Umgang mit Passwörtern von Schülerinnen und Schülern

Empfehlungen für schulinterne Fachpersonen für pädagogischen/ technischen ICT-Support

Organisieren Administrieren

Die vermehrte Nutzung von Online-Diensten im Schulalltag führt zu einer Zunahme unterschiedlicher Benutzernamen und Passwörter bei den Schülerinnen und Schülern. Um diese jederzeit abrufbar zu machen, werden sie teilweise in Listen festgehalten. Im Folgenden werden verschiedene Optionen vorgestellt, wie diese Praxis aus datenschutzrechtlicher Sicht korrekt umgesetzt werden kann.

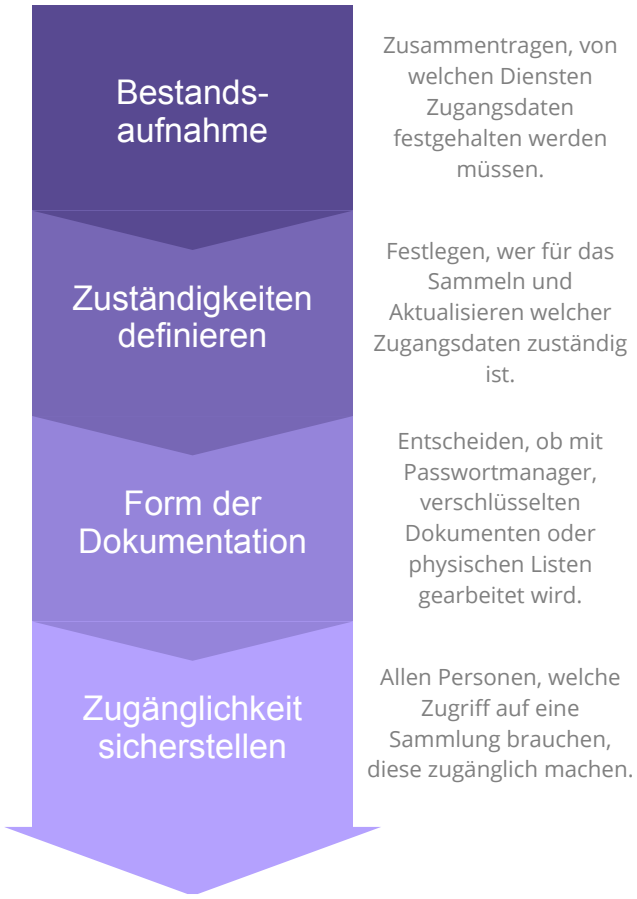
Sichere Passwörter

Die folgenden Vorgehensweisen zielen darauf ab, bei einem Passwortverlust schnell reagieren zu können, um ein rasches Weiterarbeiten zu ermöglichen. Im Allgemeinen sollte jedoch der Umgang mit und die Wichtigkeit von sicheren, merkbaren Passwörtern mit den Schülerinnen und Schülern thematisiert werden. Ein angeleitetes Vorgehen beim Setzen von Passwörtern kann diesen Prozess unterstützen. Vergleiche dazu beispielsweise "Mein sicheres Passwort" aus dem Lehrmittel Inform@21 (Zyklus 2).

Korrekter Umgang mit Sammlungen (Listen) von Passwörtern

Bei der Sammlung und Ablage von Zugangsdaten ist es empfehlenswert, einige Vorsichtsmassnahmen zu treffen, um eine datenschutzkonforme Aufbewahrung zu gewährleisten.

Vorbereitung



- In einer ersten Bestandsaufnahme wird erfasst, zu welchen Diensten Zugangsdaten gesammelt und festgehalten werden sollen.
- Für die gesamte Schule wird definiert, welche Personen für das Erstellen und Führen welcher Sammlungen zuständig sind (z. B. Klassenlehrpersonen, PICTS).
- In diesem Zusammenhang ist zudem festzulegen, wie mit den Sammlungen und den darin enthaltenen Zugangsdaten umgegangen wird, wann sie zum Einsatz kommen und welche Rechte und Pflichten die zugangsberechtigten Personen zu beachten haben.
- Des Weiteren ist zu klären, in welcher Form die Zugangsdaten festgehalten werden sollen.
- Passwort-Manager bieten den Vorteil, dass die darin gespeicherten Passwörter automatisch verschlüsselt gespeichert werden. Je nach Produkt können verschiedene Sammlungen (z. B. nach Klassen, nach Anwendung, usw.) angelegt und geteilt werden. Zugriff haben nur Personen, welche das Masterpasswort kennen. Da die Passwort-Datenbank in der Cloud gespeichert ist, wird ein ortsunabhängiger Zugriff ermöglicht. Beispiele für Passwort-Manager (Open-Source und in einer Basisversion gratis nutzbar): Proton Pass, Clipperz, Psono.
- Bei Sammlungen in digitalen Dokumenten besteht die Möglichkeit, diese durch ein Passwort zu schützen (Beispiel Mac, Beispiel Windows), welches nur den jeweiligen Berechtigten bekannt gegeben wird. Passwortgeschützte Dokumente können auch in einer Cloud abgelegt werden, was mehreren Personen den ortsunabhängigen Zugriff ermöglicht.
- Bei physischen Listen ist sicherzustellen, dass diese an einem verschliessbaren Ort aufbewahrt werden, zu welchem ausschliesslich die jeweils Berechtigten Zugriff haben.
- Zuletzt erfolgt die Definition der Zugriffsberechtigungen für die einzelnen Sammlungen. Das Ziel ist, dass jeweils nur so viele Personen wie nötig Zugriff erhalten, um einen effizienten und effektiven Zugang zu den Daten zu gewährleisten.

Umsetzung

- Alle Beteiligten werden über das Vorgehen bei Verlust oder Vergessen eines Passwortes informiert.
- Die Mitarbeitenden, welche für das Führen und Aufbewahren von Listen zuständig sind, werden entsprechend eingeführt und geschult.

Überprüfung

- Sammlungen, welche nicht mehr in Gebrauch sind, werden gelöscht beziehungsweise vernichtet. Bei schulinternen Übergängen und Wechseln besteht die Möglichkeit, die Sammlungen weiterzugeben.
- Es wird eine Person bestimmt, die die jährlich wiederkehrenden Prozesse koordiniert.
- Die technische Unterstützung für die Umsetzung der verschiedenen Massnahmen ist gewährleistet. Es steht eine direkte Ansprechperson zur Verfügung.

Zurücksetzen von Passwörtern

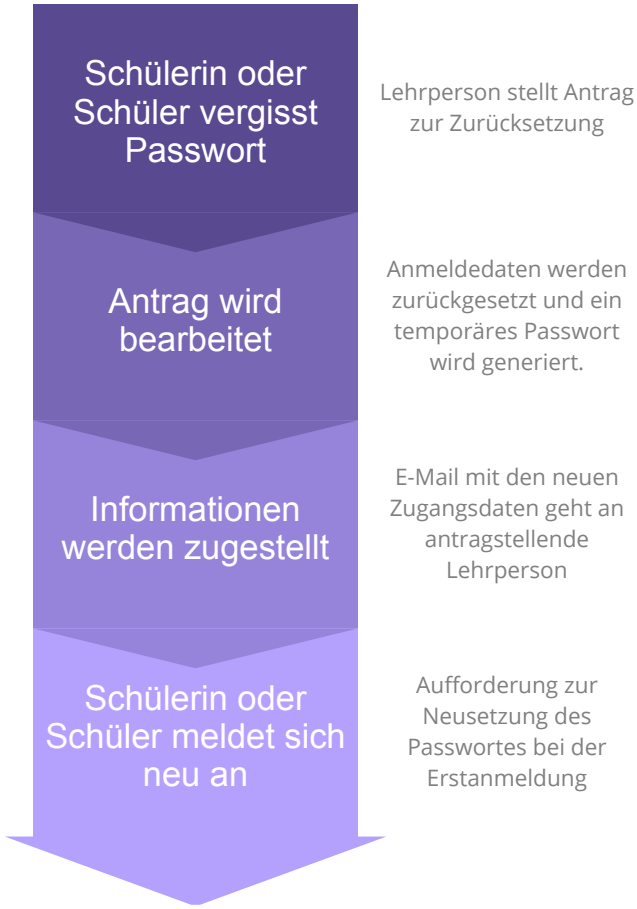
Bei bestimmten Diensten, darunter Microsoft 365, besteht die Möglichkeit, Passwörter auf Administratorenebene zurückzusetzen. Die gezielte Vergabe dieser Administratorenrechte ermöglicht es, vergessene Zugangsdaten zeitnah zurückzusetzen und neu zu vergeben. Sofern es der Dienst ermöglicht, ist diese Variante zu bevorzugen, da so das Sammeln und Festhalten von Passwörtern gänzlich vermieden werden kann.

Vorbereitung

- Es wird geklärt, welche Passwörter auf Systemverwaltungsebene zurückgesetzt werden können.
- Es wird definiert, welchen Personen (z. B. PICTS/TICTS) in der Schule die erforderlichen Administratorenrechte erteilt werden. Die Vergabe der Rechte erfolgt so, dass im Falle des Vergessens das betroffene Passwort möglichst schnell zurückgesetzt und neu vergeben werden kann. Gleichzeitig ist sicherzustellen, dass nur so viele Personen wie nötig über diese Rechte verfügen.
- Es wird festgelegt, wie bei Verlust oder Vergessen eines Passworts vorzugehen ist.

Umsetzung

- Personen mit Administratorenrechten werden entsprechend eingeführt und geschult.
- Alle Beteiligten werden über das Vorgehen bei Verlust oder Vergessen eines Passwortes informiert.



Überprüfung

- Die vergebenen Rechte werden jährlich überprüft und gegebenenfalls angepasst. Es ist sicherzustellen, dass jeweils nur so viele Personen wie nötig über die entsprechenden Berechtigungen verfügen.
- Die technische Unterstützung für die Umsetzung der verschiedenen Massnahmen ist sichergestellt. Es steht eine direkte Ansprechperson zur Verfügung.

Edulog

Edulog vereinfacht den Zugang auf zahlreiche Dienste, darunter Lernplattformen, digitale Lehr- und Lernmittel sowie Schuladministrationslösungen. Schülerinnen und Schüler können sich mit einem einzigen Zugang bei verschiedenen Diensten anmelden, um diese zu nutzen.
Für detailliertere Informationen wenden Sie sich an bitte an avkschulentwicklung@tg.ch.

Impressum: Version 3.2; Dezember 2024; CC BY 4.0, Angebote und Entwicklung, av.tg.ch