-Ordner anlegen und teilen ...“** wählen.
2. **Wo?** Einen leeren Ordner wählen – oder einen Ordner, in dem Krywerk einen neuen Unterordner anlegt (Feld „Neuer Unterordner“). Für die Zusammenarbeit eignet sich ein Ordner in OneDrive.
3. **Name des Team-Ordners** – so sehen ihn die anderen in Krywerk. Leer = Name des Ordners.
4. **Wer?** Personen oder Gruppen suchen (Name, E-Mail oder Gruppe) und hinzufügen:
 - **„Hinzufügen“** – als **Mitglied**: kann den Team-Ordner öffnen, Dateien lesen und bearbeiten.
 - **„Als ‚verwaltet‘ hinzufügen“** – kann zusätzlich Personen aufnehmen und entfernen, Zugriff gewähren, den Wiederherstellungsschlüssel anzeigen, den Notfallzugriff einrichten, archivieren und den Schlüssel erneuern.

Beim Krywerk Server erscheinen Personen in der Suche erst, nachdem sie sich einmal mit Krywerk (oder Cryptomator) angemeldet haben – bitten Sie neue Kolleginnen und Kollegen also zuerst, ihr Organisationskonto zu verbinden.

5. „**Team-Ordner anlegen**“ klicken.

6. Krywerk zeigt den **Wiederherstellungsschlüssel** an – siehe [Kapitel 5](#). Drucken oder speichern Sie ihn, kreuzen Sie „Ich habe den Wiederherstellungsschlüssel sicher aufbewahrt.“ an und klicken Sie auf „Fertig“.

7. **Teilen Sie den Ordner zusätzlich in OneDrive** mit denselben Personen (Rechtsklick › Teilen). Krywerk regelt nur, wer die Dateien entschlüsseln kann – verteilt werden sie weiter von OneDrive.

Empfehlung: Tragen Sie eine zweite Person als „verwaltet“ ein und richten Sie den Notfallzugriff ein. Fallen Sie aus, kann sonst niemand mehr Personen aufnehmen oder Zugriff gewähren.

Zugriff gewähren

Wer neu in einen Team-Ordner aufgenommen wurde, bekommt den Schlüssel erst, wenn eine verwaltende Person den Zugriff **gewährt**. Das geht nur von deren Computer aus, weil Krywerk dabei den Schlüssel für die neue Person verschlüsselt.

Krywerk weist Sie darauf hin:

- auf der Übersicht: „1 Person wartet auf Zugriff ...“ und beim Team-Ordner „1 wartet auf Zugriff“,
- im Infobereich: Tooltip des Symbols und Eintrag „Freigaben: ...“ im Rechtsklick-Menü.

Klicken Sie beim Team-Ordner auf „**Verwalten**“, kreuzen Sie unter „Warten auf Zugriff“ die Personen an und klicken Sie auf „**Zugriff gewähren**“. Personen, deren Identität noch nicht bestätigt ist („**nicht bestätigt** ▲“), prüfen Sie vorher mit „**Identität prüfen ...**“ – siehe [Kapitel 5](#).

Ihr Fingerabdruck

Bevor jemand Ihnen Zugriff gewährt, kann er prüfen, ob der Schlüsselservers ihm wirklich **Ihren** Schlüssel liefert. Ihren Fingerabdruck finden Sie unter **Einstellungen › Organisationskonto › „Fingerabdruck anzeigen“** (acht Blöcke aus Ziffern und den Buchstaben A–F). Beim ersten Mal auf einem Computer fragt Krywerk einmal nach Ihrem Freischaltcode. Lesen Sie den Fingerabdruck der fragenden Person **am Telefon oder persönlich** vor – nicht per E-Mail oder Chat, denn die könnten über dieselben Wege laufen wie der Schlüsselservers.

5. Team-Ordner verwalten (für Verantwortliche)

Dieses Kapitel ist für Personen, die einen Team-Ordner **verwalten** – in der Liste steht dann „verwaltet von Ihnen“, und es gibt den Knopf „**Verwalten**“.

Personen und Gruppen

Unter „**Verwalten**“ sehen Sie alle Mitglieder mit ihrer Rolle.

- **Aufnehmen:** Bei „Hinzufügen“ Name, E-Mail oder Gruppe suchen, dann „**Hinzufügen**“ (Mitglied) oder „**Als ‚verwaltet‘ hinzufügen**“. Danach unter „Ausstehende Freigaben“ die Personen ankreuzen und auf „**Zugriff gewähren**“ klicken – am besten erst, nachdem Sie ihre Identität geprüft haben (siehe unten).
- **Rolle ändern:** „**Zu ‚verwaltet‘ machen**“ bzw. „**Zu ‚Mitglied‘ machen**“.
- **Entfernen:** „**Entfernen**“ bei der Person. Das wirkt für künftiges Öffnen. Wer den Team-Ordner schon geöffnet hatte, kann bereits heruntergeladene Dateien und eine Kopie des Schlüssels behalten haben. Bei vertraulichen Inhalten deshalb danach den **Schlüssel erneuern** (siehe unten).

Gruppen kommen aus Ihrem Organisationskonto (zum Beispiel Microsoft-365-Gruppen). Neue Gruppenmitglieder bekommen Zugriff, sobald Sie ihn gewährt haben.

Identität prüfen

Beim Gewähren verschlüsselt Krywerk den Schlüssel des Team-Ordners an den Schlüssel, den der Schlüsselsever für die Person liefert. Ein manipulierter Schlüsselsever könnte dabei einen fremden Schlüssel unterschieben. Mit „**Identität prüfen ...**“ stellen Sie sicher, dass der Schlüssel wirklich der Person gehört.

Unter „Warten auf Zugriff“ und bei den Mitgliedern steht bei jeder Person:

- „**bestätigt ✓**“ – Sie haben die Identität geprüft (oder eine Person, deren Identität Sie geprüft haben, hat sie geprüft). Die Person ist zum Gewähren vorausgewählt.
- „**nicht bestätigt Δ**“ – noch nicht geprüft, oder die Person hat neue Schlüssel bekommen (zum Beispiel nach einem zurückgesetzten Konto). Die Person ist **nicht** vorausgewählt.

So prüfen Sie eine Identität:

1. Rufen Sie die Person an oder sprechen Sie sie persönlich an – **nicht per E-Mail oder Chat**.
2. Bitten Sie sie, in Krywerk  **Einstellungen** > **Organisationskonto** > „**Fingerabdruck anzeigen**“ zu öffnen und Ihnen den Fingerabdruck vorzulesen.
3. Klicken Sie bei der Person auf „**Identität prüfen ...**“ und tippen Sie die ersten Zeichen ein (wie viele, steht im Dialog; mindestens 8). Leerzeichen und Groß-/Kleinschreibung spielen keine Rolle.

4. Beim allerersten Prüfen auf einem Computer fragt Krywerk zusätzlich nach **Ihrem** Freischaltcode. Danach geht es auf diesem Computer ohne.
5. **„Identität bestätigen“**. Stimmen die Zeichen nicht überein, bestätigt Krywerk nichts – lassen Sie sich den Fingerabdruck noch einmal vorlesen. Bleibt es dabei, gewähren Sie keinen Zugriff und informieren Sie die IT-Administration.

Sie können eine nicht bestätigte Person trotzdem ankreuzen. Krywerk zeigt dann eine Warnung und fragt vor dem Gewähren noch einmal nach. Das ist nur sinnvoll, wenn Sie dem Schlüsselservers vertrauen.

Auch beim **Notfallzugriff** zeigt Krywerk an, wenn die Identität von Gremiumsmitgliedern oder der beantragenden Person nicht bestätigt ist. Krywerk blockiert dort nichts. Prüfen Sie die Identität und richten Sie den Notfallzugriff im Zweifel neu ein.

Wiederherstellungsschlüssel

Jeder Team-Ordner hat einen **Wiederherstellungsschlüssel** (28 Vierergruppen aus Buchstaben und Ziffern). Damit lässt sich der Team-Ordner **auch ohne Schlüsselservers** öffnen – zum Beispiel, wenn der Server ausfällt oder abgeschaltet wird. Wer ihn hat, kann alle Dateien des Team-Ordners lesen.

- Krywerk zeigt ihn beim Anlegen einmal an. Später erneut: **„Verwalten“ > „Wiederherstellungsschlüssel anzeigen ...“**.
- Aufbewahren: **„Drucken ...“** und versiegelt bei der Schulleitung hinterlegen, oder **„Als Datei speichern ...“** in einem sicheren Passwortmanager. Nicht im Team-Ordner selbst und nicht unverschlüsselt in OneDrive.
- **Öffnen ohne Server**: In der Zeile des Team-Ordners **„Ohne Server öffnen ...“** wählen und den Schlüssel eingeben. Krywerk merkt sich den Schlüssel nicht.

Notfallzugriff (Vier-Augen-Prinzip)

Fallen alle verwaltenden Personen aus, kann sonst niemand mehr Personen aufnehmen oder Zugriff gewähren. Dafür gibt es den Notfallzugriff: Ein **Notfallgremium** (zum Beispiel Schulleitung und Stellvertretung) kann gemeinsam einer Person die Rolle „verwaltet“ geben – aber nur, wenn genug Personen zustimmen.

Einrichten (verwaltende Person): **„Verwalten“ > Notfallzugriff > „Einrichten ...“**

1. Personen fürs Gremium wählen (nur Personen mit eingerichtetem Organisationskonto, keine Gruppen).
2. Festlegen, **wie viele zustimmen müssen** – mindestens 2. Eine Person allein bekommt nie Zugriff.
3. **„Notfallzugriff einrichten“**.

Im Notfall (Mitglied des Gremiums):

1. **⚙ Einstellungen > Organisationskonto > Notfallzugriff** öffnen.

2. Beim Team-Ordner „**Notfallantrag stellen ...**“ wählen und eine Begründung angeben. Die eigene Stimme zählt nicht.
3. Die anderen Gremiumsmitglieder sehen auf ihrer Übersicht den Hinweis „Ein Notfallantrag wartet auf Sie“ mit „**Prüfen**“ und stimmen mit „**Zustimmen ...**“ zu. **Stimmen Sie nur zu, wenn Sie den Antrag geprüft haben** – zum Beispiel persönlich oder telefonisch.
4. Sind genug Zustimmungen da, klickt die beantragende Person auf „**Abschließen**“ und verwaltet danach den Team-Ordner. Ein offener Antrag lässt sich mit „**Abbrechen ...**“ zurückziehen.

Schlüssel erneuern (nach einem Austritt)

Verlässt jemand die Gruppe, sollte der Team-Ordner einen **neuen Schlüssel** bekommen. Wer ausgeschlossen wurde, kann den neuen Inhalt dann auch mit einer alten Kopie des Schlüssels nicht lesen.

Vorher: Bitten Sie alle Mitglieder, den Team-Ordner zu **schließen**. Änderungen, die während des Vorgangs gemacht werden, gehen verloren. Auf Ihrem eigenen Computer schließt Krywerk den Ordner selbst.

1. „**Verwalten**“ > „**Schlüssel erneuern ...**“.
2. Unter „**Nicht übernehmen**“ die ausgetretenen Personen ankreuzen.
3. Optional „**Alte verschlüsselte Daten behalten**“ – sie bleiben dann neben dem Ordner, mit dem alten Schlüssel lesbar.
4. „**Schlüssel erneuern**“ klicken. Krywerk legt einen neuen Team-Ordner mit neuem Schlüssel an, übernimmt die Mitglieder, verschlüsselt den Inhalt neu und tauscht ihn **im selben Ordner** aus. Die OneDrive-Freigabe bleibt bestehen. Der alte Team-Ordner wird archiviert.
5. Krywerk zeigt einen **neuen Wiederherstellungsschlüssel** an. Der alte öffnet nur noch den archivierten Stand.

Danach synchronisiert OneDrive den gesamten Inhalt neu. Ältere Kopien (Papierkorb, Versionsverlauf von OneDrive, Kopien ausgetretener Personen) bleiben mit dem alten Schlüssel lesbar. Wird der Vorgang unterbrochen, setzt „**Schlüssel erneuern fortsetzen ...**“ ihn später fort.

Archivieren

„**Verwalten**“ > „**Archivieren ...**“ sperrt den Team-Ordner: Niemand kann ihn mehr öffnen, die Dateien bleiben erhalten. „**Reaktivieren**“ hebt das wieder auf.

6. Umstieg von Boxcryptor

Boxcryptor wird nicht mehr weiterentwickelt. Krywerk öffnet vorhandene Boxcryptor-Ordner weiter und stellt sie **Schritt für Schritt** auf das moderne Format um – in einen persönlichen Tresor oder in einen Team-Ordner. Sie können währenddessen normal weiterarbeiten.

Vorher: Schlüsseldatei sichern

Für Boxcryptor-Ordner brauchen Sie Ihre **Boxcryptor-Schlüsseldatei** (Endung `.bckey`, aus Boxcryptor exportiert) und Ihr **Boxcryptor-Passwort**. Ohne beides sind die Daten nicht lesbar.

- Legen Sie eine **Sicherung der Schlüsseldatei** getrennt ab, zum Beispiel auf einem USB-Stick – bis alle Ordner umgestellt sind. In Krywerk geht das unter **Einstellungen** > **Boxcryptor (alt)** > „**Schlüsseldatei sichern ...**“ (bei entsperrtem Konto).
- Üben Sie die Umstellung zuerst mit der **Kopie eines kleinen Ordners**.

Boxcryptor-Ordner einbinden

1. „**+ Hinzufügen**“ (ggf. > „**Persönlichen Tresor oder vorhandenen Ordner ...**“) wählen.
2. Als Format „**Klassisch (Übergang)**“ wählen.
3. Den **verschlüsselten Boxcryptor-Ordner** auswählen, Namen und Laufwerksbuchstaben festlegen, „**Speichern**“.
4. Auf der Übersicht erscheint die Karte „**Boxcryptor-Konto entsperren**“. Fehlt noch die Schlüsseldatei, zuerst „**Schlüsseldatei wählen ...**“.
5. Passwort eingeben, optional „**Passwort merken**“, dann „**Entsperren**“. Oben steht jetzt grün „Boxcryptor-Konto entsperrt“.
6. In der Zeile des Laufwerks „**Einhängen**“. Es trägt die Kennzeichnung „Boxcryptor (alt)“.

Unter **Einstellungen** > **Boxcryptor (alt)** finden Sie außerdem „Passwort ändern ...“, „Gespeichertes Passwort löschen“, „Sperren“ und zwei Einstellungen für klassische Laufwerke: Dateinamen neuer Dateien verschlüsseln (empfohlen) und den Rechtsklick im Explorer.

Umstellen

1. Bei eingehängtem Boxcryptor-Laufwerk auf „**Auf modern umstellen ...**“ klicken.
2. **Ziel** wählen:
 - **Passwort-Tresor** – für Ihre persönlichen Daten, mit eigenem Tresor-Passwort.
 - **Team-Ordner (Schlüsselserver)** – für Daten, die mehrere Personen nutzen. Dafür müssen Sie beim Organisationskonto angemeldet sein; sonst steht dort „**Jetzt anmelden**“.
3. **Ordner für den neuen Tresor** angeben. Krywerk schlägt einen **neuen** Ordner neben dem Boxcryptor-Ordner vor (Name mit „(Krywerk)“ am Ende); Sie können auch einen anderen

leeren Ordner wählen, zum Beispiel in OneDrive. Der Ordner darf nicht im Boxcryptor-Ordner liegen.

4. Beim Passwort-Tresor ein Tresor-Passwort festlegen, beim Team-Ordner optional einen Namen.
5. **„Umstellung beginnen“**. Beim Team-Ordner zeigt Krywerk den Wiederherstellungsschlüssel – aufbewahren (Kapitel 5).

Ab jetzt zeigt das Laufwerk **beides zusammen**: Alles Neue und jede Datei, die Sie ändern, landet automatisch im modernen Format. In der Zeile steht, wie viele Dateien noch im alten Format liegen.

Den Rest umstellen – auf eine von zwei Arten:

- **Alles auf einmal: „Alles umstellen“**.
- **Ordnerweise**: Im Explorer Rechtsklick auf einen Ordner im Laufwerk › **„Mit Krywerk ins moderne Format umstellen“**. Unter Windows 11 steht der Eintrag eventuell erst unter „Weitere Optionen anzeigen“.

Abschließen

Liegt nichts mehr im alten Format, wird **„Umstellung abschließen“** anklickbar. Danach zeigt das Laufwerk nur noch den neuen Tresor bzw. Team-Ordner. Ein Team-Ordner erscheint dann mit der Kennzeichnung „Team“; Personen und Gruppen nehmen Sie unter **„Verwalten“** auf (Kapitel 4 und 5).

Der alte Boxcryptor-Ordner wird nicht mehr gebraucht. **Prüfen Sie das Ergebnis** – öffnen Sie einige Dateien – und löschen Sie den alten Ordner erst danach. Sind alle Boxcryptor-Ordner umgestellt, blendet Krywerk alles zu Boxcryptor aus.

7. Häufige Fragen und Probleme

Oben steht „Organisationskonto: nicht angemeldet“

Krywerk merkt sich die Anmeldung nur, bis Sie Krywerk beenden. Klicken Sie auf den gelben Hinweis oder auf **„Jetzt anmelden“** und melden Sie sich im Browser an. Solange Sie nicht angemeldet sind, fehlen Team-Ordner ohne Ordner auf diesem Computer sowie „Verwalten“; persönliche Tresore funktionieren unabhängig davon.

Im Browser wurde ich automatisch angemeldet – mit dem falschen Konto

Ist im Browser bereits jemand beim Anmeldedienst angemeldet, übernimmt der Browser diese Anmeldung, ohne zu fragen. Melden Sie sich im Browser ab (beim Anmeldedienst Ihrer Organisation, z. B. Microsoft) und melden Sie sich in Krywerk erneut an. Welches Konto angemeldet ist, steht oben im Krywerk-Fenster.

Der Anmelde-Tab im Browser ist zu, Krywerk reagiert nicht mehr

Krywerk wartet bis zu 5 Minuten auf die Anmeldung. Stellen Sie den Tab wieder her (im Browser **Strg+Umschalt+T**) und melden Sie sich an – oder warten Sie, bis Krywerk die Anmeldung mit einer Meldung abbricht, und versuchen Sie es erneut.

Ein Team-Ordner zeigt „Ordner auf diesem Gerät nicht gefunden“

Der Ordner ist noch nicht auf Ihrem Computer. Prüfen Sie, ob er in OneDrive mit Ihnen geteilt und als Verknüpfung zu „Meine Dateien“ hinzugefügt ist, und ob OneDrive fertig synchronisiert hat. Oder wählen Sie ihn mit **„Ordner suchen ...“** selbst aus.

Beim Öffnen eines Team-Ordners heißt es, der Zugriff sei noch nicht gewährt

Sie wurden aufgenommen, aber die verantwortliche Person hat den Zugriff noch nicht gewährt. Bitten Sie sie, in Krywerk **„Verwalten“** > **„Zugriff gewähren“** zu klicken.

Änderungen von Kolleginnen und Kollegen kommen nicht an

Prüfen Sie zuerst, ob OneDrive synchronisiert (OneDrive-Symbol im Infobereich). Erscheinen die Änderungen trotzdem nicht oder erst spät im Laufwerk, schalten Sie unter **⚙ Einstellungen** > **Allgemein** > **Erweitert** den **Zwischenspeicher** aus und hängen das Laufwerk neu ein.

Das Laufwerk erscheint nicht

- Ist es eingehängt? In der Liste muss „Eingehängt als ...“ bzw. „Geöffnet unter ...“ stehen.
- Unter Windows muss **WinFsp** installiert sein (Kapitel 2).
- Ist der gewählte Laufwerksbuchstabe schon belegt (z. B. durch ein Netzlaufwerk), wählen Sie unter „Bearbeiten“ einen anderen oder „Automatisch“.

Ich habe das Tresor-Passwort vergessen

Ein persönlicher Tresor lässt sich ohne Passwort nicht öffnen – auch nicht durch die IT. Ist das Passwort in Krywerk gemerkt, können Sie den Tresor auf diesem Computer weiter öffnen; legen Sie dann einen neuen Tresor an und kopieren Sie die Dateien hinüber.

Ich habe meinen Freischaltcode verloren

Auf Computern, die bereits freigeschaltet sind, können Sie weiterarbeiten. Für einen neuen Computer brauchen Sie den Freischaltcode. Wenden Sie sich an Ihre IT-Administration.

Mein Computer ist verloren oder gestohlen

Melden Sie es Ihrer IT-Administration. Wer Team-Ordner verwaltet, auf die der Computer Zugriff hatte, sollte nach einem Verlust den **Schlüssel erneuern** (Kapitel 5). Persönliche Tresore mit gemerktem Passwort sind durch Ihr Windows-Benutzerkonto geschützt – ein sicheres Windows-Passwort ist deshalb wichtig.

Der Schlüsselserver ist nicht erreichbar

Bereits geöffnete Team-Ordner bleiben geöffnet. Zum Öffnen ohne Server brauchen Sie den **Wiederherstellungsschlüssel** („Ohne Server öffnen ...“, Kapitel 5) – den hat die verantwortliche Person.

Kann ich Team-Ordner auf dem Handy öffnen?

Noch nicht. Persönliche Tresore öffnen Sie mit der Cryptomator-App (Kapitel 3).

8. Begriffe

Anmeldedienst – Dienst, bei dem Sie sich mit Ihrem Organisationskonto anmelden, zum Beispiel Microsoft 365. Krywerk öffnet ihn im Browser.

Boxcryptor (alt) – Kennzeichnung für Boxcryptor-Ordner in Krywerk. Älteres Verfahren, nur für den Übergang.

Boxcryptor-Schlüsseldatei (`.bckey`) – aus Boxcryptor exportierte Datei mit Ihren Boxcryptor-Schlüsseln, geschützt mit Ihrem Boxcryptor-Passwort.

Einhängen / Aushängen – ein Laufwerk verfügbar machen bzw. wieder entfernen. Die Dateien bleiben dabei erhalten.

Fingerabdruck – 64 Zeichen (acht Blöcke), die aus den öffentlichen Schlüsseln einer Person berechnet werden. Liest die Person ihn vor und stimmt er mit der Anzeige bei Ihnen überein, gehört der Schlüssel wirklich ihr.

Freischaltcode (auch *Account Key*) – Ihr persönlicher Code für Team-Ordner. Krywerk zeigt ihn beim Einrichten des Kontos einmal an. Sie brauchen ihn, um weitere Computer freizuschalten. Nur Sie haben ihn.

Gerät freischalten – einen Computer für Ihr Organisationskonto zulassen, damit er Team-Ordner öffnen kann.

Identität bestätigt / nicht bestätigt – ob Sie (oder eine Person, der Sie vertrauen) den Fingerabdruck einer Person mit ihr verglichen haben. Vor dem Gewähren von Zugriff empfohlen.

Krywerk Server – Schlüsselserver für Team-Ordner, den Ihre Organisation selbst betreibt. Kompatibel zum Cryptomator Hub, ohne Lizenzgrenzen.

Mitglied / „verwaltet“ – Rollen in einem Team-Ordner. Mitglieder öffnen und bearbeiten Dateien; wer ihn verwaltet, nimmt zusätzlich Personen auf, gewährt Zugriff und kümmert sich um Notfallzugriff und Wiederherstellungsschlüssel.

Notfallgremium / Notfallantrag – Personen, die gemeinsam (Vier-Augen-Prinzip) einer Person Verwaltungsrechte an einem Team-Ordner geben können, wenn alle verwaltenden Personen ausfallen.

Organisationskonto – Ihr Konto bei der Schule bzw. Organisation (z. B. Microsoft 365), mit dem Sie Team-Ordner öffnen.

Persönlicher Tresor – verschlüsselter Ordner mit eigenem Passwort, im Cryptomator-Format.

Schlüssel erneuern – einem Team-Ordner einen neuen Schlüssel geben, zum Beispiel nach dem Austritt einer Person.

Schlüsselserver – verwaltet, wer welchen Team-Ordner öffnen darf (Krywerk Server oder Cryptomator Hub). Er kann die Dateien selbst nicht lesen.

Team-Ordner – verschlüsselter Ordner für mehrere Personen, geöffnet über das Organisationskonto.

Tresor-Passwort – Passwort eines persönlichen Tresors. Nicht wiederherstellbar.

Wiederherstellungsschlüssel – 28 Vierergruppen, mit denen sich ein Team-Ordner ohne Schlüsselserver öffnen lässt. Gehört sicher verwahrt zu den Verantwortlichen.

Zugriff gewähren – Schritt, mit dem eine verwaltende Person neuen Mitgliedern den Schlüssel eines Team-Ordners zugänglich macht.

Zwischenspeicher – macht Laufwerke schneller; nur bei Problemen mit Änderungen von anderen Geräten ausschalten.