Bayerisches Staatsministerium für
Unterricht und Kultus

GESTALTEN > DIGITALISIERUNG

Datensicherheit und Datenschutz an Schulen

Stand: 24.04.2024

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

Inhaltsverzeichnis

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 Internetzuganghttps://www.verkuendung-bayern.de/baymbl/2022-436/

> Bekanntmachung zum Vollzug der datenschutzrechtlichen Bestimmungenhttps://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 Schulenhttps://www.verkuendung-bayern.de/files/baymbl/2022/436/anhang/Anlage.pdf

> Muster für Nutzungsbedingungen für Lehrerdienstgeräte/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/gestalten/digitalisierung/datensicherheit/lehrerdienstgeraete#checklisten

Checkliste privaten Endgeräte/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
> https://www.km.bayern.de/download/4-23-11/Nutzungsbedingungen-für-Ausbildungsgeräte_6.0.pdf

---

Inbetriebnahme Ausbildungsgeräte – Schritt-für-

Schritt-Anleitungen

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

> iPad-Inbetriebnahme – Schritt-für-Schritt-Anleitung
> https://www.km.bayern.de/download/4-23-11/Schritt-für-Schritt_Anleitung-Ausbildungsgeräten_iPad.pdf

> Surface-Inbetriebnahme – Schritt-für-Schritt-Anleitung
> https://www.km.bayern.de/download/4-23-11/Schritt-für-Schritt_Anleitung-Ausbildungsgeräten_Surface-1.pdf

---

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.

Prozess

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

Prozessbeschreibung Apps auf Ausbildungsgeräten
https://www.km.bayern.de/download/4-23-11/Prozessbeschreibung_Ausbildungsgeräte_Apps.pdf

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
https://www.km.bayern.de/download/4-23-11/SNR_Antrag_auf_Pruefung_v1.pdf

Antrag auf Bereitstellung einer App auf den Ausbildungsgeräten (Grund-/Mittel-/Förderschulen)
https://www.km.bayern.de/download/4-23-11/SNR_Antrag_auf_Bereitstellung_GMS_FoeS_v1.pdf

Antrag auf Bereitstellung einer App auf den Ausbildungsgeräten (weiterführende Schulen)
https://www.km.bayern.de/download/4-23-11/SNR_Antrag_auf_Bereitstellung_weiterfuehrende_Schulen_v1.pdf

Bewertungsbogen
https://www.km.bayern.de/download/4-23-11/Bewertungsbogen_Muster.docx

Datenschutz an Schulen

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

Zielgruppe: Schulaufwandsträger, Schulleiter

Adressat: Lehrkraft bzw. 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
> https://www.km.bayern.de/download/4-23-12/Nutzungsbedingungen-für-Lehrerdienstgeräte.docx

Mindestsicherheitsstandards

Zielgruppe: Nutzer, Systemadministrator/-in, Sachaufwandsträger

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

> Mindestsicherheitsstandards beim Einsatz der dienstlichen Geräte
> https://www.km.bayern.de/download/4-23-12/Mindestsicherheitsstandards-beim-Einsatz-der-dienstlichen-Geraete.pdf

Checklisten

Zielgruppe: 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
https://www.km.bayern.de/download/4-23-12/Muster-einer-Checkliste-Schule.docx

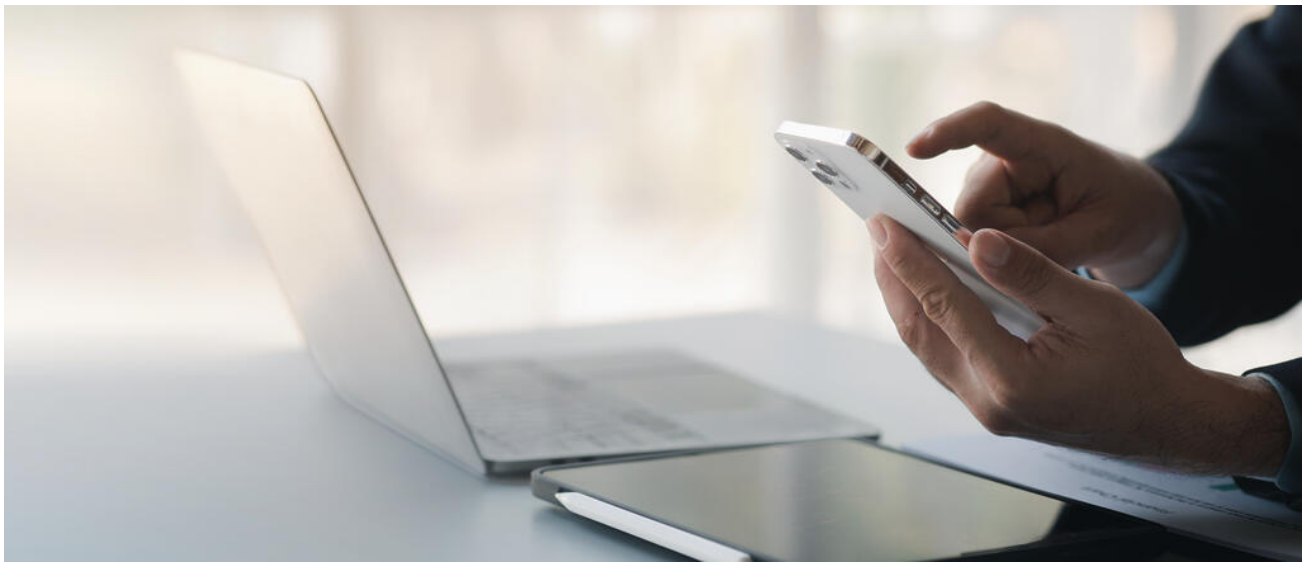
Beim Ausfüllen der Checkliste kann sich die Schulleitung an den folgenden Empfehlungen des Staatsministeriums für Unterricht und Kultus orientieren:

Empfehlung des StMUK für die Schule
https://www.km.bayern.de/download/4-24-02/Empfehlungen-des-StMUK-Lehrerdienstgeräte.pdf

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

Checkliste (Beispiele)
https://www.km.bayern.de/download/4-24-02/Beispiel-einer-Checkliste-für-ein-mobiles-Lehrerdienstgerät.pdf

Mobile Device Management



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

Allgemein

Unter einem Mobile-Device-Management versteht man ein System zur zentralisierten Verwaltung von mobilen und stationären Endgeräten sowie Apps. Die Verwaltung umfasst dabei die Inventarisierung von Geräten, Software-, Daten- und Richtlinienverteilung. Die MDM-Software läuft in der Regel auf einem lokalen Server („on premise“) oder in der Cloud. Über eine MDM-Verwaltungskonsole (z. B. per Webzugriff) können die IT-Verantwortlichen der Schule die Geräte remote konfigurieren und verwalten .

Alle mobilen Betriebssysteme bieten die Möglichkeit, dass Geräte vollautomatisiert („Zero-Touch-Konfiguration“) beim erstmaligen Einschalten konfiguriert werden. Dadurch sind in der Regel kaum Benutzerinteraktionen notwendig (außer z. B. das Anmelden mit einem schuleigenen Account). Dazu sind aber einige Voraussetzungen zu erfüllen:

- entsprechende Schulaccounts
- Kauf der Neugeräte bei einem autorisierten Händler
- Registrierung der Neugeräte in einem entsprechenden Schulaccount durch den Händler
- MDM-System, dass die Zero-Touch-Registrierung unterstützt

Generell benötigen neue Geräte einmalig eine Internetverbindung (verkabelt oder durch manuelle Eingabe des WLAN-Passworts), um die Initialkonfiguration durchführenzu können.

Wird das MDM ganz oder auch nur teilweise von einem externen Cloud-Anbieter bezogen, sind zusätzlich die Anforderungen aus dem Mindeststandard des BSI zur "Nutzung externer Cloud-Dienste" einzuhalten.

Allgemeine Hinweise zu MDMs

Zielgruppe: Schulleitungen, pädagogische Systembetreuer

> Hinweise für die Schulleitung
> https://www.km.bayern.de/download/4-24-02/Hinweise-für-die-Beschaffung-eines-MDMs.pdf

Zielgruppe: Systembetreuer

Hinweise zu MDM-Lösungen
https://www.km.bayern.de/download/4-24-02/Umsetzungshinweise-für-die-Einführung-eines-MDMs.pdf

Konfiguration

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.

Generell benötigen neue Geräte einmalig eine Internetverbindung (verkabelt oder durch manuelle Eingabe des WLAN-Passworts), um die Initialkonfiguration durchführen zu können.

Zielgruppe: Systembetreuer

Beispiel für die Konfiguration
https://www.km.bayern.de/download/4-24-02/Mögliche-Grundkonfigurationen.pdf

Muster für die Konfigurationstabelle
https://www.km.bayern.de/download/4-24-02/Muster-für-die-Schulen.docx

Private Endgeräte im Dienstgebrauch

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

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). 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. 3.2.4https://www.gesetze-bayern.de/Content/Document/BayVV_204_K_13178/true

> Bayerisches SchulportalDas 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
https://www.km.bayern.de/download/4-24-02/Erklärung_zur_Nutzung_privater_Endgeräte_für_dienstliche_Zwecke.pdf

Erklärung zur Nutzung privater Endgeräte für dienstliche Zwecke
https://www.km.bayern.de/download/4-24-02/Erklärung_zur_Nutzung_privater_Endgeräte_für_dienstliche_Zwecke.docx

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
https://www.km.bayern.de/download/4-24-02/Mindestsicherheitsstandards_Stand_20.09.2023.pdf

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.

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
https://www.km.bayern.de/download/4-24-02/Mindestsicherheitsstandards_Schuelerleihgeräte_Stand_01.04.2024.pdf

Mindestsicherheitsstandards beim Einsatz von Schülerleihgeräten
https://www.km.bayern.de/download/4-24-02/Mindestsicherheitsstandards_Schuelerleihgeräte_Stand_01.04.2024.pdf

Es wird empfohlen die Endgeräte vor dem ersten Einsatz sicher zu konfigurieren und die Sicherheitseinstellungen zu aktivieren. Mögliche Konfigurationen finden sich unter dem angegebenen.

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 digitale Kommunikations- und Kollaborationswerkezeuge

- Groupware (z. B. E-Mail-Postfach, Kalender, Notizen),
- Messenger
- Cloud-Speicher
- 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 sonstige 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 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 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 digitaler 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 schützen, 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 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.

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 der Inhaltsdaten mit Drittprodukten erfolgen.

Diese Maßnahmen sind einem OnePager 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.

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

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 den 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 sonstige an der Schule tätige Personal

Ein Leitfaden zum Erkennen von Phishing-E-Mails befindet sich bei den Downloads

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).

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

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).

Kalenderfreigaben sind restriktiv zu setzen. Die Darstellung ist soweit nicht 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.

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

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.

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.

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.

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 ist mit einem Drittprodukt durch den Endanwender umzusetzen.

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.

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.

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.

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.

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.

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.

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.

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

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

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 unter FAQ 2a, 2b 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)

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 folgendem OnePager 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)

E-Mail: Bei Noten ist beim E-Mail-Versand eine Verschlüsselung notwendig. Die Umsetzungshinweise können Sie dem folgenden OnePager 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)

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 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)

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.

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, und verschlüsselt abgelegt werden. Die

Zugriffsberechtigungen müssen restriktiv eingestellt werden.

Hinweis: Der Verwaltungsbereich der BayernCloud Schule steht voraussichtlich im ersten Quartal 2025 zur Verfügung.

ja

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

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 ByCS-Dienst-E-Mail).

Der Messenger bietet meist eine Ende-zu-Ende-Verschlüsselung. Die Nachrichten können in diesem Fall nur durch die beiden Kommunikationspartner im Klartext gelesen werden.

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.

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

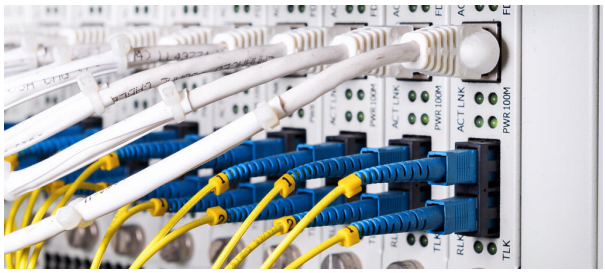
Downloads

Hinweise zur Schutzbedarfsfeststellung https://www.km.bayern.de/download/4-24-04/Schutzbedarfsermittlung.pdf

OnePager Sichere E-Mail-Kommunikation https://www.km.bayern.de/download/4-24-04/OnePager_sichere_E-Mail-Kommunikation.pdf

Leitfaden „Erkennen einer Phishing-E-Mail" https://www.km.bayern.de/download/4-24-04/Erkennen_von_Phishing_Mails.pdf

Schulnetz



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

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).

Die Aufteilung der Netzbereiche Verwaltung und Unterrichtsnetz ist begründet und bewährt. Eine Trennung auf Netzwerkebene kann zur Übersichtlichkeit beitragen und die Sicherheit prinzipiell erhöhen. Dies allein ist kein Garant für den Schutz von Daten.

Für einen effektiven Schutz müssen alle Ebenen berücksichtigt werden.

Berechtigungsmatrix

Eine Schule muss festlegen, auf welche Netze, Server oder Clouddienste der Schule die einzelnen Benutzer Zugang haben. Dabei sind stets das need-to-know-Prinzip und die gesetzlichen Vorgaben zu beachten. Aus der Berechtigungsmatrix muss ersichtlich sein, welche Dienste aus dem Verwaltungsnetz bzw. aus Unterrichtsnetz erreichbar sind.

Die Berechtigungsmatrix ist zu Dokumentationspflichten zu verakten und vor unberechtigtem Zugang zu schützen.

Zielgruppe: Schulleitung, Systembetreuer

Beispiel einer Berechtigungsmatrix https://www.km.bayern.de/download/4-24-02/Beispiel-Berechtigungsmatrix.pdf

Muster Berechtigungsmatrix https://www.km.bayern.de/download/4-24-02/Mustertabelle-Berechtigungsmatrix.docx

---

Fernzugriff auf das Verwaltungsnetzwerk

Fernzugänge ermöglichen z. B. der Schulleitung den flexiblen Zugriff auf Daten und Technikern die Möglichkeit, administrative Arbeiten per Fernzugriff auszuführen.

Bei der Verarbeitung personenbezogener Daten sind besondere Anforderungen an das Thema Datenschutz zu stellen. Vertraulichkeit, Authentizität und Datenintegrität müssen bei der Kommunikation berücksichtigt werden.

Zielgruppe: Systemadministratoren; Sachaufwandsträger

Auf welche Weise ein Zugang zum Verwaltungsnetz bereitgestellt werden kann, wird von drei Voraussetzungen (Personengruppe, Endgerät und Technik) bedingt.

Alle Kriterien müssen bei einer Entscheidung berücksichtigt werden und können situativ Ausgangspunkt der Betrachtung sein.

Die Schablone soll die verschiedenen Möglichkeiten aufzeigen, z. B.: Eine Lehrkraft sollte mit seinem mobilen Endgerät über eine Terminalservice auf eine bestimmte Anwendung im Verwaltungsnetz zugreifen können.

Der Systembetreuer sollte mit seinem mobilen Endgerät über eine VPN-Lösung oder über eine RDP-Lösung auf das Verwaltungsnetz zugreifen können, um Wartungsarbeiten vornehmen zu können.

Darstellung der Kriterien https://www.km.bayern.de/download/4-24-02/Darstellung-der-Kriterien.pdf

Beschreibung der Technik https://www.km.bayern.de/download/4-24-02/Beschreibung-der-Technik.pdf

Verschlüsselu

ng

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

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

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)

Der Inhalt eines Dokuments wird verschlüsselt. Der Dateiname ist normalerweise im Klartext vorhanden.

Beispiel: Verschlüsselung in Office-Programmen

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.

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 (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).

Für MacOS bietet das Programm Keka ähnliche Funktionen wie 7-Zip für

Windows. Komprimierte und verschlüsselte Ordner sind zwischen den Programmen kompatibel.

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 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 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.