Bayerisches Staatsministerium für
Unterricht und Kultus

GESTALTEN > DIGITALISIERUNG

Datensicherheit und Datenschutz an Schulen

Stand: 28.01.2026

→ www.km.bayern.de / gestalten / digitalisierung / datensicherheit

Inhaltsverzeichnis

Datensicherheit und Datenschutz an Schulen 4

Allgemeine Hinweise 5
Strategische Dokumente 5
Taktische Dokumente 6
Operative Dokumente 6

Umgang mit Ausbildungsgeräten 7
Nutzungsbedingungen 7
Inbetriebnahme 8
Apps 8

Sichere Nutzung von Browsern 11

Datensicherung 16
Datensicherung im Kontext Schule 16
Vorgehensweise für die Erstellung eines Backup-Plans 17
FAQs Datensicherung 18
Downloads 20

Datenschutz an Schulen 21

Dienstliche Verwendung digitaler Kommunikations- und Kollaborationswerkzeuge 22
Kategorisierung des Schutzbedarfs 23
Betrieb, Authentifizierung und Datenübertragung 25
Groupware 26
Messenger 28
Cloud-Speicher 29
Videokonferenzwerkzeug 31
Besonders zur Geheimhaltung verpflichtete Personen 32
FAQ zu diesem Thema 34
Downloads 40

Umgang mit Lehrerdienstgeräten 41
Nutzungsbedingungen für Lehrerdienstgeräte 41
Mindestsicherheitsstandards 42
Checklisten 42

Mobile Device Management 44
Allgemein 44
Checkliste und Dokumente 45
Auswahl eines MDM-Systems 46

Betrieb eines MDM-Systems 48
Konfiguration der Endgeräte 51
FAQ zu MDM-Systemen 51

Nutzungsordnung 55

Private Endgeräte im Dienstgebrauch 57
Zulassung 57
Mindestsicherheitsstandards 58
FAQs 59

Umgang mit Schülerleihgeräten 61

Schulnetz 63
Sicherheit im Schulnetz 63
Schulnetzdesign 64
Fernzugriff (VPN) 65
Firewall 66
Webfilter 67
WLAN 69

Verschlüsselung 72
Verschlüsselung von Dateien, Wechseldatenträgern oder Container 72
Beispiele für Verschlüsselungsprogramme 74
Sichere Übertragung 75

Sensibilisierung und Awareness 76

Berechtigungsmanagement 78
Netz- und Hardware-Ebene 79
Dienste- und Anwendungs-Ebene 79

Datensicherheit und Datenschutz an Schulen

Allgemeine Hinweise

Datensicherheit ist ein unverzichtbarer Bestandteil des bayerischen Schulwesens ©Thapana_Studio - stock.adobe.com

Informationssicherheit nimmt in Zeiten der fortschreitenden Digitalisierung und der steigenden Bedrohung durch Angriffe auf Daten und IT-Systeme einen immer höheren Stellenwert ein. Für die Schulen ist eine sichere Informations- und Kommunikationstechnik von höchster Bedeutung, denn sie resultiert aus der Verpflichtung, verantwortungsvoll bei der Verarbeitung von Daten vorzugehen.

Die Verfügbarkeit, Integrität und Vertraulichkeit der in IT-Systemen gespeicherten und dort übertragenen Daten muss durch technische und organisatorische Maßnahmen gewährleistet werden. Das Staatsministerium für Unterricht und Kultus legt mit den unten aufgeführten Dokumenten einen Sicherheitsrahmen fest.

Strategische Dokumente

Strategische Dokumente bestimmen und beschreiben die strategische Ausrichtung bei der Umsetzung von Informationssicherheit an Schulen. Diese Dokumente enthalten **allgemein gültige, kurze und verständliche Regelungen verpflichtenden Charakters.**

KMBek Schulische IT-Infrastruktur und Internetzugang
https://www.verkuendung-bayern.de/baymbl/2022-436/

Bekanntmachung zum Vollzug der datenschutzrechtlichen Bestimmungen
https://www.verkuendung-bayern.de/baymbl/2022-435/

Taktische Dokumente

Taktische Dokumente definieren Umsetzungsvorgaben und setzen einen **verpflichtenden Regelungsrahmen**, der von den Verantwortlichen ggf. verschärft werden kann. Diese Dokumente enthalten **Ergänzungen und Konkretisierungen** der übergeordneten strategischen Dokumente. Beispiele hierfür sind:

Muster für eine Nutzungsordnung zur Nutzung der schulischen IT-Infrastruktur und des Internetzugangs an Schulen
https://www.verkuendung-bayern.de/files/baymbl/2022/436/anhang/Anlage.pdf

→ **Muster für Nutzungsbedingungen für Lehrerdienstgeräte**
https://www.km.bayern.de/gestalten/digitalisierung/datensicherheit/lehrerdienstgeraete#nutzungsbedingungen-fuer-lehrerdienstgeraete

Operative Dokumente

Operative Dokumente beschreiben Hilfestellungen zur Umsetzung der Vorgaben in der Schule. Diese Dokumente enthalten konkrete und ausführliche Beschreibungen für die Umsetzung von Sicherheitsmaßnahmen, z. B.

→ **Checkliste Lehrerdienstgeräte**
https://www.km.bayern.de/gestalten/digitalisierung/datensicherheit/lehrerdienstgeraete#checklisten

→ **Checkliste privaten Endgeräte**
https://www.km.bayern.de/gestalten/digitalisierung/datensicherheit/private-endgeraete-im-dienstgebrauch

Die Handreichungen und Checklisten (taktische und operative Dokumente) dienen als Orientierungshilfe für die technischen und pädagogischen Systembetreuer. Sie sollen aufzeigen, wie z.B. das Schulnetz sinnvoll und angemessen (gemäß Schutzbedarf der verarbeiteten Daten) gesichert werden soll.

Für die pädagogischen Mitarbeiter dienen die Handreichungen und Checklisten unter anderem auch als Prüfwerkzeug gegenüber den eingesetzten IT-Dienstleistern.

Umgang mit Ausbildungsgeräten

Standards garantieren einen sicheren Einsatz von digitalen Medien ©twinsterphoto - stock.adobe.com

Die Ausbildung der zukünftigen Lehrkräfte im Vorbereitungsdienst ist eine staatliche Aufgabe, bei der einheitliche Ausbildungsstandards und gleichwertige Prüfungsbedingungen im Vordergrund stehen. Unter fachkundiger Begleitung durch die Seminarlehrkräfte sollen die angehenden Lehrkräfte durch den praktischen Einsatz der Ausbildungsgeräte medienbezogene Lehrkompetenzen aufbauen und die im Studium erworbenen Fertigkeiten durch praktische Anwendung im eigenen Unterricht ausbauen.

Das Bayerische Staatsministerium für Unterricht und Kultus stellt hierfür die Ausbildungsgeräte bereit. In Zusammenarbeit mit der Telekom Deutschland GmbH wird zusätzlich ein umfassendes Service- und Dienstleistungspaket angeboten.

Nutzungsbedingungen

Der Einsatz von digitalen Endgeräten birgt jedoch auch Risiken und muss unter angemessenen Bedingungen erfolgen.

Daher ist es notwendig, die Endgeräte durch geeignete Sicherheitsmaßnahmen angemessen zu schützen, die Benutzer auf Risiken hinzuweisen und die zulässigen

Nutzungsmöglichkeiten aufzuzeigen.

Dies geschieht insbesondere durch die Nutzungsbedingungen. Sie werden der Anwenderin bzw. dem Anwender bei Ausgabe des Geräts vorgelegt. Die Kenntnisnahme ist durch die Schule in geeigneter Weise zu dokumentieren.

Zielgruppe: Schulleiterinnen und Schulleiter, Systembetreuerinnen und Systembetreuer

Adressaten: Studienreferendarinnen und -referendare, Lehramtsanwärterinnen und -anwärter, Fachlehreranwärterinnen und -anwärter, Förderlehreranwärterinnen und -anwärter, Seminarlehrkräfte

Musternutzungsbedingungen für Ausbildungsgeräte
/download/4-23-11/Nutzungsbedingungen-f%C3%BCr-Ausbildungsger%C3%A4te_6.0.jpg

---

Inbetriebnahme Ausbildungsgeräte – Schritt-für-Schritt-Anleitungen

Die folgenden Dokumente beschreiben die Inbetriebnahme von iPads bzw. Surface-Geräten.

iPad-Inbetriebnahme – Schritt-für-Schritt-Anleitung
/download/4-23-11/Schritt-f%C3%BCr-Schritt_Anleitung-Ausbildungsger%C3%A4ten_iPad.jpg

Surface-Inbetriebnahme – Schritt-für-Schritt-Anleitung
/download/4-23-11/Schritt-f%C3%BCr-Schritt_Anleitung-Ausbildungsger%C3%A4ten_Surface-1.jpg

---

Apps auf den Ausbildungsgeräten

Bei den Geräten handelt es sich um **staatliche Geräte**. Sie werden mit notwendigen Restriktionen und technischen Einschränkungen ausgeliefert, die das Herunterladen von Apps aus den bekannten Stores (bspw. App Store und Microsoft Store) auf das Gerät aus Sicherheitsgründen und aufgrund des Datenschutzes technisch unterbinden.

Um gleichwohl einen sinnvollen Einsatz in der Ausbildung sicherzustellen, der den

datenschutztechnischen und -rechtlichen Vorgaben genügt, galt es, eine vorhergehende sicherheitstechnische Überprüfung der Apps vorzunehmen, für die Verwendungsbedarf besteht. Daher hat das Bayerische Staatsministerium für Unterricht und Kultus den vertraglich gebundenen Dienstleister Telekom Deutschland GmbH mit der datenschutztechnischen bzw. datenschutzrechtlichen Prüfung von Apps beauftragt. **Die Auswahl der zu überprüfenden Apps erfolgt durch die Schulen nach deren jeweiligen Bedarfen.**

Hinweis zur Nutzung von Apps aus dem Catalog
/download/4-24-05/Software_Apps_f%C3%BCr_Ausbildungsger%C3%A4te_V7.jpg

Prozess

Das folgende Dokument zeigt den Prozess der Einführung einer App als Schaubild.

Prozessbeschreibung Apps auf Ausbildungsgeräten
/download/4-23-11/Prozessbeschreibung_Ausbildungsger%C3%A4te_Apps.jpg

Antragsdokumente

Mit den folgenden Dokumenten kann die Prüfung einer App bzw. deren Bereitstellung beantragt werden. Zur Dokumentation findet sich auch noch ein Musterbewertungsbogen.

Antrag auf Prüfung einer App auf den Ausbildungsgeräten
/download/4-23-11/SNR_Antrag_auf_Pruefung_v1.jpg

Antrag auf Bereitstellung einer App auf den Ausbildungsgeräten (Grund-/Mittel-/Förderschulen)
/download/4-23-11/SNR_Antrag_auf_Bereitstellung_GMS_FoeS_v1.jpg

Antrag auf Bereitstellung einer App auf den Ausbildungsgeräten (GYM/RS/BerS)
/download/4-23-11/SNR_Antrag_auf_Bereitstellung_weiterfuehrende_Schulen_v1.jpg

Bewertungsbogen
/download/4-23-11/Bewertungsbogen_Muster.jpg

Sichere Nutzung von Browsern

Browsersicherheit schafft Datensicherheit ©Robert Avgustin - stock.adobe.com

Empfehlungen zur Nutzung von Browsern

Der Browser ist eine der am häufigsten genutzten Anwendungen auf dem Endgerät. Er ermöglicht den Zugriff auf eine Vielzahl von Internetangeboten, Webanwendungen und Clouddiensten auf Webservern. Unter Berücksichtigung der nachfolgend aufgeführten Aspekte lässt sich die Sicherheit bei der Nutzung dieser Angebote erhöhen:

- Sicherer Aufruf von Webseiten
- Regelmäßiges Löschen zwischengespeicherter, insbesondere personenbezogener, Daten
- Datensparsame Nutzung und sicherheitsrelevante Einstellungen an Browsern bei Endgeräten, die von mehreren Personen genutzt werden

Die nachfolgenden Klapptexte liefern weitere Informationen zur sicheren Nutzung von Browsern.

Sichere Kommunikation

Die Verschlüsselung der Übertragungsdaten zwischen Browser und Webserver ist inzwischen Standard. Moderne Browser zeigen dies durch ein Symbol (z.B. ein Schloss) in der Adressleiste an. Nur wenn der Webserver die Verschlüsselung unterstützt und ein gültiges Zertifikat nachweisen kann, wird der Browser die Verbindung als gesichert markieren.

TLS (Transport Layer Security) ist das aktuelle Verfahren bzw. Protokoll zur sicheren Internetkommunikation. Es wird von allen aktuellen Browsern unterstützt und ist automatisch aktiv, wenn eine Webseite über HTTPS (Hypertext Transfer Protocol Secure) aufgerufen wird. Der Aufruf einer verschlüsselten Verbindung erfolgt durch die Eingabe von "https://" vor der Webadresse in der Adressleiste des Browsers. In vielen Fällen leiten Webserver automatisch von HTTP auf HTTPS um, um eine sichere Verbindung zu gewährleisten.

⚠ Hinweis

Die Tatsache alleine, dass die Verbindung verschlüsselt ist und durch ein gültiges Zertifikat verifiziert werden konnte, ist noch keine Garantie dafür, dass die aufgerufene Seite keine bösartigen Inhalte, wie beispielsweise Malware oder Phishing-Formulare, bereitstellt.

Umgang mit Downloads

Beim Arbeiten im Internet lädt der Nutzende Dateien (z. B. Bilder, pdf-Dateien usw.) herunter, die standardmäßig im Download-Verzeichnis des Betriebssystems gespeichert werden. Auf diese Weise können sich so schnell viele Dateien ansammeln, die beträchtlichen Speicherplatz belegen können. In diesen Dateien können auch **personenbezogene Daten** (z. B. Anhänge von E-Mails, Klassenlisten etc.) enthalten sein, die regelmäßig gelöscht werden sollten.

Das regelmäßige Löschen des Inhalts des Download-Ordners führt nicht nur zu mehr freiem Speicherplatz, sondern schützt auch vor ungerechtfertigter Vorhaltung personenbezogener Daten.

Umgang mit Browsercache und Cookies

Bei jedem Zugriff auf einen Webserver werden Daten übertragen. Eine Speicherung dieser Daten durch den Browser reduziert die zu übertragende Datenmenge, beispielsweise bei erneutem Aufrufen von Bildern. Die lokale Verfügbarkeit der Inhalte fördert den schnellen Aufbau der Webseite, da die Daten bereits im Zwischenspeicher (Cache) des Endgerätes abgelegt wurden.

Der Zugriff auf diese Inhalte ermöglicht jedoch umfangreiche Rückschlüsse auf das Surfverhalten. In Abhängigkeit vom jeweiligen Nutzungsprofil des Nutzers sowie des genutzten Endgerätes ist eine regelmäßige Löschung des Caches zu empfehlen.

Die regelmäßige Löschung des Caches gewährleistet, dass keine personenbezogenen Daten auf dem Endgerät zurückbleiben und der verfügbare Speicherplatz freigegeben wird. Der zuvor beschriebene Prozess kann zudem über die Browsereinstellungen automatisiert werden, sodass nach Beendigung der Browsernutzung alle zwischengespeicherten Daten gelöscht werden.

Neben den Inhalten einer Webseite werden im Browser ergänzende Informationen gespeichert, sogenannte "Cookies". Diese Informationen dienen unterschiedlichsten Zwecken, wie beispielsweise der Erfassung des Besuchs einer Webseite oder der Steigerung der Nutzerfreundlichkeit. Cookies können sowohl technisch notwendige Funktionen erfüllen als auch Komfortfunktionen in der Nutzung von Browsern bereitstellen. Dazu zählt beispielsweise die Unterstützung beim Ausfüllen von Formularen oder beim Speichern von Online-Warenkörben.

Über Cookies lässt sich aber auch das Surfverhalten der Nutzenden, deren Wege über verschiedene Webseiten oder deren Klickverhalten analysieren.

Zur Sicherung der Privatsphäre besteht die Möglichkeit, Cookies regelmäßig oder automatisch beim Schließen des Browsers zu löschen. Die Konfiguration erfolgt über das Menü „Einstellungen“ des Browsers. Sie ist über das Stichwort „Cookies“ in der Suchfunktion der Einstellungen zu finden.

Umgang mit Passwörtern

Bei einer Anmeldung auf einer Webseite ist die Eingabe persönlicher Zugangsdaten erforderlich. Browser bieten die Möglichkeit, die erforderlichen Daten zu speichern, welche im Passwortspeicher des Browsers hinterlegt werden.

Sofern eine andere Person Zugriff auf das Endgerät und damit auf die Browserdaten hat, besteht die Möglichkeit, sich mit vorgetäuschter Authentizität bei den gespeicherten Webseiten anzumelden. Dies birgt ein beträchtliches Sicherheitsrisiko.

Daher ist es unerlässlich, den Zugriff auf das Endgerät sowie die gespeicherten Zugangsdaten durch ein komplexes Passwort zu schützen.

Es ist nicht immer gleich nachvollziehbar, ob Passwörter lokal auf dem Endgerät oder in einem Cloud-Konto des Browserherstellers gespeichert werden. Eine Speicherung in einem Cloud-Konto sollte wohlüberlegt sein, da dem Anbieter vertraut werden muss.

Besser ist es, dass auf eine Speicherung im Browser verzichtet wird und stattdessen ein Passwort-Manager zum Einsatz kommt. Oftmals bieten Passwort-Manager auch die Möglichkeit der Generierung von sicheren und komplexen Passwörtern.

Zugriff auf Gerätefunktionen

Webseiten und deren integrierte Anwendungen können Zugriff auf bestimmte Gerätefunktionen (z. B. Kamera, Mikrofon oder Standort) verlangen. Als Beispiel sei hier das Videokonferenztool ViKo der ByCS angeführt, welche ohne die Einbindung von Kamera und Mikrofon nicht sinnvoll nutzbar ist.

Der Zugriff auf den Standort ist auf die unbedingt erforderlichen Funktionen bei mobilen Endgeräten zu beschränken. Es sollte grundsätzlich überprüft werden, ob der Standort tatsächlich für die ordnungsgemäße Funktion erforderlich ist.

Im Zweifelsfall sollten Berechtigungen im Nachgang wieder entzogen oder gar nicht erst erteilt werden.

Die erteilten Berechtigungen können über das Menü „Einstellungen“ des Browsers eingesehen werden. Sie sind meist über das Stichwort „Berechtigungen“ in der Suchfunktion der Einstellungen zu finden.

Multi-User und Kiosk-Nutzung

Im Kontext schulischer Nutzung ist es nicht ungewöhnlich, dass ein Gerät von mehreren Personen verwendet wird. In pädagogischen Einrichtungen wie Klassenzimmern, Bibliotheken oder Lehrerzimmern stehen den Schülerinnen und Schülern sowie dem Lehrpersonal Endgeräte zur gemeinsamen freien Nutzung zur Verfügung, wobei mitunter eine benutzerindividuelle Authentifizierung nicht erforderlich ist.

Unter den genannten Einsatzbedingungen ist eine automatische Löschung temporärer Daten (u. a. Cache, Browserverläufe, Cookies) nach jeder Sitzung erforderlich. Dadurch wird auch der unbefugte Zugriff auf personenbezogene Daten verhindert. Gleiches gilt für das Download-Verzeichnis. Die entsprechenden Einstellungen sind ggf. auf administrativer Ebene vorzunehmen.

Es empfiehlt sich die Verwendung des Privat- bzw. Inkognito-Modus (Funktionsbezeichnung ist vom Browser abhängig). Dabei werden beim Schließen des Fensters automatisch benutzerbezogene Informationen, wie der Verlauf und Cookies, gelöscht. Auch offene Websitzungen werden beendet. Zu beachten ist jedoch, dass Dateien, die heruntergeladen wurden, auch in diesem Modus auf dem Endgerät verbleiben und manuell gelöscht werden müssen.

Browsererweiterungen (Plug-Ins)

Browsererweiterungen, sogenannte Plug-Ins, sind kleine Programme, die dem Browser zusätzliche Funktionen hinzufügen. Ihre Funktion besteht in der Erweiterung des Funktionsumfangs, der Erhöhung der Sicherheit oder der Blockierung unerwünschter Werbung.

Die Verwendung von Browsererweiterungen sollte mit Vorsicht erfolgen, da diese potenziell Zugriff auf sensible Daten haben. Es wird empfohlen, Erweiterungen nur aus vertrauenswürdigen Quellen zu installieren und diejenigen zu wählen, die regelmäßig aktualisiert werden. Die Anzahl der installierten Zusatzfunktionen sollte mit Bedacht gewählt werden, da jede Erweiterung ein zusätzliches Sicherheitsrisiko birgt. Die geforderten Berechtigungen der Browsererweiterungen müssen hinsichtlich des Anwendungszwecks kritisch geprüft werden.

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 https://www.km.bayern.de#downloads 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 Vorhaltedauer 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	· **Einfache Handhabe** bei der Erstellung und Wiederherstellung · **Übersichtlich** auch für Laien · Sehr einfaches Wiederherstellen von **einzelnen Dateien**	· Großer **Speicherplatzbedarf** · Lange **Sicherungsdauer**
Synchronisieren	Beim Synchronisieren werden zwei **Datenbestände abgeglichen**. Es wird lediglich kopiert oder erstellt (Dateien oder Sektoren), was sich verändert hat.	· **Einfache Handhabe** bei der Erstellung und Wiederherstellung · **Sehr kurze** Sicherungsdauer · **Sehr geringer** Speicherplatzbedarf · Sehr einfaches Wiederherstellen von **einzelnen Dateien**	· 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.	· Per se **verschiedene Datenstände** · **kurze** Sicherungsdauer · **Geringer** Speicherplatzbedarf	· **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	· Per se **verschiedene Datenstände** · **Keine lange** Sicherungsdauer · **relativ geringer** Speicherplatzbedarf	· **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, die 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
/download/4-24-04/Beispiel_Backupplan.jpg

Vorlage Backup-Plan
/download/4-24-04/Muster_Backupplan.jpg

Datenschutz an Schulen

Dienstliche Verwendung digitaler Kommunikations- und Kollaborationswerkzeuge

©Svitlana - stock.adobe.com

Für die Erledigung dienstlicher Aufgaben kann auch in der Schule auf digitale Kommunikations- und Kollaborationswerkzeuge zurückgegriffen werden.

Da bei der Aufgabenerfüllung mitunter sensible personenbezogene Daten verarbeitet werden, muss auch ein besonderes Augenmerk auf die Datensicherheit gelegt werden.

Im Folgenden werden die digitalen Kommunikations- und Kollaborationswerkzeuge

- Groupware (z. B. E-Mail-Postfach, Kalender, Notizen),
- Messenger,
- Cloud-Speicher und
- Videokonferenzwerkzeuge

näher betrachtet und **technische und organisatorische Maßnahmen beschrieben**. Die Maßnahmen orientieren sich an den Anforderungen des BSI IT-Grundschutzes. Die Umsetzung der Maßnahmen stellen die Mindestsicherheitsstandards dar. Die Pflicht zur Umsetzung der in Nr. 6 Anlage 2 Abschnitt 7 zu § 46 BaySchO festgelegten technischen und organisatorischen Maßnahmen bleibt unberührt.

Die **Zielgruppe** der beschriebenen Maßnahmen ist: Schulleitung, pädagogischer Systembetreuer, Dienstleister, Lehrkräfte und sonstiges an der Schule

tätiges Personal , Schulaufwandsträger

Regelung zur Datenverarbeitung und Rechenschaftspflicht der Schule

Die **Schule legt** innerhalb des Rahmens der gesetzlichen Vorgaben auf Basis ihrer Organisationshoheit **fest, welche Daten** mittels **welchem digitalen Kommunikations - und Kollaborationswerkzeugs** verarbeitet werden dürfen.

Dies dient dazu, dass die Schulleitung ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 i.V.m. Art. 32 DSGVO nachkommt.

Das Staatsministerium hat zu diesem Zweck die bereitgestellten (Muster-)Verarbeitungsbeschreibungen überarbeitet. Diese müssen an den dafür vorgesehenen Stellen ausgefüllt, zum Verarbeitungsverzeichnis genommen und bei Änderungen entsprechend aktualisiert werden.

Zielgruppe: Schulleitung

Kategorisierung des Schutzbedarfs

Gemäß IT-Grundschutz-Methodik des BSI https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-2-IT-Grundschutz-Methodik/bsi-standard-200-2-it-grundschutz-methodik_node.html hängen die für einen sicheren Einsatz von Kommunikations- und Kollaborationswerkzeugen notwendigen Maßnahmen vom Schutzbedarf der
darin verarbeiteten Daten ab.

Dabei unterscheidet man zwischen

- normalem Schutzbedarf (Regelfall)
- hohem Schutzbedarf, z.B. bei der Verarbeitung von Daten, die einem besonderen strafrechtlichen Geheimnisschutz
  unterliegen (z. B. § 203 StGB) (vgl. Nr. 3.4 Anlage 2 Abschnitt 7 zu § 46 BaySchO), bei der Verarbeitung von besonderen Kategorien personenbezogener Daten i. S. d. Art. 9 DSGVO, insbesondere Gesundheitsdaten (vgl. Nr. 3.4 Anlage 2 Abschnitt 7 zu § 46 BaySchO)

Folgende Tabelle stellt einen Überblick über in der Schule verarbeitete Daten (excl. der oben bereits genannten Daten) und deren Schutzbedarf dar.

Zielgruppe: Schulleitung, pädagogischer Systembetreuer, Dienstleister, Lehrkräfte und sonstiges an der Schule tätiges Personal

Überblick über in der Schule verarbeitete Daten mit ihrer Schutzbedarfskategorie

normal

- Allgemeine Bekanntmachungen
- Vorbereitung und Nachbereitung von Fortbildungen
- Vorbereitung und Nachbereitung von Fachsitzungen
- Bericht zur allgemeinen Klassensituation, ohne konkreten Bezug zu Einzelpersonen
- Unterrichtsmaterialien
- Informationen zu beurteilungs-relevanten Themen wie Nachweise zu besuchten Fortbildungen bzw. außerschulischen Aktivitäten (nicht die Beurteilung selbst!)
- Informationen im Zusammenhang mit dem Sachaufwand
- Einzelnoten
- Fehlzeiten ohne Bezug zum Gesundheitszustand

hoch

- Krankmeldungen
- Informationen über familiäre und soziale Hintergründe und soziale Beziehungen von Schülerinnen und Schülern oder Lehrkräften
- Informationen über Ordnungsmaßnahmen
- Kommunikation über das Verhalten einzelner Schülerinnen und Schüler
- Notenlisten

Der Umgang mit Einzelnoten und Notenlisten ist in den → FAQ https://www.km.bayern.de#faq-zu-diesem-thema entsprechend geregelt.

HINWEIS

Aufgrund der heterogenen Schullandschaft kann die Vollständigkeit vom Staatsministerium für Unterricht und Kultus nicht gewährt werden. In Einzelfällen, die in der Tabelle nicht erfasst sind, muss die Schule selbstständig eine Schutzbedarfsfeststellung vornehmen, um die notwendigen Maßnahmen zu ergreifen.
Hierzu dienen auch die Hinweise zur Schutzbedarfsfeststellungen in den Downloads

Betrieb, Authentifizierung und Datenübertragung

Betrieb

Die digitalen Kommunikations- und Kollaborationswerkzeuge müssen sicher betrieben werden. Die relevanten Vorgaben ergeben sich aus dem IT-Grundschutz Kompendium (in der aktuellsten Fassung) und müssen vom Verantwortlichen umgesetzt werden.

Dazu zählen unter anderem:

- Patch- und Schwachstellenmanagement
- Schutz vor Schadprogrammen
- Protokollierung
- Datensicherungsmanagement
- Detektionsmanagement
- Incidentmanagement

Sofern ein Dienstleister oder der Schulaufwandsträger für den Betrieb zuständig ist, muss sich die Schule die Umsetzung von Sicherheitsmaßnahmen schriftlich bestätigen lassen. Dies kann beispielsweise in einer Vereinbarung über die Auftragsverarbeitung (AVV) – konkret in den zu regelnden technischen und organisatorischen Maßnahmen - mit dem Dienstleister oder dem Schulaufwandsträger erfolgen.

Authentifizierung

Um den Zugriff von Unberechtigten auf die Daten, die mittels der Kommunikations-Kollaborationswerkzeuge verarbeitet werden, zu unterbinden, ist eine Authentifizierung vorzusehen (i.d.R. Benutzername und sicheres Passwort). Dies muss durch den Betreiber des digitalen und Kommunikations- und Kollaborationswerkzeugs sichergestellt sein.

Datenübertragung

Alle Daten, die zwischen den Kommunikationspartnern ausgetauscht werden, sind während der Übermittlung über das Internet zu verschlüsseln (Transportverschlüsselung über TLS). Dies muss durch den Betreiber des digitalen Kommunikations- und Kollaborationswerkzeugs sichergestellt sein. Der Stand der Technik ist bei der Verschlüsselung stets zu beachten und umzusetzen.

Weiterführende Informationen können unter der Rubrik → Verschlüsselung https://www.km.bayern.de/gestalten/digitalisierung/datensicherheit/verschluesselung eingesehen werden.

Die weiteren spezifischen Mindestanforderungen werden bei den einzelnen Kommunikations- und Kollaborationswerkzeugen genannt.

Groupware

Unter Groupware versteht man in diesem Kontext eine Anwendung mit folgenden Funktionen:

- E-Mail-Postfach
- Kalender
- Kontaktverzeichnis
- Aufgaben/Notizen

Da in Groupware unter anderem besonders vertrauliche Daten verarbeitet werden, sollte der Zugang mit einer spezifischen Authentisierung (z. B. 2-Faktor-Authentisierung) geschützt werden. Dies muss durch den Betreiber sichergestellt sein.

Übertragung von Daten per E-Mail

Wenn E-Mails unverschlüsselt übertragen werden, können sich nicht berechtigte Dritte leicht Zugriff auf den Inhalt verschaffen. Daher muss darauf geachtet werden, dass Inhalte sicher übertragen werden. Das gilt insbesondere dann, wenn die E-Mail personenbezogene Daten enthält.

Daher müssen folgende Maßnahmen bei der E-Mail-Kommunikation beachtet werden:

Diejenigen personenbezogenen Daten, die über die notwendigen Angaben zu Absender und Empfänger hinausgehen, müssen **Ende-zu-Ende-verschlüsselt** übertragen werden. Die technischen Voraussetzungen müssen durch den Betreiber bereitgestellt werden. Ansonsten muss die Erzeugung und → Verschlüsselung https://www.km.bayern.de/gestalten/digitalisierung/datensicherheit/verschluesselung der

Inhaltsdaten mit Drittprodukten erfolgen.

Diese Maßnahmen sind einem → OnePager https://www.km.bayern.de/gestalten/digitalisierung/datensicherheit/dienstliche-verwendung-digitaler-kommunikations#downloads zusammengefasst.

> **Hinweis**
>
> Die E-Mail-Kommunikation, die über das im Bayerischen Schulportal integrierte Outlook Web Access (OWA) erfolgt, ist von oben genannten Maßnahmen nicht betroffen, da andere Sicherheitsmaßnahmen umgesetzt wurden.

Automatisches Weiterleiten

Die automatische Weiterleitung an ein privates Postfach ist verboten und sollte technisch durch den Betreiber des Groupware-Dienstes unterbunden werden. Sofern dies nicht möglich ist, muss durch die Schulleitung eine organisatorische Regelung getroffen werden.

Phishing-E-Mails

Die E-Mail-Kommunikation wird auch von Kriminellen in Form von Phishing-E-Mails ausgenutzt, um an sensible Informationen (Zugangsdaten etc.) zu gelangen (**Social Engineering**). Zudem werden Dateien mit **Schadsoftware** als Anhang von E-Mails versendet. Falls solche E-Mails nicht durch Sicherheitsmechanismen gefiltert werden und die Dateien ausgeführt werden, wird die Schadsoftware „aktiviert“. Diese kann z.B. durch „Verschlüsselungstrojaner“ zu erheblichen Schäden für die schulischen IT-Systeme führen.

E-Mails mit schädlichem Inhalt können täuschend echt aussehen. Es gibt jedoch Anzeichen, an denen die betrügerischen E-Mails erkannt werden können.

Zielgruppe: Schulleitung, pädagogischer Systembetreuer, Dienstleister, Lehrkräfte und sonstiges an der Schule tätiges Personal

Ein Leitfaden zum Erkennen von Phishing-E-Mails befindet sich bei den → Downloads https://www.km.bayern.de#downloads

Aufgaben und Notizen

Aufgaben und Notizen sollen so wenig wie möglich personenbezogene Inhalte enthalten. Dokumente als Anhang einer Aufgabe, die Daten mit hohem Schutzbedarf enthalten, müssen gegen einen Fremdzugriff geschützt werden (vgl. → OnePager https://www.km.bayern.de/gestalten/digitalisierung/datensicherheit/dienstliche-verwendung-digitaler-kommunikations#downloads).

Es wird empfohlen, Verweise auf Dokumente (z.B. Link auf ein Dokument im Cloud-Speicher) zu hinterlegen, deren Zugriff entsprechend geschützt ist.

Kalendereinträge

Kalendereinträge (insbesondere Betreff und Textfeld) sollen so wenig wie möglich personenbezogene Inhalte enthalten. Dokumente als Anhang des Kalendereintrags, die Daten mit hohem Schutzbedarf enthalten, müssen gegen einen Fremdzugriff geschützt werden (vgl. → OnePager https://www.km.bayern.de/gestalten/digitalisierung/datensicherheit/dienstliche-verwendung-digitaler-kommunikations#downloads).

Kalenderfreigaben sind restriktiv zu setzen. Die Darstellung ist soweit nicht andres erforderlich auf die Anzeige „frei“ oder „gebucht“ einzuschränken.

Messenger

Beim Messenger werden organisatorische und technische Mindestanforderungen unterschieden. Die technischen Anforderungen müssen durch den Betreiber des Werkzeugs sichergestellt sein.

Organisatorische Maßnahmen beim Messenger

Der Name von Chatgruppen soll keine identifizierenden Informationen zu Personen oder dem besonders vertraulichen Inhalt enthalten.

Technische Maßnahmen beim Messenger

Der Zugriff auf die lokal gespeicherten Nachrichten im Messenger (z.B. auf einem Smartphone) muss durch angemessene Maßnahmen geschützt werden (z. B. Pin-Eingabe beim Öffnen der Anwendung).

Daten dürfen nur über Messenger ausgetauscht werden, wenn sichergestellt ist, dass nur die Berechtigten (i. d. R. Absender und Empfänger) Zugriff auf diese Daten haben. Es ist eine Ende-zu-Ende-Verschlüsselung vorzusehen. Der Stand der Technik ist bei der Ende-zu-Ende-Verschlüsselung stets zu beachten und umzusetzen. Eine Ausnahme ist für die Überprüfung auf Schadsoftware gestattet . Der Zugriff auf die Metadaten, die beim Austausch von Nachrichten anfallen, ist nur den Berechtigten gestattet.

Bei Verlust des Endgeräts sollte es möglich sein, die Chatverläufe durch die Administration zu löschen.

Cloud-Speicher

Unter einem Cloud-Speicher versteht man in diesem Kontext einen Speicherort und/oder eine Austauschplattform einschließlich integrierter Kollaborationswerkzeuge, wie z.B. Weboffice.

Wird ein Cloud-Speicher als Speicherort genutzt, ist dieser für den schulischen Einsatz in einen

- Verwaltungsbereich und
- einen pädagogischen Bereich

zu unterteilen.

Der Zugang zum Cloud-Speicher und der Zugriff auf Daten, auch auf solche im „Papierkorb“ und in Backups, ist generell in einem **Rollen- und Berechtigungskonzept** restriktiv zu regeln.

Unterteilung des Cloud-Speichers

Die Unterteilung des Cloud-Speichers in einen Verwaltungsbereich und einen pädagogischen Bereich muss nicht durch zwei physisch getrennte Systeme erfolgen, sondern kann auch über ein restriktives Rollen- und Berechtigungskonzept umgesetzt werden.

Sofern die Realisierung des Verwaltungsbereichs über ein restriktives Rollen- und

Berechtigungskonzept erfolgt, müssen die Verzeichnisse, die dem Verwaltungsbereich zugeordnet sein sollen, eindeutig und unterscheidbar bezeichnet werden.

Authentisierung und Datenspeicherung bei physisch getrennten Systemen

Da der Verwaltungsbereich besonders vertrauliche Daten enthalten kann, ist der Zugang zum Verwaltungsbereich mit einer spezifischen Authentisierung (z. B. 2-Faktor-Authentisierung) zu schützen. Die Daten im Ruhezustand müssen im Verwaltungsbereich des Cloud-Speichers **durch eine Verschlüsselung** geschützt werden. Der Stand der Technik ist bei der Verschlüsselung stets zu beachten und umzusetzen. Dies muss durch den Betreiber des Cloudspeichers sichergestellt sein. Liegen beide Bedingungen vor, dürfen Daten mit hohem Schutzbedarf ohne weitere Maßnahmen im Verwaltungsbereich abgelegt werden.

Im pädagogischen Bereich ist eine Verschlüsselung nicht zwingend erforderlich. Diese wird aber empfohlen. Der Zugang zum pädagogischen Bereich kann rollenspezifisch mit einer spezifischen Authentisierung (z. B. 2-Faktor-Authentisierung für Lehrkräfte) geschützt werden.

Authentisierung und Datenspeicherung bei Realisierung über ein Rollen- und Berechtigungskonzept

Der Zugang zum Cloud-Speicher sollte **rollenspezifisch** mit einer spezifischen Authentisierung (z. B. 2-Faktor-Authentisierung für Lehrkräfte) versehen werden.

Die Daten im Ruhezustand müssen im Cloud-Speichers **durch eine Verschlüsselung** geschützt werden. Der Stand der Technik ist bei der Verschlüsselung stets zu beachten und umzusetzen. Dies muss durch den Betreiber des Cloudspeichers sichergestellt sein.

Sofern die Daten im Ruhezustand des Cloud-Speichers nicht **durch Verschlüsselung und mit einer spezifischen Authentisierung** geschützt sind, dürfen Dokumente, die Daten mit hohem Schutzbedarf enthalten, nur verschlüsselt abgelegt werden. Die → Verschlüsselung https://www.km.bayern.de/gestalten/digitalisierung/datensicherheit/verschluesselung ist mit einem Drittprodukt durch den Endanwender umzusetzen.

Cloud-Speicher als Austauschplattform

Die vorangestellten Maßnahmen für den Cloudspeicher sind auch für ausschließliche

Nutzung als Austauschplattform anzuwenden.

Berechtigten Dritten darf der Zugriff auf die Daten nur zeitlich begrenzt (z. B. begrenzte Gültigkeitsdauer oder beschränkte Anzahl an Aufrufen) durch einen Link (für Externe) oder eine Berechtigung erteilt werden. Der Zugriff über einen Link soll passwortgeschützt erfolgen. **Werden Daten mit hohem Schutzbedarf ausgetauscht, muss der Link passwortgeschützt sein.** Die Übertragung des Passworts und des Links müssen über unterschiedliche Kommunikationswege erfolgen.

Cloud-Speicher als Kollaborationswerkzeug

Die vorangestellten Maßnahmen für den Cloudspeicher sind auch für ausschließliche Nutzung als Austauschplattform anzuwenden.

Daten mit hohem Schutzbedarf dürfen kollaborativ verarbeitet werden, sofern sichergestellt ist, dass die Daten während der Bearbeitung **durchgehend verschlüsselt** sind. Eine geeignete Verschlüsselung mit entsprechendem Schutzniveau muss durch den Betreiber des Cloudspeichers sichergestellt sein.

Videokonferenzwerkzeug

Beim Videokonferenzwerkzeug werden organisatorische und technische Mindestanforderungen unterschieden. Die technischen Anforderungen müssen durch den Betreiber des Werkzeugs sichergestellt sein.

Organisatorische Maßnahmen

Der Name des einzurichtenden Videokonferenzraums soll keine identifizierenden Informationen zu Personen oder dem besonders vertraulichen Inhalt enthalten.

Unberechtigter Zugang zur Videokonferenz ist über einen personalisierten Einwahllink oder durch die Aktivierung des Warteraums zu verhindern. Dies gilt insbesondere auch bei Beratung und die Beschlussfassungen schulischer Gremien mittels Videokonferenzen (§ 18a BaySchO).

Die Teilnehmerinnen und Teilnehmer müssen sich angemessen und geeignet authentisieren. Dies kann zum Beispiel mittels Bild- und/oder Tonübertragung erfolgen.

Technische Maßnahmen

Daten mit hohem Schutzbedarf dürfen nur über ein Videokonferenzwerkzeug ausgetauscht werden, wenn eine **hinreichende Absicherung gegen Zugriffe über die Server** des Anbieters vorgesehen ist. Diese Vorgabe gilt als erfüllt, wenn das Videokonferenzwerkzeug zentral vom Freistaat Bayern über das Staatsministerium bereitgestellt wird oder eine Ende-zu-Ende-Verschlüsselung vorsieht, bei der die Schlüssel nur den Berechtigten (Teilnehmern der Videokonferenz) zugänglich sind.

Technische Maßnahmen beim Chat und beim Dateiaustausch innerhalb des Videokonferenzwerkzeugs

Daten mit hohem Schutzbedarf dürfen nur über den Chat und/oder den Dateiaustausch innerhalb des Videokonferenzwerkzeugs ausgetauscht werden, wenn **eine hinreichende Absicherung gegen Zugriffe über die Server des Anbieters** vorgesehen ist. Diese Vorgabe gilt als erfüllt, wenn das Videokonferenzwerkzeug zentral vom Freistaat Bayern über das Staatsministerium bereitgestellt wird oder eine Ende-zu-Ende-Verschlüsselung vorsieht, bei der die Schlüssel nur den Berechtigten (Teilnehmern der Videokonferenz) zugänglich sind.

Zudem müssen nach Beendigung der Videokonferenz der Chat und die ausgetauschten Daten unwiderruflich gelöscht werden.

Besonders zur Geheimhaltung verpflichtete Personen

Besonders zur Geheimhaltung verpflichtete Personen im Schulbereich (z. B. Schulpsychologinnen und Schulpsychologen, Personalräte) stehen nicht nur in der besonderen Verantwortung eines Berufsgeheimnisträgers, sondern haben regelmäßig Umgang mit Daten mit hohem Schutzbedarf. Deren Kommunikation in dieser Funktion unterfällt zusätzlich den nachfolgenden Voraussetzungen, sofern Daten mit hohem Schutzbedarf ausgetauscht werden. Dies gilt entsprechend für Beratungslehrkräfte (vgl. insbesondere Abschnitt III Nr. 4.1. der Bekanntmachung des Bayerischen Staatsministeriums für Unterricht und Kultus über die Schulberatung in Bayern vom 29. Oktober 2001 (KWMBl. I S. 454, StAnz. Nr. 47), die zuletzt durch Bekanntmachung vom 17. März 2023 (BayMBl. Nr. 148) geändert worden ist). Beim Austausch von Daten muss sichergestellt werden, dass diese nur an Personen übertragen werden, denen gegenüber eine Offenlegung der Daten gestattet ist. Die Identität des Kommunikationspartners ist in geeigneter Weise zu

überprüfen.

E-Mail-Kommunikation

Sofern bereits Daten über Sender und/oder Empfänger den Vorschriften zum besonderen strafrechtlichen Geheimnisschutz unterfallen, muss eine Einwilligung ausdrücklich auch diesen Aspekt umfassen.

Eine Kommunikation von Funktionsträgern im Rahmen der entsprechenden Funktion, die einer besonderen Geheimhaltungsverpflichtung unterfallen, hat über ein eigenes, dafür vorgesehenes E-Mail-Postfach zu erfolgen. Dieses Postfach muss nach außen erkennbar der jeweiligen Funktion des Postfachinhabers zugeordnet sein.

Messenger

Sofern bereits Daten über Sender und/oder Empfänger den Vorschriften zum besonderen strafrechtlichen Geheimnisschutz unterfallen, muss eine Einwilligung ausdrücklich auch diesen Aspekt umfassen.

Weitere Teilnehmerinnen und Teilnehmer dürfen nur nach ausdrücklicher Zustimmung der bisherigen Beteiligten in den Chatraum aufgenommen werden.

Nach Abschluss der Kommunikation über eine bestimmte Angelegenheit, ist der Chatverlauf und gegebenenfalls der Chat unverzüglich zu löschen.

Cloud-Speicher

Die im Rahmen der Funktion angelegten Ordner sind speziell zu bezeichnen.

Videokonferenzwerkzeuge

Für jede Sitzung ist ein neuer Videokonferenzraum zu erstellen (Verbot der Doppelnutzung).

Personenbezogene Daten sind nach Beendigung der Sitzung aus der Teilnehmerverwaltung des Videokonferenzwerkzeugs, in der Regel durch Auflösung des Konferenzraums, unverzüglich vom Initiator der Konferenz zu löschen.

Spezielle Regelungen für besondere Personengruppen bleiben unberührt.

FAQ zu diesem Thema

Erfüllen die Kommunktions- und Kollaborationsprodukte (Messenger und Drive) der ByCS die genannten Anforderungen?

Der ByCS-Messenger und ByCS-Drive werden den Schulen kostenfrei vom Freistaat Bayern zu Verfügung gestellt.

Der ByCS-Messenger erfüllt die oben genannten Anforderungen an die Datensicherheit für einen Messenger.

ByCS-Drive erfüllt die oben genannten Anforderungen an die Datensicherheit für den pädagogischen Bereich eines Cloud-Speichers. Werden die Daten vor der Ablage in Drive zusätzlich verschlüsselt, werden auch die Anforderungen an einen Verwaltungsspeicherbereich erfüllt.

Es sollen Daten mit normalen Schutzbedarf an einen Dritten übermittelt werden. Wie ist vorzugehen?

- E-Mail: Beim E-Mail-Versand sind keine weiteren Maßnahmen zu beachten, wenn nicht personenbezogene Daten im Textfeld oder als Anhang übertragen werden (z.B. Einzelnoten). In diesem Fall ist die Vorgehensweise der folgenden beiden FAQs zu beachten.
- Messenger: Die Übertragung über den Messenger ist möglich.
- Kommunikationstool innerhalb einer Schulanwendung: Eine Übertragung ist ohne weitere Maßnahmen möglich, sofern der Zugriff auf die Anwendung passwortgeschützt und verschlüsselt (Transportverschlüsselung) erfolgt. (Siehe hierzu auch: → Verschlüsselung https://www.km.bayern.de/gestalten/digitalisierung/datensicherheit/verschluesselung)

Es sollen Noten an eine andere Lehrkraft übermittelt werden oder ein Notenbild

ausgetauscht werden. Wie ist vorzugehen?

- E-Mail: Bei Einzelnoten ist ein E-Mail-Versand über das dienstliche E-Mail-Postfach ohne weitere Maßnahmen möglich, wenn der Absender und der Empfänger dieselbe E-Mail-Domäne verwenden (z.B. ...@schulen.bayern.de). Notenlisten hingegen haben einen hohen Schutzbedarf und müssen verschlüsselt werden. Das Passwort zum Entschlüsseln wird über einen gesonderten Kommunikationsweg (z. B. Messenger, Telefon) übermittelt. Die Umsetzungshinweise können Sie dem folgenden → OnePager https://www.km.bayern.de/gestalten/digitalisierung/datensicherheit/dienstliche-verwendung-digitaler-kommunikations#downloads entnehmen.
- Messenger: Eine Übertragung per Messenger ist bei Einzelnoten sowie Notenlisten ohne weitere Maßnahmen möglich.
- Kommunikationstool innerhalb einer Schulanwendung: Eine Übertragung ist bei Einzelnoten sowie Notenlisten ohne weitere Maßnahmen möglich, sofern der Zugriff auf die Anwendung passwortgeschützt und verschlüsselt (Transportverschlüsselung) erfolgt. (Siehe hierzu auch: → Verschlüsselung https://www.km.bayern.de/gestalten/digitalisierung/datensicherheit/verschluesselung)

Es sollen Noten an Erziehungsberechtigte übermittelt werden. Wie ist vorzugehen?

- E-Mail: Bei Noten ist beim E-Mail-Versand eine Verschlüsselung notwendig. Die Umsetzungshinweise können Sie dem folgenden → OnePager https://www.km.bayern.de/gestalten/digitalisierung/datensicherheit/dienstliche-verwendung-digitaler-kommunikations#downloads entnehmen.
- Messenger: Eine Übertragung per Messenger ist bei Einzelnoten sowie Notenlisten ohne weitere Maßnahmen möglich.
- Kommunikationstool innerhalb einer Schulanwendung: Eine Übertragung ist bei Einzelnoten sowie Notenlisten ohne weitere Maßnahmen möglich, sofern der Zugriff auf die Anwendung passwortgeschützt und verschlüsselt (Transportverschlüsselung) erfolgt. (Siehe hierzu auch: → Verschlüsselung https://www.km.bayern.de/gestalten/digitalisierung/datensicherheit/verschluesselung)

Die Krankmeldungen der Lehrkräfte und Schüler sollen elektronisch übermittelt werden. Wie ist vorzugehen?

- E-Mail: Krankmeldungen haben einen hohen Schutzbedarf. Die Krankmeldung muss deswegen als Anhang verschlüsselt werden und kann anschließend versendet werden. Die Umsetzungshinweise können Sie dem folgenden → OnePager https://www.km.bayern.de/gestalten/digitalisierung/datensicherheit/dienstliche-verwendung-digitaler-kommunikations#downloads entnehmen.
- Messenger: Die Krankmeldung kann ohne weitere Maßnahmen an den Empfänger versendet werden.
- Kommunikationstool innerhalb einer Schulanwendung: Eine Übertragung ist ohne weitere Maßnahmen möglich, sofern der Zugriff auf die Anwendung passwortgeschützt und verschlüsselt (Transportverschlüsselung) erfolgt. (Siehe hierzu auch: → Verschlüsselung https://www.km.bayern.de/gestalten/digitalisierung/datensicherheit/verschluesselung)

Austausch der Schule zum Gesundheitszustand eines Schülers. Wie ist hier in der Kommunikation vorzugehen?

- E-Mail: Entsprechende Informationen müssen verschlüsselt werden und können anschließend versendet werden. Die Erziehungsberechtigten sind diesbezüglich zu sensibilisieren.
- Messenger: Die entsprechenden Informationen können ohne weitere Maßnahmen übertragen werden.

Bereitstellung eines Protokolls einer Konferenz oder Besprechung. Wie ist hier in der Kommunikation vorzugehen?

Verwaltungsbereich auf physisch getrennten Systemen: Es sind keine weiteren Maßnahmen erforderlich. Die Zugriffsberechtigungen müssen restriktiv eingestellt werden.

Einheitlicher Cloud-Speicher: Das Dokument muss in einem Verzeichnis, das dem Verwaltungsbereich zugeordnet ist verschlüsselt abgelegt werden. Die Zugriffsberechtigungen müssen restriktiv eingestellt werden.

Lehrkräfte tauschen sich bezüglich Unterrichtsplanung aus und teilen Materialien.

- Die Daten haben einen normalen Schutzbedarf und können auf jedem Kommunikations- und Kollaborationswerkzeug ohne weitere Maßnahmen übermittelt werden.

Eine Lehrkraft wendet sich an den Personalrat in einer persönlichen Angelegenheit.

- E-Mail: Für besondere Funktionen in der Schule gibt es Funktions-E-Mailadressen, Bsp.: Schulpsychologe, Beratungslehrkraft oder Personalrat.
  Diese sind getrennt von persönlichen Postfächern zu führen. Diese speziellen Postfächer sind zu adressieren. Die Daten haben einen hohen Schutzbedarf und müssen verschlüsselt werden. Das Passwort zum Entschlüsseln wird über einen gesonderten Kommunikationsweg (z. B. Messenger, Telefon) übermittelt.
- Messenger: Die Übertragung über den Messenger ist möglich.

Was unterscheidet die Kommunikation über E-Mail von der Kommunikation über Messenger?

- E-Mail-Austausch muss als unsicher eingestuft werden, da der Kommunikationspfad nicht vorhersagbar ist und Daten auch unverschlüsselt ausgetauscht werden könnten.
  Eine Ausnahme bildet die Kommunikation über einen Webclient am gleichen Mailsystem (Bsp.: Zwei Lehrkräfte nutzen beide die Dienst-E-Mail der ByCS).
- Messenger bieten meist eine Ende-zu-Ende-Verschlüsselung. Die Nachrichten können in diesem Fall nur durch die beiden Kommunikationspartner im Klartext gelesen werden.

Wann hat ein Videokonferenzwerkzeug eine hinreichende Absicherung?

- Diese Vorgabe gilt als erfüllt, wenn das Videokonferenzwerkzeug zentral vom Freistaat Bayern über das Staatsministerium bereitgestellt wird oder eine Ende-zu-Ende-Verschlüsselung vorsieht, bei der die Schlüssel nur den Berechtigten (Teilnehmern der Videokonferenz) zugänglich sind

Was ist beim Einsatz von M365 an einer Schule zu beachten?

Ein gehärteter M365-Tenant schützt Daten vor unbefugtem Zugriff, verhindert Missbrauch durch eingeschränkte Funktionen und erhöht so die Datensicherheit. Für eine robuste und zuverlässige Grundlage beim schulischen Einsatz von Microsoft 365 stehen nachfolgend ein zip-File mit Anleitung und entsrpechende PS-Skript-Dateien für die IT-Verantworlichen zum Download zur Verfügung, um den M365-Tenant vor der Inbetriebnahme entsprechend zu härten.

M365 Anleitung zur sicheren Konfiguration von M365 an bayerischen Schulen
Version 2.0
/download/4-25-10/2025_Anleitung_zur_sicheren_Konfiguration_von_M365_an_bayerischen_Schulen.jpg

M365 Anhang Gruppenrichtlinien
/download/4-25-10/2025_M365_Anhang_Gruppenrichtlinien.jpg

M365 PowerShell-Skripte zur Umsetzung der Konfigurationsempfehlungen
/download/4-25-10/2025_M365-PowerShell-Skripte.jpg

Zum Juli 2025 wurde die „Anleitung zur sicheren Konfiguration von M365 an bayerischen Schulen“ in einer neuen Version erstellt. Die Änderungen zum Vorgänger-Dokument sind in dem nachfolgend bereitgestellten Dokument zur besseren Nachvollziebarkeit aufgeführt.

M365 Änderungsverlauf zu Version 2.0
/download/4-25-10/2025_%C3%84nderungsverlauf_V2.jpg

Für dem laufenden Betrieb von M365 stellt der Anhang zur „Anleitung zur sicheren Konfiguration von M365 an bayerischen Schulen“ eine Aufgabenliste zur Verfügung.

M365 Anhang Aufgabenliste für den laufenden Betrieb
/download/4-25-10/2025_Anhang_Aufgabenliste_f%C3%BCr_den_laufenden_Betrieb.jpg

FAQs zum Einsatz von M365

Kann man die Administration eines Microsoft-Tenants an einen Dienstleister auslagern?

Ja, die Auslagerung der Administration an einen externen Dienstleister ist möglich. Eine sorgfältige Auswahl des Dienstleisters ist zu beachten, da dieser als Administrator einen Vollzugriff auf den Tenant hat. Zudem muss ein Notfallaccount beim Inhaber des Tenants verbleiben (z.B. Schulträger).

Warum sind M365 A3 Lizenzen den A1 Lizenzen vorzuziehen?

Microsoft365 gliedert sich in verschiedene Dienste, die bekanntesten sind hierbei Office365, Entra (ehemals Azure Active Directory) und Microsoft Intune. Die Lizenzierung der verschiedenen Dienste erfolgt in drei Stufen, A1, A3 und A5. Die kostenlose A1 Lizenzstufe enthält ausschließlich die M365 Apps (z. B. Office) als eingeschränkte Onlinevariante und Basisfunktionen für E-Mail und eingeschränkte Sicherheitsfunktionen besonders im Identitätsmanagement.
In der kostenpflichtigen Microsoft365 A3 Lizenz sind hingegen die Vollversionen der Office-Apps enthalten, sowie die Geräteverwaltung Intune und Windows 11 Education-Lizenzen enthalten. Für die verschiedenen Cloudspeicher steht im Vergleich zur A1 Lizenz mehr Speicherplatz zur Verfügung. Darüber hinaus sind weitergehende Sicherheitsfunktionen im Bereich des Identitätsmanagement Entra enthalten. Die vollzeitbeschäftigten Personen (z. B. Sekretariat, Lehrkräfte) an Schulen werden mit kostenpflichtigen Lizenzen ausgestattet.

Lernende hingegen profitieren vom sog. Student Benefit und können kostenlos mit A3-Lizenzen ausgestattet werden.
Die A5 Lizenz enthält im Wesentlichen noch weitergehende Sicherheitsmöglichkeiten.

Welche Arten von Cloudspeichern gibt es bei Microsoft?

Microsoft bietet verschiedene Cloudspeicherlösungen an. Im schulischen Umfeld sind das OneDrive, OneDrive Business und SharePoint.
OneDrive: Mit einem persönlichen Microsoft-Konto erhält der Nutzende Zugriff auf OneDrive, das sich an Privatpersonen richtet. Es handelt sich um einen persönlichen Cloudspeicher, der es Nutzern ermöglicht, Dateien zu speichern, zu teilen und über das Internet darauf zuzugreifen. OneDrive ist in Windows integriert und bietet nahtlose Synchronisation mit anderen Microsoft-Diensten.
OneDrive for Business: Verfügt eine Schule über einen M365 Tenant und entsprechende Lizenzen, können die Nutzenden mit ihren schulischen Konten OneDrive for Business nutzen. Es handelt sich dabei um eine erweiterte Version von OneDrive. Sie bietet zusätzliche Sicherheits- und Verwaltungstools, um Compliance Anforderungen z. B. von Unternehmen gerecht zu werden.
SharePoint: SharePoint ist ein kollaborativer Cloudspeicher, der vorrangig bei der Nutzung von MS-Teams zum Einsatz kommt. Er ermöglicht es in Teams Dokumente abzulegen, zu teilen und gemeinsam daran zu arbeiten.

Wie ist die Speicherung auf den Cloudspeichern von Microsoft gegen Zugriffe Dritter abgesichert?

Bei der Absicherung der Daten in OneDrive und SharePoint erfolgt sowohl während der Datenübertragung als auch im Ruhezustand auf dem Datenträger. Die Kommunikation mit den Cloudspeichern über das Internet folgt mittels verschlüsselten SSL-/TSL-Verbindungen. Die Daten werden auf BitLocker-verschlüsselten Datenträgern abgelegt. Sie werden in einzelne Blöcke aufgeteilt, die jeweils mit eindeutigen individuellen Schlüsseln verschlüsselt werden. Die Schlüssel werden wiederum verschlüsselt von Microsoft gespeichert.

Wo werden die M365-Dienste betrieben?

Microsoft hat 2023 die Initiative „EU Data Boundary“ gestartet, die darauf abzielt, dass die Daten von europäischen Kunden ausschließlich in Europa verarbeitet und gespeichert werden. Mit der EU Data Boundary sollen europäische Kunden sicherstellen können, dass ihre Daten nicht außerhalb der EU übertragen werden. Das umfasst sowohl Kundendaten, als auch pseudonymisierte personenbezogene Daten und professionelle Servicedaten aus technischen Supportfällen. Die EU Data Boundary umfasst u. a. die Microsoft 365, Microsoft 365 Copilot, Microsoft 365 Copilot Chat, Dynamics 365, Power Platform und viele Azure-Dienste. Die EU Data Boundary ist für Kunden, die eine Rechnungsadresse in der EU haben, standardmäßig für die Microsoft 365 Dienste aktiv.

Ergänzend dazu hat Microsoft die „Microsoft Sovereign Cloud-Initiative“ für alle Kunden in Europa ins Leben gerufen, um u. a. europäischen Behörden (z. B. Schulen) zu helfen, die Anforderungen an Datensouveränität, Sicherheit und Compliance zu erfüllen. Im Bereich der öffentlichen Cloud (Public Cloud) bietet Microsoft die Sovereign Public Cloud an, die eine Datenverarbeitung ausschließlich in europäischen Rechenzentren nach EU-Recht umfasst.

Der Zugriff auf die Infrastruktur wird von Microsoft Mitarbeitern mit Wohnsitz in Europa kontrolliert.

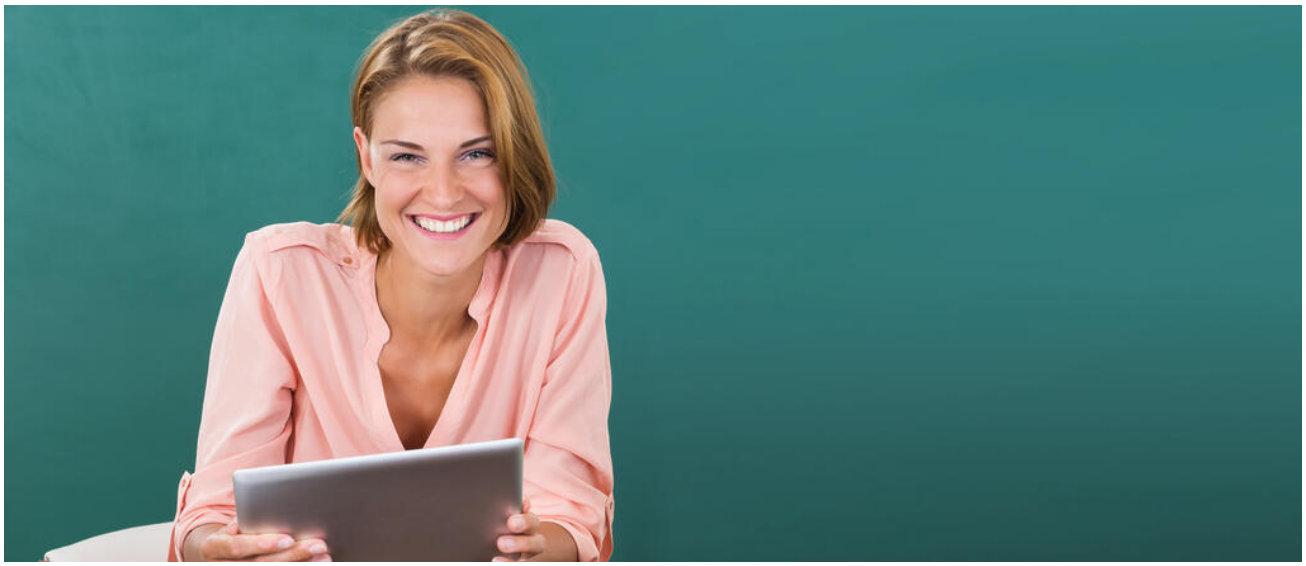
Downloads

Hinweise zur Schutzbedarfsfeststellung
/download/4-24-04/Schutzbedarfsermittlung.jpg

OnePager Sichere E-Mail-Kommunikation
/download/4-24-04/OnePager_sichere_E-Mail-Kommunikation.jpg

Leitfaden „Erkennen einer Phishing-E-Mail
/download/4-24-04/Erkennen_von_Phishing_Mails.jpg

Umgang mit Lehrerdienstgeräten



Standards garantieren einen sicheren Einsatz von digitalen Endgeräten ©Andrey Popov - stock.adobe.com

Ein digitales Endgerät stellt im Schulalltag heutzutage ein zentrales Werkzeug dar, um sowohl die pädagogischen Aufgaben als auch die Verwaltungsaufgaben zu erfüllen. Anliegende Informationen sollen einen sicheren Umgang damit gewährleisten.

Die Funktionsfähigkeit des Endgeräts oder die Vertraulichkeit der verarbeiteten Informationen sind verschiedenen Gefährdungen ausgesetzt, z. B.:

- Schadsoftware
- Unberechtigte Nutzung
- Fehlerhafte Administration
- Fehlerhafte Nutzung

Daher ist es notwendig, die Endgeräte durch geeignete Sicherheitsmaßnahmen angemessen zu schützen und die Benutzer auf Risiken hinzuweisen.

Dies soll durch Nutzungsbedingungen der Schule und Mindestsicherheitsstandards erfolgen.

Nutzungsbedingungen für Lehrerdienstgeräte

Zielgruppen: Schulaufwandsträger, Schulleiter

Adressat: Lehrkräfte bzw. das sonstige an der Schule tätige Personal (Im Folgenden: Nutzer)

Die Musternutzungsbedingungen werden von der Schulleitung ggf. in Zusammenarbeit mit dem Schulaufwandsträger finalisiert (d.h. Ausfüllen der grau hinterlegten Platzhalter, Auswahl der für die konkrete Schule gewählten Alternative). Es wird empfohlen, bei der Finalisierung den Rahmen des Mustertexts und der darin vorgesehenen Optionen beizubehalten.

Die Nutzungsbedingungen werden dem Nutzer bei Ausgabe des Geräts vorgelegt. Die Kenntnisnahme wird durch die Unterschrift der Nutzer dokumentiert. Das unterschriebene Dokument wird zu Dokumentationszwecken in der Schule veraktet.

Nutzungsbedingungen für Lehrerdienstgeräte
/download/4-24-06/Nutzungsbedingungen-f%C3%BCr-Lehrerdienstger%C3%A4te_2.0_240311.jpg

Mindestsicherheitsstandards

Zielgruppen: Nutzer, Systemadministratoren, Sachaufwandsträger

Mindestsicherheitsstandards stellen einen Sicherheitsrahmen dar, um die Endgeräte vor Angriffen von außen zu schützen.

Mindestsicherheitsstandards beim Einsatz der dienstlichen Geräte
/download/4-23-12/Mindestsicherheitsstandards-beim-Einsatz-der-dienstlichen-Geraete.jpg

Checklisten

Zielgruppen: Schulleitung, Schulaufwandsträger

Die ausgefüllte Checkliste spiegelt die von der Schule umgesetzten technisch-organisatorischen Maßnahmen wider. Sie muss für jeden Endgerätetyp, der bei der Schule als Dienstgerät ausgegeben wird, von der Schule ausgefüllt und veraktet werden.

Die Checkliste dient den Schulen dadurch als Nachweis, dass sie ihrer Rechenschaftspflicht

nach Art. 5 i.V.m. Art. 32 DSGVO nachgekommen sind.

Checkliste Lehrerdienstgeräte
/download/4-23-12/Muster-einer-Checkliste-Schule.jpg

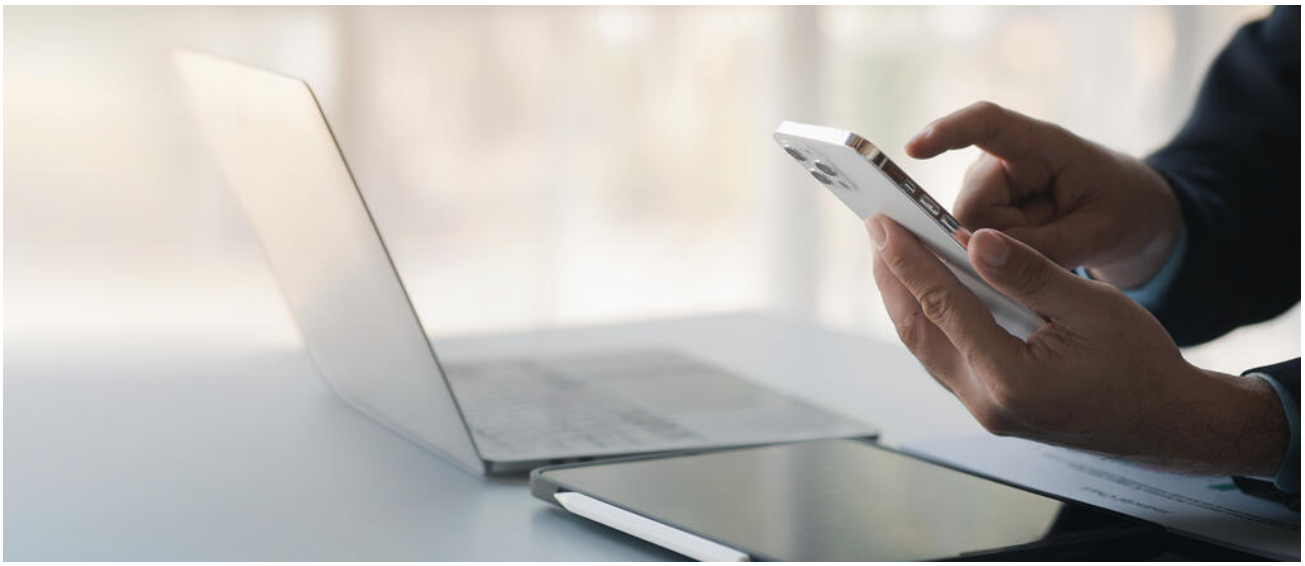
Beim Ausfüllen der Checkliste kann sich die Schulleitung an den folgenden Empfehlungen des Staatsministeriums für Unterricht und Kultus orientieren:

Empfehlung des StMUK für die Schule
/download/4-24-02/Empfehlungen-des-StMUK-Lehrerdienstger%C3%A4te.jpg

Beim Ausfüllen der Checkliste kann sich die Schulleitung am nachfolgenden Beispiel orientieren:

Checkliste (Beispiele)
/download/4-24-02/Beispiel-einer-Checkliste-f%C3%BCr-ein-mobiles-Lehrerdienstger%C3%A4t.jpg

Mobile Device Management



Durch Mobile Device Management lässt sich Geräteverwaltung vereinfachen. ©PhotosD - stock.adobe.com

Allgemein

Ein Mobile Device Management (MDM-System) ist eine zentrale Anwendung zur Verwaltung mobiler Endgeräte wie Tablets oder Laptops. Mit einem MDM-System können IT-Verantwortliche mobile Endgeräte aus der Ferne konfigurieren, steuern und absichern. Dies umfasst unter anderem

- die Ersteinrichtung und Inventarisierung der Geräte,
- die Konfiguration der Geräte,
- das Einrichten von Netzwerkzugängen,
- die zentrale Installation und Deinstallation von Anwendungen (Apps) sowie
- das Verteilen von System- und Softwareupdates.

Ein wesentlicher Vorteil beim Einsatz eines MDM-Systems liegt in der Effizienz und Sicherstellung der passgenauen Geräteeinstellungen. MDM-Systeme ermöglichen es, unterschiedliche Nutzergruppen – wie beispielsweise Schüler und Lehrkräfte – mit maßgeschneiderten Profilen auszustatten. Während Schülergeräte während der Unterrichtszeit beispielsweise nur eingeschränkt nutzbar sind, behalten Lehrkräfte vollen Zugriff auf ihre digitalen Werkzeuge. Gleichzeitig kann das MDM-System Daten, etwa durch die Möglichkeit, verlorene Geräte zu sperren oder zu löschen, schützen. Auch

datenschutztechnische Anforderungen lassen sich mit einem MDM einfacher erfüllen, da beispielsweise private und schulische Inhalte strikt voneinander getrennt werden und die Geräte gemäß dem Prinzip der Datensparsamkeit konfiguriert werden können. Eine Verwaltung der Endgeräte durch die Schule selbst ist ebenso denkbar wie die Verwaltung durch den Schulaufwandsträger oder einer beauftragten Firma.

Hinweis

Entgegen der verbreiteten Meinung ist über ein MDM-System kein Zugriff auf lokal oder in einer Cloud gespeicherte Inhaltsdaten, wie Fotos, Videos, Browser- und Suchverläufe, private Dokumente o. ä. möglich. Auch die Inhalte von App-Daten (z.B. Chats) können über ein MDM-System nicht eingesehen werden.

Trotz dieser Vorteile bringt der Einsatz von MDM-Systemen auch einige Herausforderungen mit sich. An Schulen müssen technische Lösungen mit pädagogischen Anforderungen und Datenschutzrichtlinien in Einklang gebracht werden.

Die Einrichtung und Pflege eines MDM-Systems erfordert nicht nur technisches Know-how, sondern auch klare Abstimmungen innerhalb der Schulfamilie, sowie zwischen der Schulleitung, den IT-Verantwortlichen und Schulaufwandsträgern. Auch die Vielfalt der eingesetzten Endgeräte und Betriebssysteme stellt Schulen vor die Aufgabe, einheitliche Standards zu schaffen, ohne die individuelle Nutzung zu stark zu begrenzen.

Checkliste und Dokumente

Da beim Einsatz eines MDM-Systems viele verschieden Aspekte zu berücksichtigen sind, stellt das StMUK eine **Checkliste** zum Download bereit. Sie dient als Übersicht und kann gleichzeitig zu Dokumentationszwecken verwendet werden.

Zusätzlich finden sich hier auch weitere Dokumente zur **Information der Erziehungsberechtigten** zum Einsatz eines MDM.

Zielgruppe: Schulleitungen, pädagogische Systembetreuer, örtliche Datenschutzbeauftragte

Checkliste zum Einsatz eines MDM-Systems
/download/4-25-09/251106_MDM_Checkliste.jpg

Muster Elternanschreiben zum Einsatz eines MDM-Systems
/download/4-25-09/250911_MDM_Muster-Elternanschreiben.jpg

Elterninformation zum MDM
/download/4-25-09/250611_MDM_Elterninformation.jpg

Elterninformation zum MDM (einfache Sprache)
/download/4-25-09/250611_MDM_Elterninformation_einfache-Sprache.jpg

Eine **Muster-Verarbeitungsbeschreibung** ist im Schulportal hinterlegt.

Auswahl eines MDM-Systems

Im Bereich der mobilen Endgeräte gibt es unterschiedliche Betriebssystemhersteller: Insofern werden MDM-Systeme in zwei Arten eingeteilt:

- **Spezialisierte Lösungen**, die nur **ein Betriebssystem** unterstützen, und
- **Generalistische Lösungen**, die **mehrere Betriebssysteme** unterstützen.

Ein MDM-System muss zu den individuellen technischen Rahmenbedingungen der Schule passen. Diese gilt es gemeinsam mit dem Schulaufwandsträger zu analysieren, um anschließend ein für die Schule passendes System auszuwählen. Die Beratung für digitale Bildung kann dabei unterstützen.

Die verschiedenen MDM-Systeme unterscheiden sich zum Teil erheblich in ihren Funktionalitäten. Die nachfolgenden **Kriterien** an ein MDM-System sollen bei der Auswahlentscheidung unterstützen:

Kriterien zur Auswahl eines MDM-Systems

Datenschutzkonformität: Das gewählte MDM-System muss den datenschutzrechtlichen Anforderungen des Grundsatzes der Erforderlichkeit, der Rechtmäßigkeit der Datenverarbeitung, der Zweckbindung, der Datenminimierung und der Transparenz entsprechen. Zudem sollte stets geprüft werden, ob sogenannte souveräne bzw. in der EU ansässige Anbieter in Betracht gezogen werden können. Der Anbieter muss offenlegen, in welcher Form welche Drittanbieter, Sub- und Nachunternehmer an der Erbringung des

Dienstangebotes vertraglich und funktional beteiligt sind.

Möglichkeit der Registrierung von persönlichen und schulischen Endgeräten im MDM-System: Viele Betriebssysteme ermöglichen die Registrierung eines Endgeräts als persönliches Gerät in einem MDM-System, was die Trennung von privaten und schulischen Daten erleichtert. Privat installierte Apps sind dabei über das MDM i. d. R. nicht sichtbar. Für die Integration in das MDM-System sind schulische Konten erforderlich, die parallel zu privaten Konten genutzt werden können.

Funktion zur Bildung von (dynamischen) Gerätegruppen: Endgeräte werden zur Verteilung von schulischen Anwendungen und Richtlinien (Profilen) in Gerätegruppen eingruppiert. Die Zuteilung erfolgt optimalerweise automatisiert mit Hilfe von Zuordnungsregeln. Typische Gerätegruppen wären z. B. Lehrergeräte, Schülergeräte, klassenspezifische Gerätegruppen.

Möglichkeit des temporären Ausspielens von Richtlinien (z. B. Einschränkungen) auf das Endgerät während der Unterrichtszeit: Bei elternfinanzierten Endgeräten soll außerhalb der Unterrichtszeit eine private Nutzung möglich sein. Aus diesem Grund sind administrative Vorkehrungen zu treffen, damit etwaig vorhandene während der Unterrichtszeit geltende Restriktionen aufgehoben werden. Folgende Möglichkeiten stehen hierfür zur Verfügung:

- zeitgesteuert
- standortbezogen (z. B. per GPS)
- netzwerkbezogen (z. B. im schulischen WLAN)
- benutzerbezogen
- App-gesteuert

Anfallende Lizensierungskosten: Bei der Auswahl eines MDM-Systems sollte darauf geachtet werden, welche Arten von Lizenzen angeboten werden (z. B. jährliche, dauerhafte) und ob weitere Kosten (z. B. einmalig anfallende Kosten, Kosten für das Hosting) anfallen. Darüber hinaus müssen ggf. vergaberechtliche Aspekte in Abstimmung mit dem Schulaufwandsträger bedacht werden.

Möglichkeit der Nutzung einer Testumgebung: Die Verwaltung von mobilen Endgeräten ist eine administrative Tätigkeit, die eine konzeptionelle Vorarbeit erfordert. Die vorher genannten Anforderungen können nur im Rahmen einer Teststellung getestet werden und mit weiteren schulischen Anforderungen überprüft werden. Eine Teststellung ist i. d. R. über den Hersteller kostenlos einrichtbar. Teststellungen sind zeitlich oder gerätebezogen begrenzt, jedoch nicht im Funktionsumfang.

Hosting: Viele MDM-Systeme sind als reine Cloud-Lösungen konzipiert, bieten aber auch die Möglichkeit eines lokalen Betriebs in einem eigenen Rechenzentrum (On-Premises). Cloudbasierte MDM-Systeme bieten Kosteneinsparungen und Flexibilität, während On-Premises-Lösungen mehr Kontrolle und Sicherheit bieten können. Der Serverstandort soll, unabhängig vom gewählten Hosting-Modell, innerhalb Deutschlands oder der EU liegen.

optionale Funktionalitäten: Integriertes Ausleihsystem, eigene pädagogische Anwendungen, Verwaltung von weiteren Geräten, wie z. B. Displays, Möglichkeit der Konfiguration von

Anwendungen (z. B. Browser)

Zudem sind Anforderungen an die Datensicherheit zu berücksichtigen. Diese sind insbesondere die nachfolgend genannten:

Anforderungen an die Datensicherheit

Nachweis der IT-Sicherheit: Der Anbieter muss in geeigneter Form nachweisen, dass er ein Informationssicherheitsmanagementsystem betreibt. Bei Betrieb des MDM-Systems in der Cloud muss dieses auch die Sicherheit der Cloud umfassen.

Rollen und Berechtigungen: Das MDM-System soll über ein vordefiniertes Rollen- und Berechtigungskonzept verfügen. Der administrative Zugriff soll granular einstellbar sein, damit auch verschiedene Berechtigungsstufen abgebildet werden können.

Sichere Authentifizierung: Authentifizierungsvorgänge müssen mittels MFA möglich sein und dürfen nur über TLS-verschlüsselte Kanäle erfolgen.

Mandantentrennung: Der Anbieter muss bei Nutzung die vollständige Trennung der mandantenbezogenen Daten gewährleisten.

Patchmanagement: Der Anbieter muss gewährleisten, dass sicherheitsrelevante Updates (Sicherheitspatches) für Komponenten in seinem Verantwortungsbereich zeitnah eingespielt werden.

Betrieb eines MDM-Systems

Konfiguration des MDM-Systems

Bei der Inbetriebnahme muss die Schule ggfs. in Abstimmung mit dem Schulaufwandsträger oder einem externen Dienstleister ein Rollen- und Berechtigungskonzept nach dem → „Least Privilege“ und „Need to know“ Prinzip https://www.km.bayern.de/gestalten/digitalisierung/datensicherheit/berechtigungsmanagement festlegen. Bei einem Mehrmandanten-Einsatz muss sichergestellt werden, dass eine klare Trennung zwischen den Mandaten stattfindet. Administratoren eines Mandaten dürfen keine Daten eines anderen Mandaten sehen können. Ausnahmen hiervon sind z. B. für Administratoren möglich, die mehrere Mandanten zentral verwalten.

Der Zugriff auf die (Web-)Oberfläche des MDM-Systems muss nach aktuellen Sicherheitsstandards erfolgen. Für Administratoren muss eine Zwei-Faktoren-Authentifizierung verfügbar sein. Um Zugriff auf App-Marktplätze zu erhalten, muss das MDM-System mit dem Bildungsaccount der Schule bei den Betriebssystemherstellern verbunden werden.

Registrierungsmöglichkeiten der Endgeräte im MDM-System

Bei der Registrierung der mobilen Endgeräte im MDM-System (dem Enrollment) sind grundsätzlich zwei Möglichkeiten zu unterscheiden:

- Registrierung als schuleigenes Gerät (Umfängliche Verwaltung oder Vollverwaltung)
- Benutzergesteuerte Registrierung als persönliches Gerät (Eingeschränkte Verwaltung oder Teilverwaltung)

Daraus ergeben sich verschiedene Steuerungsmöglichkeiten, die im Folgenden kurz dargelegt werden sollen.

Enrollment als schuleigenes Endgerät (z. B. Leihgeräte, Lehrergeräte, Ausbildungsgeräte)

Bei der Vollverwaltung wird das Endgerät umfangreich durch die Schule bzw. den Schulaufwandsträger verwaltet. Im Normalfall wird es zuerst im zentralen Bildungsaccount der Schule hinterlegt. Anschließend werden die Endgeräte automatisch im MDM-System der Schule registriert und können anschließend umfangreich verwaltet werden. Der Nutzende kann normalerweise nicht eigenständig die MDM-Verwaltung verlassen. Es sind dann u. a. folgende administrative Tätigkeiten möglich:

Automatische Ersteinrichtung des Endgeräts („Zero-Touch“) Installation von Betriebssystemupdates Installation von Anwendungen und -updates Ausspielen von Gerätekonfigurationen (z. B. Netzwerkeinstellungen, notwendige Zertifikate) Installation von befristeten Geräteeinschränkungen Ausblenden von nicht-unterrichtlichen Anwendungen Zurücksetzen und Neueinrichtung des mobilen Endgeräts Lösen von Gerätesperrungen (z. B. per Bildschirmcode) Remote-Sperren und Orten des (mobilen) Endgeräts

Benutzergesteuertes Enrollment (z. B. für private bzw. elternfinanzierte Geräte)

Das mobile Endgerät wird als persönliches Endgerät mit Hilfe eines schuleigenen Benutzerzugangs beim MDM-System der Schule direkt registriert. Das Betriebssystem richtet dann einen persönlichen und schulischen Bereich ein, die voneinander getrennt sind. Über das MDM können dann u. a. folgende administrative Tätigkeiten ausgeführt werden:

Installation von Anwendungen und -updates Installation von Betriebssystemupdates Ausspielen von Gerätekonfigurationen (z. B. Netzwerkeinstellungen, notwendige Zertifikate) Installation von befristeten Geräteeinschränkungen

Das Verlassen des MDM-Systems ist jederzeit möglich. Eine Zurücksetzung des mobilen Endgeräts ist nicht notwendig. Schulische Daten sollten vorher gesichert werden, da es ansonsten zu einem Datenverlust kommen kann. Nach dem Verlassen des MDM-Systems ist der Zugriff auf die schulischen Anwendungen nicht mehr möglich, und diese werden vom mobilen Endgerät automatisch entfernt.

Zusammenspiel zwischen MDM-System und Schulkonten der Betriebssystemhersteller

Für eine sinnvolle Administration der mobilen Endgeräte ist ein entsprechender Bildungsaccount bei den Betriebssystemherstellern (z. B. Apple School Manager, Google Workspace und Microsoft 365 Tenant) anzulegen. Dadurch erhält die Schule Zugriff auf die herstellereigenen App-Marktplätze, der für die Verteilung der Anwendungen an die mobilen Endgeräte Voraussetzung ist. Die Schule erhält so die Möglichkeit von Bildungsrabatten zu profitieren und kann Volumenlizenzen für Anwendungen erwerben. Die mobilen Endgeräte sollten bei einem zertifizierten Bildungshändler des Betriebssystemherstellers gekauft werden, da diese Händler dazu berechtigt sind, die beschafften mobilen Endgeräte direkt im Bildungsaccount zu hinterlegen und fest mit diesem zu verknüpfen. Ebenfalls kann über diese Händler auch notwendiges Guthaben für den Kauf von kostenpflichtigen Anwendungen aus dem App-Store erworben werden.

Innerhalb der Schulaccounts können schuleigene Cloud-Accounts zur Anmeldung auf den mobilen Endgeräten eingerichtet und verwaltet werden. Hierbei sind die datenschutzrechtlichen Anforderungen zu beachten.

Das gewählte MDM-System wird mit dem Bildungsaccount der Schule verbunden. Anschließend können die hinterlegten Endgeräte, die lizensierten Anwendungen sowie etwaige Schulaccounts dem MDM zur zentralen Verwaltung zugewiesen werden. Es ist darauf zu achten, dass die notwendigen Zertifikate (Tokens) und Lizenzen rechtzeitig erneuert werden. Die Kommunikation zwischen Bildungsaccount und MDM-System erfolgt

verschlüsselt.

Entfernen von Endgeräten aus dem MDM-System

Beim Entfernen der mobilen Endgeräte aus dem MDM-System muss wieder zwischen voll- bzw. teilverwalteten Geräten unterschieden werden.

Vollverwaltete Endgeräte sind stärker mit der MDM-Lösung und dem Bildungsaccount verzahnt, weswegen eine Loslösung nicht ohne weiteres möglich ist und eine Zurücksetzung des mobilen Endgeräts regelmäßig erforderlich ist. Deswegen sollten zuerst lokal gespeicherte Daten vom mobilen Endgerät gesichert werden. Anschließend wird das mobile Endgerät auf die Werkseinstellungen zurückgesetzt und alle Daten vom Endgerät gelöscht (Enterprise-Wipe). Das kann über das MDM oder manuell am Endgerät über die Rücksetzungsfunktionen erfolgen. Im nächsten Schritt wird das mobile Endgerät aus dem MDM und dem Bildungsaccount der Schule gelöscht.

Bei **teilverwalteten Endgeräten** kann das MDM-System direkt, durch Entfernen des Schulaccounts verlassen werden.

Konfiguration der Endgeräte

Endgeräte sollen so konfiguriert sein, dass sie das erforderliche Schutzniveau angemessen erfüllen. Dafür muss eine passende Grundkonfiguration der Sicherheitsmechanismen und -einstellungen zusammengestellt und dokumentiert werden. Nicht benötigte Funktionen sollten deaktiviert werden.

Die untenstehende Excel-Tabelle bildet für verschiedene Endgeräte Konfigurationsempfehlungen ab. Die Tabelle kann an die Gegebenheiten der Schule angepasst und beispielsweise ergänzend dem Elterninformationsschreiben als Anhang hinzugefügt werden.

Zielgruppe: pädagogischer Systembetreuer, MDM-Administrator

Konfigurationsempfehlungen für verschiedene Endgeräte
/download/4-25-09/250911_MDM_Ger%C3%A4tekonfiguration.jpg

FAQ zu MDM-Systemen

Welche Arten von Konten können für die Anmeldung auf Endgeräten verwendet werden?

Zur Anmeldung auf Endgeräten (z. B. Notebook, Desktop-PC, Tablet) kommen **Cloud-Konten** und **lokale Konten** in Frage.

Cloud-Konten können bei Microsoft (Windows), Apple (iPadOS, macOS) oder Google (Android, ChromeOS) für die Anmeldung auf dem Endgerät angelegt werden.

Lokale Konten können für Windows, Linux oder macOS angelegt werden.

Welche Konten kommen in windowsbasierten Domänen zum Einsatz?

Windows-basierte Endgeräte werden im Schulumfeld häufig in Windows-Domänen eingebunden und werden damit Teil eines lokalen Verzeichnisdienstes (Active Directory). Diese Strukturen können über den Entra-Connect-Dienst auch mit dem Cloud-Identitätsdienst Microsoft Entra aus der Microsoft-Cloud verbunden werden. Die lokalen Benutzerkonten aus dem Active Directory werden anschließend in die Cloud synchronisiert und können für die Anmeldung an Windows und den Microsoft365-Diensten verwendet werden.

Welche Arten von Cloud-Konten gibt es und welche Unterschiede zwischen Ihnen bestehen?

Bei Cloud-Konten kann zwischen **persönlichen** und **schulischen Konten** unterschieden werden. Ein persönliches Cloud-Konto wird mit einer persönlichen Mail-Adresse von den Nutzenden selbstständig angelegt. Die Verwaltung des Kontos liegt in der Verantwortung des Nutzenden. Neben der Anmeldung auf dem Endgerät dienen persönliche Konten als Zugang zu herstellereigenen Apps-Stores, können für Familienfunktionen oder zur Anmeldung bei Herstellerdiensten (z. B. Cloud-Dienste oder zur Ortung des eigenen Endgeräts) verwendet werden.

Schulische Cloud-Konten werden von der Schule mit einer schulischen Mail-Adresse angelegt. Die Verwaltung des Kontos wird durch die zuständige IT-Administration der Schule sichergestellt. Die Konten werden zur Anmeldung auf schulischen Endgeräten verwendet und können auch zur Lizenzierung von schulischen Anwendungen eingesetzt werden. Zu

beachten ist, dass die IT-Administration keinen Zugriff auf Inhaltsdaten (z. B. Suchverläufe, Fotos oder Videos) der Nutzenden hat.

Was ist beim Einsatz eines Geräts zu beachten, welches von mehreren Personen genutzt wird?

Bei Endgeräten, die von mehreren Personen verwendet werden, gilt es, der Datensicherheit und dem Datenschutz ein besonderes Augenmerk zu schenken. So muss sichergestellt werden, dass auf sensible Daten, wie z. B. Fotos, Videos, Browser- und Suchverläufe, kein anderer Nutzer Zugriff hat. Das kann technisch durch geeignete Nutzungskonzepte, wie z. B. durch den Gastmodus erreicht werden. Bei diesem Modus werden alle während der Sitzung generierten lokale Daten nach der Abmeldung verworfen und gelöscht. Eine organisatorische Maßnahme wäre die feste Zuweisung eines (mobilen) Endgeräts an einen Lernenden. Alternativ können auch unterschiedliche personalisierte Accounts zur Anmeldung auf dem Endgerät zum Einsatz kommen. Die lokal gespeicherten Daten sind dann nur für den jeweils angemeldeten Nutzenden zugreifbar.

Was ist der Vorteil bei der Nutzung von App-Stores der Hersteller?

Die klassischen App-Stores wie der Apple App Store oder Google Play Store garantieren einen hohen Schutz durch strenge Prüfungen und Überwachung aller angebotenen Apps. Zudem erhält die Schule einen besseren Überblick über die eingesetzten Apps und profitiert von Bildungskonditionen.

Was ist der Unterschied zwischen einem MDM-System und einem Classroom-Management-System?

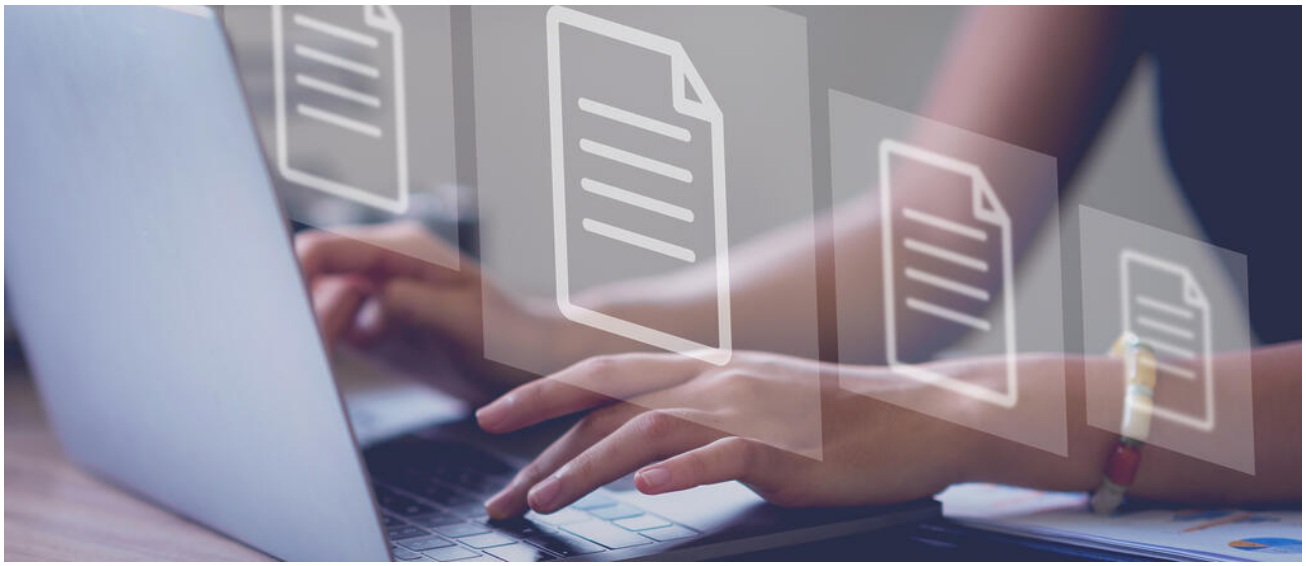
MDM-Systeme und Classroom-Management-Systeme werden oft in einem Atemzug genannt. Es handelt sich aber um verschiedene Werkzeuge, die unterschiedliche Aufgaben erfüllen und sich an unterschiedliche Zielgruppen richten.

Mit einem MDM-System können **IT-Verantwortliche** teilnehmende Geräte zentral verwalten – das umfasst das Einrichten, Aktualisieren, Installieren von Apps und Durchsetzen von Sicherheitsregeln für alle Tablets oder Laptops in einer Schule. MDM sorgt also dafür, dass alle Geräte grundsätzlich sicher und einsatzbereit sind.

Ein Classroom-Management-System (z. B. Apple Classroom, Veyon) richtet sich vor allem an

Lehrkräfte, um während des Unterrichts die Steuerung der Schülergeräte zu ermöglichen. Damit können zum Beispiel die Bildschirme aller Tablets auf eine bestimmte App beschränkt, einzelne Geräte gesperrt oder Bildschirminhalte von Einzelgeräten für die Klasse projiziert werden. Ziel ist es, den Unterricht zu steuern und Störungen vorzubeugen.

Nutzungsordnung



Eine Nutzungsordnung verschafft Klarheit über Verantwortung und Zuständigkeiten ©Premreuthai - stock.adobe.com

Eine Nutzungsordnung verschafft Klarheit über die Verantwortlichkeiten der verschiedenen Nutzergruppen. Sie gibt jeweils den Rahmen, die Bedingungen und Regeln vor, um eine möglichst sichere Nutzung der schulischen IT-Infrastruktur zu gewährleisten. Jede Schule muss sich verpflichtend eine Nutzungsordnung geben.

Mit der Bekanntmachung https://www.gesetze-bayern.de/Content/Document/BayVV_2010_K_13179 des Bayerischen Staatsministeriums für Unterricht und Kultus über die Hinweise zur Nutzung der IT-Infrastruktur und des Internetzugangs an Schulen (Schulische IT-Infrastruktur und Internetzugang) vom 14. Juli 2022 wird ein Muster für eine entsprechende Nutzungsordnung zur Verfügung gestellt. Darin sind teils verpflichtende, teils optionale Bausteine enthalten. Es ist in einen allgemeinen Teil und jeweils einen spezifischen Teil für Schülerinnen und Schüler sowie Lehrkräfte gegliedert. Das Musterdokument soll das Erstellen einer bedarfsgerechten Nutzungsordnung der jeweiligen Schule erleichtern, indem beispielsweise Regelungen zum Zugang, insbesondere zu den schulischen Netzen, der Gestattungsrahmen privater Nutzung und die Verantwortlichkeiten und Aufgaben der Zuständigen vor Ort abgedeckt werden.

Dieses Musterdokument, sowie die dazugehörigen Erklärungen der Kenntnisnahme können nachfolgend herunter geladen werden.

Downloads

Muster-Nutzungsordnung (Anlage 1 zu KMBek)
/download/4-24-10/1.1_Anlage_zur_KMBek__Muster_f%C3%BCr_eine_Nutzungsordnung.jpg

Erklärung Schülerinnen und Schüler (Anhang 1 zu Anlage 1 zu KMBek)
/download/4-24-10/1.2_Anhang_1_zur_Anlage_zur_KMBek__Erkl%C3%A4rung_f%C3%BCr_Sch%C3%BClerinnen_und_Sch%C3%BCler.jpg

Erklärung Lehrkräfte (Anhang 2 zu Anlage 1 zu KMBek)
/download/4-24-10/1.3_Anhang_2_zur_Anlage_Erkl%C3%A4rung_f%C3%BCr_Lehrkr%C3%A4fte_und_sonstiges_an_der_Schule_t%C3%A4tiges_Personal.jpg

Private Endgeräte im Dienstgebrauch

Unter bestimmten Voraussetzungen ist der Einsatz privater Endgeräte in Schulen möglich. ©Svitlana - stock.adobe.com

Umgang mit schulfremden Dienstgeräten

Die hier bereitgestellten Vorgaben und Formulare gelten ebenso für Dienstgeräte anderer Organisationen, die in der Schule zum Einsatz kommen. Die Formulare können entsprechend angepasst werden.

Zulassung

Für die Organisation dienstlicher Abläufe und damit auch die Ausgestaltung von IT-gestützten Prozessen, die für dienstliche Zwecke genutzt werden, ist die Schule verantwortlich. Dies gilt ggf. auch für die Entscheidung, private Geräte zur dienstlichen Nutzung zuzulassen.

Ob und inwieweit private Endgeräte für dienstliche Zwecke verwendet werden dürfen, insbesondere bei der Verarbeitung personenbezogener Daten, **entscheidet die Schulleiterin oder der Schulleiter** (vgl. § 27 Abs. 7 LDO https://www.gesetze-bayern.de/Content/Document/BayVwV288393-27). Die Entscheidung umfasst auch die Festlegung, welche **Anwendungen** hierbei genutzt werden

dürfen (z. B. durch Führen einer Softwareliste).

Zielgruppe: Schulleitung

Adressat: Lehrkraft bzw. das sonstige an der Schule tätige Personal

Regelungen:

KMBek zum Vollzug des Datenschutzrechts an staatlichen Schulen vom 14. Juli 2022, Nr. 3.2.4
https://www.gesetze-bayern.de/Content/Document/BayVV_204_K_13178/true

Bayerisches Schulportal
Das Muster für eine Datenschutz-Geschäftsordnung für Schulen ist für die Schulleitungen im Schulportal abrufbar.
https://portal.schulen.bayern.de/my.policy

Private Endgeräte (z. B. Laptop, Smartphone), auf welchen für dienstliche Zwecke personenbezogene Daten gespeichert werden, sind vor der erstmaligen Nutzung der Schule **anzuzeigen**.

Hierfür geben die Lehrkräfte, die private Endgeräte nutzen, die **„Erklärung zur dienstlichen Nutzung privater Endgeräte“** ab. Nähere Informationen zur Anzeigepflicht enthält die Datenschutz-Geschäftsordnung der Schule (vgl. Anlage 5 Nr. 3 Muster-DS-GO).

Erklärung zur Nutzung privater Endgeräte für dienstliche Zwecke
/download/4-24-02/Erkl%C3%A4rung_zur_Nutzung_privater_Endger%C3%A4te_f%C3%BCr_dienstliche_Zwecke_240930.jpg

Erklärung zur Nutzung privater Endgeräte für dienstliche Zwecke
/download/4-24-02/Erkl%C3%A4rung_zur_Nutzung_privater_Endger%C3%A4te_f%C3%BCr_dienstliche_Zwecke_240930.jpg

Die Schulleitung oder eine von ihr beauftragte Person belehrt und informiert die Lehrkräfte und das sonstige an der Schule tätige Personal in geeigneter Weise über die Voraussetzungen der Nutzung privater Endgeräte für dienstliche Zwecke.

Mindestsicherheitsstandards

Um die **erforderliche Datensicherheit zu gewährleisten**, müssen alle privaten Endgeräte **bestimmte Sicherheitsstandards** erfüllen. Sofern die Schule keine weiterreichenden Sicherheitsstandards festgelegt hat, sind dies die vom StMUK aufgestellten

Mindestsicherheitsstandards .

Mindestsicherheitsstandards
/download/4-24-02/Mindestsicherheitsstandards_Stand_20.09.2023.jpg

Datenschutzrechtliche Verantwortung

Die datenschutzrechtliche Verantwortung der Schule erstreckt sich nach § 2 Abs. 1 Muster-Datenschutz-Geschäftsordnung ausdrücklich auch auf den Umgang von Lehrkräften mit im schulischen bzw. dienstlichen Zusammenhang verarbeiteten personenbezogenen Daten auf deren privaten Endgeräten.
Daher wird auch für diesen Fall explizit auf die Geltung der Datenschutz-Geschäftsordnung der Schule hingewiesen und insbesondere auf das Verfahren nach § 10 Muster-DS-GO für den Fall einer Verletzung des Schutzes personenbezogener Daten.

FAQs

Muss das private (Mobil-)Telefon angezeigt werden, wenn darüber dienstliche Gespräche geführt werden?

Verwendet man den häuslichen Telefonanschluss oder das private Smartphone lediglich für dienstliche Telefonate (z.B. Reisebüro: Ticketdaten wegen eines Schüleraustauschs; während eines Wandertags/Studienfahrt müssen Eltern angerufen werden (Zeckenbiss, Erkrankung, Abholen lassen)) muss das Telefon bzw. das Smartphone nicht angezeigt werden, da auf dem Endgerät keine lokale Datenverarbeitung erfolgt.

Muss das private Endgerät auch angezeigt werden, wenn Anwendungen, wie beispielsweise WebUntis damit verwendet werden?

Anwendungen wie WebUntis verarbeiten personenbezogene Daten (unter anderem Name, Klasse, Abwesenheiten, etc.). Daher ist eine Anzeige notwendig, sofern diese auf privaten Geräten eingesetzt werden.

Auch bei der Nutzung von solchen Anwendungen über den Browser können beispielsweise Berichte heruntergeladen werden, die personenbezogene Daten enthalten.

In diesem Kontext empfehlen wir, in der Erklärung unter Ziffer 2 die **zweite** Alternative anzukreuzen und die entsprechende Anwendung (z. B. WebUntis (über Webbrowser oder native App)) zu nennen.

Umgang mit Schülerleihgeräten

Standards garantieren einen sicheren Umgang mit Schülerleihgeräten ©Drazen - stock.adobe.com

Die vorliegenden Nutzungsbedingungen für Schülerleihgeräte sollen den Einsatz in der Schule ermöglichen.

Zielgruppe: Schulaufwandsträger, Schulleitung, Lehrkraft

Adressat: Erziehungsberechtigte, Schülerinnen und Schüler

Die Musternutzungsbedingungen werden von der Schulleitung ggf. in Zusammenarbeit mit dem Schulaufwandsträger finalisiert (d. h. Ausfüllen der grau hinterlegten Platzhalter, Auswahl der für die konkrete Schule gewählten Alternative) und den Erziehungsberechtigten/Schülerinnen und Schüler bei Ausgabe des Geräts vorgelegt.

Durch ihre Unterschrift verpflichten sich die Erziehungsberechtigten/Schülerinnen und Schüler zur Einhaltung der Nutzungsbedingungen.

Das unterschriebene Dokument wird zu Dokumentationszwecken in der Schule veraktet.

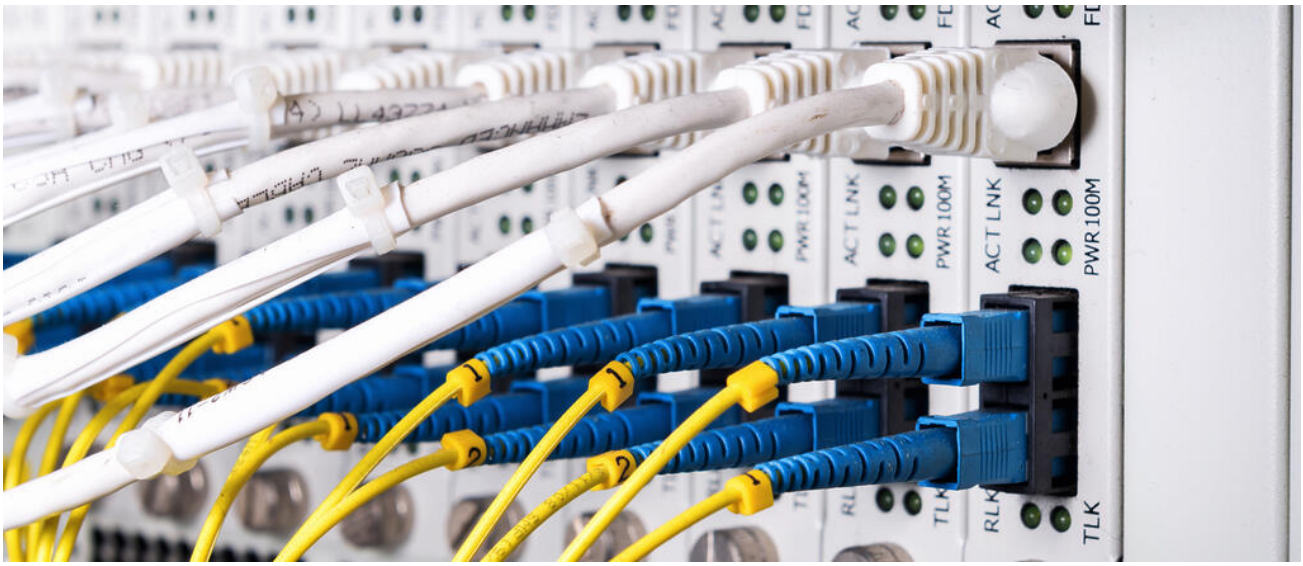
Es ist sinnvoll, für die Schülerinnen und Schüler einen Onepager (altersgerecht) mit den wichtigsten Informationen zur Verfügung zu stellen.

Nutzungsbedingungen für Schülerleihgeräte
/download/4-24-02/Nutzungsbedingungen-f%C3%BCr-Sch%C3%BClerleihger%C3%A4te.jpg

Mindestsicherheitsstandards beim Einsatz von Schülerleihgeräten
/download/4-24-02/Mindestsicherheitsstandards_Schuelerleihger%C3%A4te_Stand_01.04.2024.jpg

Es wird empfohlen die Endgeräte vor dem ersten Einsatz sicher zu konfigurieren und die Sicherheitseinstellungen zu aktivieren. Mögliche → Konfigurationen https://www.km.bayern.de/gestalten/digitalisierung/datensicherheit/mobile-device-management#konfiguration finden sich unter dem angegebenen.

Schulnetz



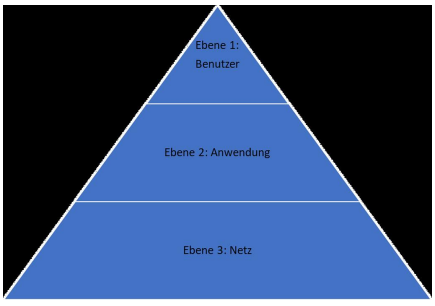
Standards garantieren einen sicheren Aufbau des Schulnetzes ©jackykids - stock.adobe.com

Sicherheit im Schulnetz

Datenschutz, Datensicherheit und Funktionsstabilität sind zentrale Anforderungen an ein funktionierendes Schulnetz.

Sicherheit im Schulnetz

- bezieht sich auf benutzerbasierte individuelle Aspekte (Ebene 1)
- und hat einen Bezug zu Anwendungen und den möglichen Zugriff auf Ressourcen (Ebene 2).
- Bereits auf der Netzwerkebene kann der Wirkbereich eines Nutzers eingeschränkt und damit die Sicherheit erhöht werden (Ebene 3).



©Bayerisches Staatsministerium für Unterricht und Kultus

Während die Ebenen 1 und 2 an anderen Stellen dieses Internetauftritts behandelt werden, gibt diese Seite einen Überblick über die wichtigsten Komponenten und Maßnahmen der Netzebene (Ebene 3), damit ein reibungsloser und sicherer Betrieb des Schulnetzes gewährleistet ist.

Zielgruppe: Systembetreuer, Schulleitung, Schulaufwandsträger

Schulnetzdesign

Schulnetze stehen teilweise unter enormen Belastungen, da Lernende und Lehrkräfte gleichzeitig auf das WLAN und das Internet zugreifen. Ohne eine gut geplante und strukturierte Netzwerkinfrastruktur drohen Leistungseinbußen und Sicherheitsrisiken. Besonders wichtig ist die **Trennung von pädagogischem Netzwerk und Verwaltungsnetz**, um sensible Daten zu schützen. Eine durchdachte Segmentierung mit Virtual LANs (VLANs) und Firewalls sorgt dafür, dass verschiedene Netzbereiche eine sichere und effiziente Kommunikation ermöglichen. Nur so lassen sich die Anforderungen an Datensicherheit und Datenschutz erfüllen, während das Netz auch Lastspitzen problemlos bewältigt.

Mehr zu Netzdesign

Funktionsstabilität und Datensicherheit

Schulnetze sind hohen Lastsituationen ausgesetzt. In kurzen Zeitabschnitten melden sich Lernende und Lehrkräfte an, greifen auf das WLAN und das Internet zu. Ein gut strukturiertes und dimensioniertes Schulnetz bietet die notwendige Funktionsstabilität und diese Lastspitzen verarbeiten zu können.
Voraussetzung dafür sind ausreichende Bandbreiten auf den Übertragungsstrecken, leistungsfähige Netzwerkgeräte und eine, von der Schulnetzgröße abhängige, Segmentierung. Durchgängig performante Kommunikationspfade sind das Ergebnis einer korrekten Planung und Umsetzung.

Weitere Anforderungen

Neben dem pädagogischen Netzwerk ist das Verwaltungsnetz ein weiterer Bereich der Schulnetzinfrastruktur. Im Verwaltungsnetz gelten hohe Anforderungen bezüglich der Datensicherheit und des Datenschutzes.

Die Kommunikation zwischen den Teilnetzen Unterrichtsnetz und Verwaltungsnetz sollte, aufgrund der hohen Vertraulichkeit im Verwaltungsnetz, unmöglich oder aber auf sehr wenige spezifische Ausnahmefälle beschränkt sein.

Netzwerktechnik

Mit geeigneten Netzwerkgeräten lassen sich Teilnetze innerhalb der Infrastruktur bilden. Die Technik **Virtual LAN (VLAN)** bietet die Möglichkeit, das Schulnetz zu segmentieren. Schulinterne Firewalls steuern die Kommunikation zwischen diesen Netzbereichen. Die Firewall-Funktionen sind Bestandteil der zentralen Router bzw. L3-Switches.

Beispiele für Netzsegmente bzw. Teilnetze in der Schule sind: Unterricht-, Schüler-WLAN,

Verwaltungsnetz.

Weiterführende Informationen zum Netzdesign und eine Konfigurationsübersicht mit Checkliste zum Switch befinden sich in den nachfolgenden Dokumenten.

Handreichung Netzdesign
/download/4-24-11/241107_Handreichung_Netzdesign.jpg

Beispielkonfiguration Netzdesign
/download/4-24-11/241107_Beispielkonfiguration_Netzdesign.jpg

Muster Netzdesign
/download/4-24-11/241107_Muster_KonfigNetzdesign.jpg

Fernzugriff (VPN)

Der Fernzugriff auf das Schulnetzwerk über VPN bietet eine sichere Möglichkeit, sensible Daten zu übertragen, birgt jedoch auch potenzielle Risiken. Um unbefugten Zugriff zu verhindern, ist eine starke Authentifizierung unerlässlich. Neben der Verschlüsselung der Daten ist die Implementierung von Zwei-Faktor-Authentifizierung (2FA) eine wichtige Sicherheitsmaßnahme. Ein VPN-Gateway auf der Schulseite und ein kompatibler Client auf der Nutzerseite sind Voraussetzung für den sicheren Betrieb. Besonders bei der Anbindung externer Standorte (Site-to-Site-VPN) müssen erhöhte Sicherheitsanforderungen beachtet werden.

Mehr zu Fernzugriff (VPN)

Mit VPN-Technik auf das Netz der Schule zugreifen.

Der Zugriff auf Daten oder Systeme im Netzwerk der Schule kann aus verschiedenen Gründen notwendig sein. Da dies nur ausgewählten Personen möglich sein soll, muss die **Authentizität** nachgewiesen werden.

Zur Wahrung der **Vertraulichkeit** ist es erforderlich, die Daten zu verschlüsseln.

VPN-Technologien (Virtual Private Network) bieten die Merkmale einer sicheren Datenübertragung und ermöglichen damit die vertrauliche Kommunikation über unsichere

Netze (Internet).

Der Zugriff auf das Schulnetz bzw. das Netzwerk der Verwaltung einer Schule darf nur ausgewählten Personen möglich sein. Dazu zählen Schulleitungen oder Mitarbeitende der IT-Administration (Client-to-Site-VPN). Erhöhte Sicherheitsanforderungen können die Integration einer 2-Faktor-Authentifizierung (2FA) erforderlich machen.

Um eine VPN-Verbindung nutzen zu können, muss auf der Seite der Schule die Funktion des VPN-Gateways eingerichtet sein. Auf der Anwenderseite ist ein kompatibler Client erforderlich.

Die Anbindung einer Außenstellung ist ein weiteres Szenario für den Einsatz von VPN (Site-to-Site-VPN).

Eine mögliche VPN-Technik ist das Protokoll IPSec.

Weiterführende Informationen zu VPN und eine Konfigurationsübersicht mit Checkliste befinden sich in den nachfolgenden Dokumenten

Handreichung VPN
/download/4-24-11/241111_Handreichung_VPN.jpg

Beispielkonfiguration VPN
/download/4-24-11/241111_Beispielkonfiguration_VPN.jpg

Muster VPN
/download/4-24-11/241111_Muster_VPN.jpg

Firewall

Für eine sichere und kontrollierte Kommunikation in Schulnetzen sind Firewalls unverzichtbar. Sie filtern Datenpakete nach vordefinierten Regeln und verhindern unbefugte Zugriffe, insbesondere aus dem Internet. Der Zugriff ins Schulnetz von außen ist nur über sichere VPN-Verbindungen möglich. Gleichzeitig wird der ausgehende Datenverkehr auf notwendige Protokolle beschränkt. Firewalls trennen zudem interne Netzbereiche, um unerlaubte Zugriffe, etwa vom Unterrichts- ins Verwaltungsnetz, zu verhindern. Moderne Lösungen wie Next-Generation-Firewalls bieten zusätzlichen Schutz vor komplexen Bedrohungen.

Mehr zu Firewall

Firewall-Systeme blockieren unerwünschte Kommunikation

Die sichere Kommunikation über Netzgrenzen hinweg, erfordert die kontrollierte Weiterleitung oder auch das Blockieren von Daten. Dies gilt sowohl für schulinterne Kommunikationsprozesse als auch für den Datenaustausch mit dem Internet.

Firewalls untersuchen die übertragenden Datenpakete und filtern auf Basis vordefinierter Regeln.

Der Verbindungsaufbau aus dem Internet in das lokale Schulnetz muss verhindert werden. Eine Ausnahme bilden kontrollierte Zugänge per VPN. Viele Hackerangriffe lassen sich durch Firewalls wirkungsvoll blockieren.

Der Netzwerkverkehr aus dem Schulnetz in das Internet sollte gefiltert und damit auf die notwendigen Protokolle begrenzt werden. Dies verhindert unerwünschte Verbindungs-aufbauten auf Netzwerkebene.

Firewall-Systeme werden darüber hinaus auch für die Steuerung der schulinternen Datenkommunikation eingesetzt. Auf diese Art lassen sich Netzbereiche voneinander abtrennen. Ein unerlaubter Zugriff, zum Beispiel aus dem Unterrichts- auf das Verwaltungsnetz, ist damit unterbunden.

Die Firewall-Funktion ist in aller Regel Bestandteil der eingesetzten Router. In besonderen Fällen ist können dedizierte Firewalls (IPS/IDS, Next-Generation-Firewall) spezielle erhöhte Sicherheitsanforderungen erfüllen.

Detaillierte Informationen, sowie eine Checkliste und eine Beispielkonfiguration zu Firewalls und Routern finden sich in den nachfolgenden Dokumenten.

Handreichung Router mit Firewall
/download/4-24-11/241108_Handreichung_RouterFirewall.jpg

Beispielkonfiguration Firewall-Router
/download/4-24-11/241108_Beispielkonfiguration_RouterFirewall.jpg

Muster Firewall-Router
/download/4-24-11/241108_Muster_KonfigRouterFirewall.jpg

Webfilter

Webfilter bieten einen wichtigen Schutz vor ungeeigneten Inhalten und Bedrohungen im Internet. Sie sperren nicht nur gefährliche Websites, sondern auch den Internetzugriff von Apps und Links aus Spam-Mails. Besonders die DNS-Filtertechnologie überzeugt durch Skalierbarkeit und Geschwindigkeit, ohne spezielle Hardware zu benötigen. Schulen sind zwar nicht verpflichtet, Webfilter einzusetzen, doch sie bieten eine effektive Möglichkeit die Schülerinnen und Schüler zu schützen. Bei der Auswahl eines Filters sollten Kriterien wie Jugendschutz, Zuverlässigkeit und einfache Konfiguration im Fokus stehen.

Mehr zu Webfiltern

Webfilter in der Schule

Nicht alle Internetseiten und Inhalte sind lernförderlich, im Schuleinsatz erwünscht oder sogar jugendgefährdend. Mit Webfiltern können Zugriffe auf solche unerwünschten Webseiten und Inhalte eingeschränkt werden.

Rahmenbedingungen und Herausforderungen

Schulnetzwerke zeichnen sich durch heterogene Systeme bzw. Endgeräte aus. Webfilter müssen daher an einer zentralen Kommunikationsschnittstelle platziert werden. Der Internetzugangsrouter oder ein zentraler DNS-Server der Schule sind solche Schnittstellen. Bei entsprechender Konfiguration müssen alle Endgeräte diese Dienste nutzen.

An diesen Stellen können Filterfunktionen integriert werden. Relativ einfach und effektiv lassen sich Filter auf Basis der Namensauflösung DNS (Domain Name Service) realisieren.

Technik

Ein DNS-Filterdienst kategorisiert Webseiten und meldet, wenn eine Webseite zu einer Sperrkategorie gehört. Dieser Filterserver ist auf dem Router der Schule eingetragen, alternative DNS-Server sind durch die Firewall nicht erreichbar.

Neben der DNS-basierten Filtertechnologie gibt es weitere, meist komplexere Web- und Content-Filter. Die Heterogenität der (mobilen) Clients, die Anforderung an eine performante Netzwerkkommunikation sowie die einfache Integration in das Schulnetzwerk geben in der Regel dem DNS-basierten Webfilter den Vorzug.

Filterfunktionen und Grenzen

Der Aufruf von Webseiten erfolgt über die Angabe des Namens der Seite bzw. des Webservers. Ist bekannt, dass dieser Server jugendgefährdende Inhalte (z.B. Gewalt, Pornografie, Waffen etc.) anbietet, wird er entsprechend kategorisiert und die Web-Kommunikation mit diesem Server unterbunden. DNS-Filter sind nicht dafür ausgelegt, spezifische Inhalte zu erkennen und zu filtern. Auch für die Erkennung von Spam oder Malware müssen andere Systeme hinzugezogen werden.

Hinweise

Der Einsatz von Webfiltern obliegt der pädagogischen Verantwortung der Schule. Es besteht keine grundsätzliche Verpflichtung für den Einsatz von Filtertechnik.

Weiterführende Informationen finden sich in den „Empfehlungen zur IT-Ausstattung von Schulen“ unter dem folgenden Link.

Votum 23/24 S. 48ff
https://mebis.bycs.de/beitrag/votum

WLAN

Sicheres WLAN ist in Schulen unerlässlich, um sowohl den Zugang zum Internet als auch zu lokalen Ressourcen zu ermöglichen. Doch drahtlose Netzwerke bergen Risiken: Da Daten über Funk übertragen werden, sind sie potenziell abhörbar. Um dies zu verhindern, sollten moderne Verschlüsselungsstandards wie WPA2/3 eingesetzt werden. Besonders wichtig ist die Trennung von Netzen, um sensible Daten von allgemeinen Internetzugängen zu schützen. Multi-SSID-Lösungen und VLANs ermöglichen eine flexible Netzwerknutzung mit unterschiedlichen Sicherheitsstufen für Schüler, Lehrkräfte und Gäste. Die richtige Konfiguration der Access Points, eine starke Authentifizierung und regelmäßige Firmware-Updates sind entscheidend, um Sicherheitslücken zu vermeiden und den Unterrichtsbetrieb nicht zu gefährden.

Mehr zu WLAN

Kabellos im Unterricht

Wireless-LAN (WLAN) bietet mobilen Endgeräten den unkomplizierten Zugang zum Schulnetz mit Internetzugang.

Sicherheit

Da die Datenübertragung per WLAN nicht an eine geschützte Verkabelung gebunden ist, müssen zusätzliche Maßnahmen zur Absicherung getroffen werden. Aktuelle Sicherheitsmechanismen bieten die Authentifizierung mittels gemeinsamen Passwortes und die Verschlüsselung der Daten (WPA2/3-PSK). Die Forderungen an einen einfachen, technisch niederschwelligen, aber auch sicheren Netzzugang, können mit diesem Verfahren

erfüllt werden.

Besondere Anforderungen im Verwaltungsnetz

Für das Verwaltungsnetz der Schule bestehen erhöhte Sicherheitsanforderungen. In diesem Bereich sollte auf den Einsatz von WLAN verzichtet werden.

Segmentierung

Um die Funktionsstabilität und Sicherheit zu steigern, kann das WLAN als ein separates Teilnetz (WLAN als VLAN) betrieben werden. Dabei ist zu prüfen, auf welche internen Systeme der Schule (Drucker, Bildschirmübertragung etc.) WLAN-Clients zugreifen müssen. Der Zugang zum Internet und Cloud-Diensten wird Schwerpunkt der Nutzung sein.
WLAN in der Schule bedeutet die Berücksichtigung von Lastsituationen (Hochlastbetrieb, High Density). Die Anforderungen an eine solche Umgebung gilt es bereits bei der Planung zu beachten.

Die Administration und Wartung der WLAN-Access-Points erfolgen in aller Regel über einen WLAN-Controller.

Detailliertere Informationen und Beispiele zur Dokumentation beim Einsatz von WLAN in Schulen befinden sich in der nachfolgenden Handreichung.

Handreichung WLAN
/download/4-24-11/241111_Handreichung_WLAN.jpg

Beispielkonfiguration WLAN
/download/4-24-11/241111_Beispielkonfiguration_WLAN.jpg

Muster WLAN
/download/4-24-11/241111_Muster_WLAN.jpg

WLAN in der Nutzungsordnung

Der Zugang zum WLAN und die Verantwortlichkeiten der Nutzenden sind in der Nutzungsordnung zu regeln.

Verweis auf die Empfehlungen zur IT-Ausstattung von Schulen

Alle Themen dieser Seite werden auch im Votum betrachtet.

Verschlüsselung

Verschlüsselung von Dateien, Wechseldatenträgern oder Container

Das Ziel einer Verschlüsselung von Dateien oder Datenträgern ist die Sicherstellung der Vertraulichkeit. Nur die Besitzer eines Schlüssels bzw. Passworts (die Begriffe werden hier synonym verwendet) können den Inhalt einer Datei lesen bzw. öffnen.

Mit anderen Worten, obwohl man Zugriff auf eine verschlüsselte Datei hat, darf es nicht möglich sein, den Inhalt zu lesen, ohne im Besitz des richtigen Schlüssels zu sein. Das bedeutet, dass ausschließlich Berechtigten der Zugriff auf die Klartextinformationen möglich ist.

Sobald vertrauliche Daten an Orten gespeichert werden, zu denen auch unberechtigte Personen Zugang haben, müssen diese verschlüsselt werden. Verschlüsselung ist auch für den Fall erforderlich, dass die Daten über einen unsicheren Transportweg (z. B. E-Mail) übertragen werden.

Wichtig: Ohne das Passwort oder den Wiederherstellungsschlüssel und ohne das zugehörige Verschlüsselungsprogramm sind die Daten nicht mehr zugänglich.

Für die Verschlüsselung sind verschiedene Aspekte zu berücksichtigen:

- Auswahl des Programms oder der Funktion zum Ver- und Entschlüsseln
- Sichere Speicherung des Schlüssels
- Beachtung der Anforderungen an die Wahl des Schlüssels
- Übertragbarkeit auf andere Systeme (Interoperabilität/Kompatibilität)
- Nutzbarkeit in der Zukunft

Zielgruppe: Schulleitung, pädagogischer Systembetreuer, Verwaltungskräfte, Lehrkräfte und sonstiges pädagogisches Personal, Schulaufwandsträger

Anforderungen an die Wahl des Schlüssels

Zum Verschlüsseln und zum Entschlüsseln in diesen genannten Verfahren wird der gleiche Schlüssel verwendet. Dieser Schlüssel muss geheim gehalten werden und „sicher“ gestaltet sein. Informationen dazu bietet das Bundesamt für Sicherheit in der Informationstechnik

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html

Der sichere Austausch von Information ist durch die Verschlüsselung problemlos möglich. Der geheime Schlüssel ist jedoch auf einem gesonderten Kommunikationsweg zu übertragen. (Beispiel: Versand eines verschlüsselten Anhangs per E-Mail; Übertragung des Passworts per Telefon)

Verschlüsselung von Einzeldokumenten

Der Inhalt eines Dokuments wird verschlüsselt. Der Dateiname ist normalerweise im Klartext vorhanden. Beispiel: Verschlüsselung in Office-Programmen

Verschlüsselung von mehreren Dokumenten in einem verschlüsselten Container

Die Dokumente liegen in einem verschlüsselten Container (z. B. eine große Datei). Nach dem Öffnen des Containers stehen alle Dokumente im Klartext zur Verfügung. Die Sicherheit hängt in der Praxis sehr stark davon ab, wie mit dem geöffneten Container umgegangen wird. Beispiele: Veracrypt, 7-Zip.

Verschlüsselung von integrierten Festplatten und Wechseldatenträgern

Dateisysteme (Festplattenpartitionen oder mobile Datenträger) können verschlüsselt werden. Wenn ein verschlüsseltes Dateisystem hochgefahren (gemountet) wird (z. B. beim Einschalten eines Computers oder beim Einstecken einer verschlüsselten USB-Festplatte), ist ein Passwort erforderlich. Danach kann mit den Daten normal gearbeitet werden. Je nach Implementierung sind die Daten erst wieder geschützt, wenn der Benutzer abgemeldet wird, der Computer heruntergefahren oder vom Strom genommen wird. Bei mobilen Endgeräten (z. B. Smartphone, Tablet) ist bei aktiviertem Bildschirmcode der integrierte Datenträger verschlüsselt. Sobald der Bildschirmcode deaktiviert wird, liegt die integrierte Festplatte unverschlüsselt vor. Moderne Desktop-Betriebssysteme bieten integrierte Verschlüsselungsprogramme an, um die Festplatte oder ggf. auch Wechseldatenträger zu verschlüsseln.

Beispiele: Verschlüsselter USB-Stick, verschlüsselte Partitionen eines Notebooks, verschlüsseltes Dateisystem auf einem Smartphone

Beispiele für Verschlüsselungsprogramme zur Verschlüsselung von integrierten Festplatten oder Wechseldatenträgern

7-Zip

7-Zip (für Windows, Linux) ist ein Kompressionsprogramm, mit dem Dateien oder Ordner komprimiert in einer Datei (Container) gespeichert und optional auch verschlüsselt werden können.

7-Zip eignet sich sehr gut, wenn Dateien oder Ordner mit vertraulichen Inhalten verschlüsselt archiviert oder transportiert werden sollen (z. B. Dauerhaftes Speichern von vertraulichen Daten, Ablage in einer Cloud, E-Mail-Anhänge).

Keka

Für MacOS bietet das Programm Keka ähnliche Funktionen wie 7-Zip für Windows. Komprimierte und verschlüsselte Ordner sind zwischen den Programmen kompatibel.

VeraCrypt

VeraCrypt (für Windows. Linux. MacOS) ist ein sehr mächtiges Verschlüsselungsprogramm. Es arbeitet mit verschlüsselten Containern, die beim Öffnen ein Passwort erfordern. VeraCrypt gewährleistet, dass auch während der Bearbeitung keine unverschlüsselten Textteile auf der Festplatte oder in einer temporären Datei abgelegt werden und bietet daher eine sehr hohe Sicherheit.

BitLocker und Bitlocker to Go

Bitlocker ist ein Bestandteil des Windows-Betriebssystems (ab Professional), dass Teile eines Datenträgers (Partitionen) oder den gesamten Datenträger verschlüsseln kann. Es eignet sich sehr gut zur Verschlüsselung von mobilen Datenträgern (z. B. USB-Sticks), wenn mit Windows gearbeitet wird, oder zur Verschlüsselung von Datenpartitionen bei Windows-Notebooks.

FileVault

FileVault nutzt als Bestandteil des macOS-Filesystems APFS, eine Verschlüsselung, um die Daten auf dem Startvolume eines Macs zu verschlüsseln. Der Wiederherstellungsschlüssel ist an den Benutzeraccount gebunden.

Sichere Übertragung: Transportverschlüsselung und Ende-zu-Ende-Verschlüsselung

Abhängig vom Schutzbedarf, sind geeignete Maßnahmen zur sicheren Datenkommunikation zu treffen. Die Anwendung und die Art der Datenübertragung sind bedeutsame Faktoren.

Die sog. Transportverschlüsselung wird zum Schutz der Daten zwischen Endgeräten oder Servern genutzt. Verfahren der Transportverschlüsselung schützen die Daten, so dass sie während des Transports nicht von Unbefugten gelesen oder unbemerkt manipuliert werden können. Ein Beispiel für den Einsatz einer Transportverschlüsselung ist TLS unter HTTPS (Hypertext Transfer Protocol Secure) bei einer Browserkommunikation.

Die Ende-zu-Ende-Verschlüsselung bietet einen höheren Grad an Sicherheit. Hierbei werden die Daten bereits in der Anwendung des Sendergerätes verschlüsselt und bleiben verschlüsselt, bis die Anwendung des Zielgerätes diese entschlüsselt. Selbst der Dienstanbieter, der die Daten übermittelt, kann sie nicht entschlüsseln, da nur die beiden Endgeräte die nötigen Schlüssel besitzen. Typischerweise wird diese Art der Verschlüsselung in Messenger-Apps verwendet, um die Vertraulichkeit der Kommunikation zu gewährleisten.

Sensibilisierung und Awareness

Sensibilisierung und Awareness sind der Schlüssel zum Schutz vor Datenverlust und Cyberangriffen

Sicherheit durch Schulung der Lehrkräfte

Aktuelle Statistiken zeigen, dass Bildungseinrichtungen zunehmend Ziel von Cyberkriminalität werden. Ein entscheidender Faktor, um Schäden durch Cyberangriffe zu vermeiden, ist die Sensibilisierung und Awareness (Aufmerksamkeit) der Lehrkräfte und Mitarbeiter. Dies beinhaltet auch den sicheren Umgang mit IT-Systemen, wie Endgeräten und Anwendungen, das Wissen um Maßnahmen zum Schutz der digitalen Identität, sowie das Erkennen von Social-Engineering-Methoden, wie beispielsweise Phishing.

Verantwortung der Schulleitung

Gemäß Art. 24 und 32 DSGVO sowie § 27 Abs. 7 LDO muss jede Schule organisatorische Maßnahmen zum Schutz der Datenverarbeitung treffen. Dies betrifft auch Maßnahmen zur Schulung von Lehrkräften und Mitarbeitern zur IT-Sicherheit an der Schule. Die Schulleitung entscheidet unter Einbezug der DSB, welche Maßnahmen umgesetzt werden. Zudem weist regelmäßig auf die Bedeutung von Awareness hin und geht mit gutem Beispiel voran.

Selbstlernkurs zur Sensibilisierung

Um die Schulen bei der Sensibilisierung für grundlegende Themen der IT-Sicherheit zu unterstützen, wird auf der Fortbildungsplattform FIBS der ALP Dillingen ein Selbstlernkurs

angeboten. Er gliedert sich in drei Module, die jeweils etwa 30 bis 45 Minuten Zeit in nehmen.

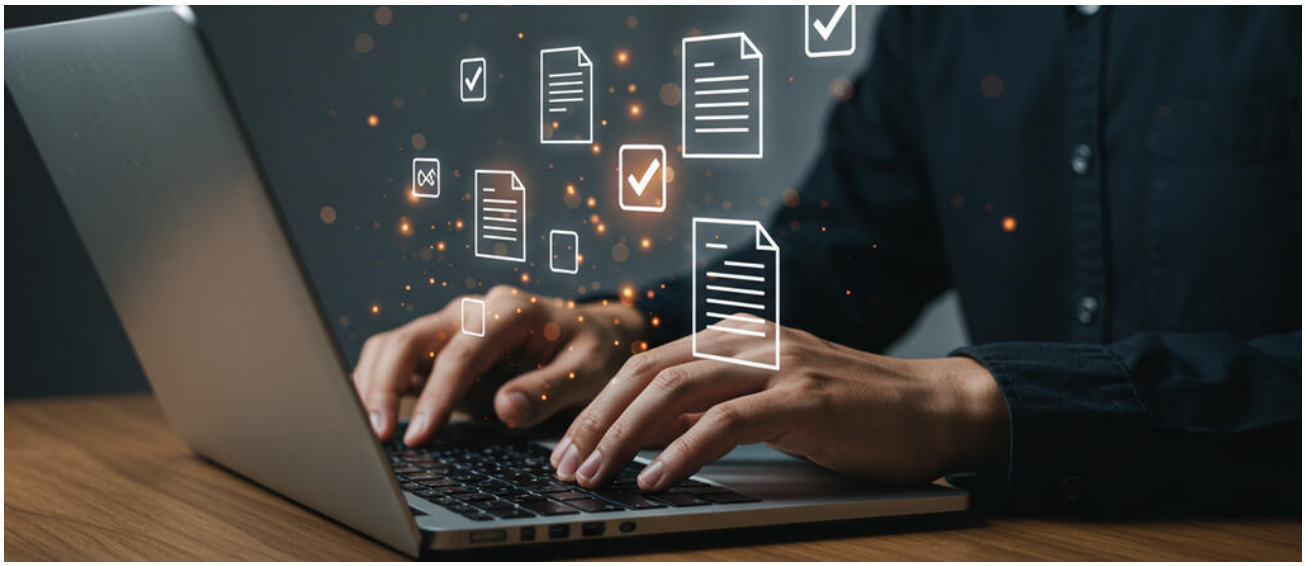
- Modul 1 behandelt potenzielle Gefährdungen und Maßnahmen zur IT-Sicherheit, einschließlich der Verwendung von Schutzprogrammen und der Umsetzung von Updates.
- Modul 2 fokussiert sich auf den Schutz der digitalen Identität, sichere Passwörter, Passwortmanager sowie die Gefahren des Social Engineering und Phishing.
- Modul 3 widmet sich der sicheren E-Mail-Kommunikation.

Mit dem Selbstlernkurs wird ein niederschwelliges Angebot geschaffen, um die Beschäftigten an der Schule für mehr IT-Sicherheit zu sensibilisieren.

Selbstlernkurs zur Sensibilisierung in der IT-Sicherheit
Link zum Lehrgangsangebot der ALP Dillingen
https://alp.dillingen.de/lehrgangs-suche/?keyword=C0BD4953F386B8A0E16B943E7F73DD65

Berechtigungsmanagement

Ein strukturiertes Berechtigungsmanagement stellt einen wesentlichen Bestandteil der Datensicherheit dar.



Need-to-know - Nur das sehen, was notwendig ist ©Block nomic Studio - stock.adobe.com

Das Berechtigungsmanagement stellt sicher, dass ausschließlich autorisierte Personen Zugang zu Daten und Systemen erhalten. In den Schulen existieren verschiedene Nutzergruppen – beispielsweise Lehrkräfte, Schüler, Verwaltungspersonal und Administratoren – die jeweils unterschiedliche Zugriffsrechte benötigen. Ein klares Berechtigungsmanagement gewährleistet sowohl die Einhaltung von Datenschutz- und Sicherheitsanforderungen als auch eine klare Aufgaben- und Verantwortungsverteilung.

Zentrale Prinzipien: Need-to-know und Least-Privilege

Das sogenannte Need-to-know-Prinzip bildet die Grundlage des Berechtigungsmanagements. Es besagt, dass Informationen und Zugriffsrechte ausschließlich denjenigen Personen zur Verfügung gestellt werden, die diese zur Erfüllung ihrer jeweiligen Aufgaben zwingend benötigen. Ergänzend dazu sollte auch das Least-Privilege-Prinzip berücksichtigt werden. Es stellt sicher, dass Nutzer nur die minimal erforderlichen Rechte erhalten – nicht nur in Bezug auf Informationen, sondern auch hinsichtlich Systemfunktionen und Ressourcen. Durch Anwendung dieser Prinzipien auf allen Ebenen und auf die verschiedenen IT-Systeme wird das Risiko unbefugter Zugriffe und Datenlecks wirksam minimiert.

Datenschutzrechtliche Vorgaben

Sofern personenbezogene Daten verarbeitet werden, fordert die DSGVO den Schutz vor „unbefugter und unrechtmäßiger Verarbeitung“ (Art. 5 Abs. 1 Buchst. f). Dies macht die Regelung von entsprechenden Zugriffsberechtigungen unmittelbar gesetzlich erforderlich.

Dabei spielt es keine Rolle in welcher Form (analog oder digital) die personenbezogenen Daten vorliegen.

Umsetzung und Dokumentation

Die Umsetzung des Berechtigungsmanagements erfolgt auf verschiedenen Ebenen, die nachfolgend näher beschrieben werden. Für die Planung, Vergabe, Dokumentation von Zugriffsrechten bieten sich sogenannte **Berechtigungsmatrizen** an. Diese stellen übersichtlich dar, welche Nutzergruppen auf welche Ressourcen mit welchen Zugriffsrechten zugreifen dürfen und ermöglichen eine regelmäßige Überprüfung und Anpassung der Rechtevergabe. Sie sind als technische bzw. organisatorische Maßnahme zu verakten.
Ein Beispiel für typische Nutzergruppen an den Schulen mit ihren Zugriffsrechten auf verschiedene Informationen ist in der nachfolgenden Tabelle abgebildet.

Netz- und Hardware-Ebene

Der Zugang zu einem Netzwerk und den Endsystemen sollte so weit wie möglich eingeschränkt werden. Das gilt sowohl für Netzwerkbereiche oder spezielle Server als auch für den **physischen Zugang**, wie bei einem Serverraum und den Endgeräten in den Räumen der Verwaltung oder im Lehrerzimmer.
Die Tabelle zeigt beispielhaft eine Berechtigungsmatrix für typische IT-Komponenten einer Schule und kann zur Weiterverarbeitung heruntergeladen werden.

Muster einer Berechtigungsmatrix
/download/4-25-06/250710_Berechtigungsmatrix_zur_Weiterverarbeitung.jpg

Dienste- und Anwendungs-Ebene

Für Anwendungen und (Cloud-)Dienste konkretisiert Anlage 2 zu § 46 BaySchO unter dem Punkt „Interne Empfänger/Zugriffsberechtigte“ die Vorgaben aus Art. 5 Abs. 1 Buchst. f DSGVO für die jeweilige Anwendung bzw. den (Cloud-)Dienst. Häufig werden dabei von den Anwendungen vorgegebene Rollenprofile angeboten, denen standardmäßig verschiedene Berechtigungen zugewiesen sind. Es ist zu prüfen, ob die Rolle den zugriffsberechtigten Personen entspricht; andernfalls müssen entsprechende Anpassungen vorgenommen werden.

Das folgende Dokument visualisiert die wesentlichen Zugriffsberechtigungen für die

einzelnen Abschnitte der Anlage 2 zu § 46 BaySchO als Berechtigungsmatrix.

Darstellungen der Zugriffsberechtigungen gemäß Anlage 2 zu BaySchO §46
/download/4-25-06/250710_BayScho_Berechtigungsmatrizen.jpg

Basiert die Verarbeitung von (personenbezogenen) Daten auf einer anderen Rechtsgrundlage als auf den in Anlage 2 zu § 46 BaySchO aufgeführten Abschnitten, ist entsprechend ein eigens angepasstes Rollen- und Berechtigungskonzept zu erstellen.