Bildnachweis: Gorodenkoff – stock.adobe.com

IT-SICHERHEIT FÜR SCHULEN

IT-Bedrohungen meistern:

Basisempfehlungen für Schulträger und Entscheider

BÜNDNIS FÜR BILDUNG

Impressum

Herausgeber
Bündnis für Bildung e.V.
Oranienburger Str. 32
10117 Berlin

www.bfb.org
bfb@b-f-b.net

Dieser Leitfaden ist in der Arbeitsgruppe Infrastruktur entstanden.

Autoren
Franziska Divis, Microsoft
Lara Fechter, Relution
Jürgen Große-Ophoff, Bielefeld
Jens Kemper, Dataport
Patrick Kleene, Landkreis Emsland
Sabrina Marohn, Bündnis für Bildung
Herbert Millemann, Landkreis Aschaffenburg
Peter Schrell, HPE Aruba
Marcel Seewald, Bechtle
Werner Umbach, Landkreis Kassel
Frank Wüst, Nürnberg

Layout & Satz
www.eschdesigns.de

Berlin, Bündnis für Bildung, Februar 2026

Bündnis für Bildung
Das Bündnis für Bildung ist ein gemeinnütziger Verein, der es sich zum Ziel gesetzt hat, den digitalen Wandel im Bildungsbereich zu unterstützen. Zu unseren Mitgliedern zählen Städte, Kommunen und Bundesländer genauso wie IT-Unternehmen, Start-ups und Verlage, die sich für die Entwicklung und Umsetzung von Standards und Referenzlösungen für Bildung und Infrastrukturen in Lehr- und Lernumgebungen engagieren. Das Bündnis für Bildung ist firmenunabhängig und ideeller Träger dieser Mission. Durch aktive Arbeitsgruppen arbeitet das Bündnis für Bildung, der Neutralität verpflichtet, an Lösungsansätzen, Referenzmodellen und Rahmenarchitekturen für aktuelle Herausforderungen bei der Bildung in einer digitalen Welt.

Inhalt

Vorwort 4

Einleitung 6

Reale IT-Sicherheitsvorfälle an Schulen 8

Bedrohungs-Szenarien 10
Unberechtigter physischer Zugriff auf Server- oder Technikräume 10
Unberechtigter Zugriff auf IT-Systeme 11
Externe Störfaktoren für den IT-Betrieb: Risiken und Auswirkungen auf die Infrastruktur 12
Ausfall des Betriebs durch interne Faktoren 14
Verlust oder Diebstahl von Hardware 15
Herausforderung: Fehlende IT-Kompetenzen und personelle Engpässe im Schulbetrieb 16

IT-Sicherheit: Top 10 Sofortmaßnahmen für Schulen – Checkliste für den digitalen Schulalltag 18

Verantwortlichkeiten und Zuständigkeiten in der Schul-IT: Wer trägt welche Rolle? 24
Sichere Schul-IT beginnt mit Verantwortung – und Bewusstsein 24
Wer ist wofür verantwortlich? 24
Exkurs: Das Problem mit der Weisungsbefugnis 25
Viele Netze – viele Anforderungen – viele Risiken 26
Zero Trust als technisches und organisatorisches Prinzip 26

Die Kommunikation im Krisenfall 28
Grundsätze der Kommunikation 28
Ablauf bei einem Sicherheitsvorfall 29
Mitglieder des Krisenteams 30
Kommunikationsmatrix 31

Dokumentation präventiver Maßnahmen 32

Fazit 33

Glossar 34

Abstract

Dieser Leitfaden bündelt die zentralen technischen, organisatorischen und personellen Sicherheitsaspekte für Schulen und dient als kompaktes Entscheidungsdokument für Schulträger, Kommunen und Verantwortliche. Ergänzend zu den bereits etablierten Ratgebern, die primär auf den Vorgaben des BSI-Grundschutzes und den Anforderungen der ISO 27001-Zertifizierung basieren, verfolgt dieser Leitfaden eine gezielt praxisorientierte Herangehensweise. Er analysiert reale Bedrohungsszenarien – von Cyberangriffen und Datenverlust bis hin zu physischem Diebstahl – und zeigt deren gravierende Auswirkungen auf den Schulbetrieb und die Beteiligten auf. Das Dokument definiert klare Zuständigkeiten zwischen Schulträger und Schulleitung und bietet mit einer „Top-10-Checkliste“ sowie Handlungsempfehlungen für den Krisenfall eine praxisnahe Orientierungshilfe. Ziel ist es, IT-Sicherheit als unverzichtbares Fundament für eine rechtssichere und verlässliche digitale Bildung zu etablieren.

Hinweis:

Aus Vereinfachungsgründen wird in diesem Dokument der Begriff ‚Schulträger‘ einheitlich als Synonym für die Aufgaben und Verantwortlichkeiten eines Sachaufwandsträgers verwendet.

Im Sinne einer besseren Lesbarkeit wird in diesem Text die männliche Form ‚Schüler‘ als geschlechtsneutraler Begriff verwendet. Diese Bezeichnung schließt ausdrücklich alle Geschlechter ein

VORWORT

Sicherheit als Fundament der digitalen Bildung: IT-Infrastruktur nachhaltig schützen

Die digitale Transformation des Bildungswesens hat die Schullandschaft in Deutschland nachhaltig verändert. Durch Programme wie den Digitalpakt Schule wurde die Basis geschaffen. Doch mit der zunehmenden Vernetzung und dem Einsatz digitaler Endgeräte wachsen auch die Risiken: IT-Sicherheit ist heute keine optionale Ergänzung mehr, sondern die Grundvoraussetzung für einen stabilen und vertrauenswürdigen Schulalltag. Das Bündnis für Bildung (BfB) setzt sich daher mit dem vorliegenden Leitfaden dafür ein, Sicherheitsaspekte systematisch in die schulische Infrastruktur zu integrieren.

Gründe für eine professionelle IT-Sicherheit in Kürze:

- **Schutz sensibler Daten:** Die persönlichen Informationen von Schülern und Lehrkräften müssen vor unbefugtem Zugriff und Missbrauch geschützt werden.
- **Aufrechterhaltung des Schulbetriebs:** Ein wirksames Sicherheitskonzept verhindert digitale Handlungsunfähigkeit durch Cyberangriffe oder Systemausfälle.
- **Vertrauen in digitale Werkzeuge:** Nur eine sicher betriebene Infrastruktur schafft die nötige Akzeptanz bei Lehrkräften, Eltern und Lernenden.

Voraussetzungen für eine sichere Schulinfrastruktur:
Die Umsetzung eines hohen Sicherheitsniveaus erfordert koordinierte Anstrengungen von Schulträgern und Schulen, unterstützt durch die Politik.

- **Klare Verantwortlichkeiten:** IT-Sicherheit kann nur funktionieren, wenn Zuständigkeiten zwischen Technik (Schulträger) und pädagogischer Nutzung (Schule) eindeutig definiert sind.

- **Ressourcen für Prävention:** Mittel müssen nicht nur für Hardware, sondern explizit für Sicherheitssysteme (z. B. MDM, Backup-Lösungen, USV) bereitgestellt werden.
- **Zentrale Administration:** Sicherheitsrelevante Aufgaben wie Patch-Management, Netzwerksegmentierung und Firewall-Betrieb müssen professionell und zentral gesteuert werden.
- **Qualifizierung und Awareness:** Regelmäßige Schulungen sind essenziell, um Lehrkräfte und Schüler für Gefahren wie Phishing zu sensibilisieren.

Aktuelle Herausforderungen:
Oftmals ist die Verantwortung für IT-Sicherheit diffus verteilt, was im Ernstfall zu gegenseitigen Schuldzuweisungen führt. Während Schulträger auf begrenzte Budgets verweisen, sehen sich Schulleitungen mit der technischen Komplexität überfordert. Das Fehlen ganzheitlicher Sicherheitskonzepte führt dazu, dass Schulen bei Vorfällen – wie Ransomware-Angriffen oder Hardwareverlust – ungeschützt sind und hohe Kosten sowie Imageverluste entstehen.

Das Bündnis für Bildung empfiehlt in diesem praxisorientierten Leitfaden Schulträgern und politischen Entscheidungsträgern, IT-Sicherheit als integralen Teil der Infrastrukturplanung zu betrachten und langfristig zu finanzieren. Nur durch professionelle Betreuung, den Einsatz moderner Prinzipien wie „Zero Trust“ und die Etablierung von Krisenteams kann die Resilienz des Bildungssystems gestärkt werden.

Dieser Leitfaden dient als Orientierungshilfe, um technische, organisatorische und personelle Schutzmaßnahmen effektiv umzusetzen. Er zeigt Wege auf, wie durch klare Kommunikation und präventives Handeln ein sicherer Raum für die pädagogische Arbeit im digitalen Zeitalter geschaffen werden kann.

EINLEITUNG

WARUM IT-SICHERHEIT AN SCHULEN UNVERZICHTBAR IST

Die vergangenen Jahre haben der Schullandschaft in Deutschland, unter anderem durch die Förderprogramme des Digitalpakts Schule, einen gewaltigen Schub in der Digitalisierung von Unterricht und Verwaltung gebracht. Das bringt nicht nur zahlreiche Vorteile, sondern auch erhebliche Sicherheitsrisiken mit sich. In diesem Zusammenhang ist es von entscheidender Bedeutung, die verschiedenen Aspekte der Sicherheit zu verstehen und geeignete Maßnahmen zu ergreifen, um die sensiblen Daten von Schülerinnen und Schülern zu schützen.

Ein fiktiver Vorfall zeigt, wie verwundbar Schulen gegenüber Cyberangriffen sind:

„An einem Montagmorgen öffnet ein Lehrer einer Gesamtschule eine vermeintlich dienstliche E-Mail mit dem Betreff „Wichtige Stundenplanänderung“. Der Anhang enthält Ransomware (Schadsoftware), die sich innerhalb weniger Minuten im gesamten Schulnetzwerk ausbreitet. Digitale Tafeln, Verwaltungssoftware, Lernplattformen und sogar die Telefonanlage fallen aus – die Schule ist in vielen Bereichen handlungsunfähig.“

Die Folgen sind gravierend: Der Schulträger muss für sein Gesamtsystem über 250.000 € für IT-Forensik, neue Hardware und externe Beratung aufbringen und sieht sich öffentlicher Kritik und datenschutzrechtlichen Prüfungen ausgesetzt. Die Schulleitung steht unter massivem Druck, da der Unterricht teilweise ausfällt und die Kommunikation mit Eltern und Lehrkräften nur noch über private Kanäle möglich ist. Das Vertrauen in die digitale Organisation der Schule ist erschüttert.

Besonders betroffen sind die Lernenden: Persönliche Daten wie Adressen, Noten, Förderpläne und psychologische Gutachten werden gestohlen und im Darknet veröffentlicht. Die Lernplattformen bleiben wochenlang offline – insbesondere Abschlussklassen geraten in der Prüfungsvorbereitung in Rückstand.

Auch die Lehrkräfte sind betroffen: Unterrichtsmaterialien und digitale Klassenbücher sind verschlüsselt oder gelöscht. Viele fühlen sich im Umgang mit der IT überfordert und unzureichend geschult. Für die Lehrkraft, die die Schadsoftware unbeabsichtigt aktiviert hat, sind eventuelle dienstrechtliche Konsequenzen zu prüfen.

Dieser Vorfall verdeutlicht, wie wichtig es ist, IT-Sicherheit an Schulen systematisch und professionell zu gestalten. Ein wirksames Sicherheitskonzept schützt nicht nur Daten und Infrastruktur, sondern auch das Vertrauen und die psychische Gesundheit aller Beteiligten.

Verantwortung – ein Spiel mit der Zuständigkeit

Nach dem Vorfall an der Gesamtschule wurde schnell deutlich, dass die Zuständigkeit häufig nicht eindeutig geregelt ist. Der Schulträger verweist auf mangelnde Ressourcen finanzieller und personeller Art. Die Schulleitung sieht sich mit den technischen Anforderungen, fehlenden Schulungen und ebenfalls zu wenig Personal überfordert.

Lehrkräfte beklagen mangelnde Unterstützung und unklare Zuständigkeiten, während sie gleichzeitig für fahrlässiges Verhalten kritisiert werden. Eltern fordern Aufklärung und Schutz, Lernende, deren Daten betroffen sind, äußern Misstrauen gegenüber allen Beteiligten.

Statt gemeinsam Lösungen zu entwickeln, entsteht ein Klima der Unsicherheit und des Rückzugs. Der Vorfall zeigt: IT-Sicherheit kann nur funktionieren, wenn alle Beteiligten Verantwortung übernehmen – abgestimmt, transparent und mit klaren Zuständigkeiten.

Mit diesem Papier wollen wir Ihnen die relevanten Sicherheitsaspekte – von physischer Sicherheit über Cybersecurity bis Datenschutz – erläutern und praxisnah darstellen, wie sich Schulträger und Schulen wirksam schützen können. Wie oben beschrieben, ist dabei die Zusammenstellung von Krisenteams und die klare Definition von Zuständigkeiten die Grundlage, um schnell und adäquat reagieren zu können. Darüber hinaus wird eine detaillierte Handlungsempfehlung für die Entwicklung einer zukunftssicheren Schulinfrastruktur erarbeitet, die eine langfristige Planung ermöglicht. Besonders wichtig sind die praktischen Hinweise für den Umgang mit konkreten Bedrohungen wie Netzunterbrechungen und Phishing-Attacken, die Schulen in die Lage versetzen, schnell und adäquat zu reagieren. Deshalb haben wir in dem Papier auch die Verantwortlichkeiten farblich gekennzeichnet.

Inhaltliche Abgrenzung:

In diesem Leitfaden steht die IT-Sicherheit im Mittelpunkt. Sie ist ein Teilbereich der Informationssicherheit, mit Fokus auf die technischen Aspekte des Schutzes. Während Datenschutz rechtliche Anforderungen an den Umgang mit personenbezogenen Daten stellt und Datensicherheit sich auf den Schutz von Daten allgemein konzentriert, betrachtet die IT-Sicherheit insbesondere die technischen und organisatorischen Maßnahmen und Systeme, die zur Erreichung dieser Schutzziele beitragen.

Im Kontext der Datensouveränität ergibt sich hierbei ein spezifisches Compliance-Dilemma, da die Nutzung internationaler Cloud-Strukturen oft zu rechtlichen Zielkonflikten zwischen außereuropäischen Zugriffsbefugnissen und EU-Datenschutzstandards führt. Diese Diskrepanz erfordert von Schulträgern, technische Sicherheitsmaßnahmen und die rechtliche Souveränität über die Daten ihrer Lernenden in einem integrierten Risikomanagement zu bewerten. Nur durch eine ganzheitliche Betrachtung lässt sich eine strategische Abhängigkeit minimieren und die rechtliche Sicherheit im digitalen Raum langfristig gewährleisten.

REALE IT-SICHERHEITS-VORFÄLLE AN SCHULEN

Die folgenden Praxisbeispiele geben einen Überblick über reale, breitgefächerte Bedrohungsszenarien.

Die große Relevanz des Themas IT-Sicherheit im Bildungsbereich wird besonders deutlich, wenn man konkrete Schadensfälle betrachtet, bei denen erheblicher Schaden entstanden ist. Im Folgenden werden einige reale Vorfälle aus unterschiedlichen Quellen kurz zusammengefasst, um die sicherheitsrelevanten Risiken und ihre Auswirkungen zu verdeutlichen:

1. Datenverlust auf Tablets in einer Notizen-App

Vorfall: Durch einen Fehler im städtischen Schulnetzwerk wurden 485 iPads abgemeldet, wodurch die Notizen-App gelöscht wurde. Viele Schüler verloren dadurch ihre über Jahre gesammelten Abiturvorbereitungen [1].

Sicherheitsaspekt: Fehlende Backup-Strategie und unzureichende Kommunikation über Datensicherungspflichten.

Lösungsansatz: Zentrale Backup-Systeme, Schulung zur Datensicherung, klare Zuständigkeiten.

2. Cyberangriff in 45 Schulen (Ransomware)

Vorfall: Ein externer IT-Dienstleister wurde Ziel eines Ransomware-Angriffs. 45 Schulen waren betroffen, Server wurden verschlüsselt [2].

Sicherheitsaspekt: Auch externe Dienstleister können betroffen sein.

Lösungsansatz: Entsprechende Personal-Kompetenzen aufbauen, mindestens für Vergaben und Steuerung der Dienstleister

3. Polizeibericht zum selben Cyberangriff

Vorfall: Die Polizei bestätigte, dass professionelle Täter Zugriff auf Schulserver hatten, Daten verschlüsselten und mit deren Veröffentlichung drohten [3].

Sicherheitsaspekt: Datenabfluss und Erpressung, unzureichende Verschlüsselung und Monitoring.

Lösungsansatz: Verschlüsselung sensibler Daten, Monitoring-Systeme, Incident-Response-Teams.

4. Technische Störung im Schulbetrieb

Vorfall: Eine technische Störung legte den Schulbetrieb lahm, der Unterricht fiel aus [4].

Sicherheitsaspekt: Mangelhafte Redundanz und Notfallplanung.

Lösungsansatz: Ausfallsichere Systeme, Notfallpläne für digitalen Unterricht.

5. Schüler hackt Schul-IT

Vorfall: Ein Schüler installierte mit Mitschülern Keylogger, spähte Lehrerdaten aus und wurde an eine andere Schule versetzt [5].

Sicherheitsaspekt: Unzureichende Zugangskontrollen und Überwachung.

Lösungsansatz: Härtung von Endgeräten, Schulung zur IT-Ethik, Logging- und Alarmsysteme.

6. Hochwasser beeinträchtigt Schulbetrieb

Vorfall: Überflutungen führten zu Schulschließungen und IT-Ausfällen [6].

Sicherheitsaspekt: Physische Gefährdung der IT-Infrastruktur.

Lösungsansatz: Standortanalyse, Schutzmaßnahmen gegen Naturgefahren, Cloud-Backups.

7. Serverraum-Einbruch im Gymnasium

Vorfall: Einbrecher entwendeten IT-Hardware aus dem Serverraum eines Gymnasiums [8].

Sicherheitsaspekt: Unzureichende physische Sicherung und Alarmierung.

Lösungsansatz: Videoüberwachung, Alarmanlagen, verschlossene Racks, Zutrittskontrollen.

8. Software-Update macht Schulcomputer unbrauchbar

Vorfall: Ein Update des Betriebssystems führte dazu, dass Schul-PCs nicht mehr funktionierten [9].

Sicherheitsaspekt: Fehlendes Testmanagement und Update-Kontrolle.

Lösungsansatz: Staging-Umgebungen (zugewiesene Nutzungsrechte), zentrale Update-Verwaltung, Rollback-Strategien.

Diese Beispiele zeigen eindrücklich, wie vielfältig und gravierend die Folgen von IT-Sicherheitsvorfällen im Schulbereich sein können – von Datenverlust über Betriebsunterbrechungen bis hin zu gezielter krimineller Ausspähung.

Referenzen

[1] Abitur-Albtraum in Koblenz wegen iPad-Datenverlusten
[2] Cyberangriff trifft zahlreiche Schulen in Rheinland-Pfalz
[3] Mehrere Schulen in Rheinland-Pfalz von Cyberangriff betroffen
[4] Bogestra: Die Bochum-Gelsenkirchener Straßenbahnen AG – WAZ.de
[5] Angriff auf Schul-IT: Schüler muss Schule verlassen
[6] In Passau gehört Hochwasser dazu – Süddeutsche.de
[7] Das NCG trifft sich im virtuellen Klassenzimmer
[8] WAZ | Bochum Lokalredaktion

BEDROHUNGS-SZENARIEN

In diesem Kapitel werden verschiedene Schadensfälle vorgestellt. Zu Beginn finden Sie jeweils eine kompakte Definition der Bedrohung sowie deren mögliche Auswirkungen. Anschließend werden konkrete präventive Maßnahmen beschrieben, mit denen sich die jeweiligen Angriffe wirksam verhindern lassen. Abschließend folgen Handlungsempfehlungen für den Ernstfall, die aufzeigen, welche Schritte im Schadensfall zu ergreifen sind.

Hinweis:

Aus Vereinfachungsgründen wird der Begriff ‚Schulträger' einheitlich als Synonym für die Aufgaben und Verantwortlichkeiten eines Sachaufwandsträgers verwendet.

Unberechtigter physischer Zugriff auf Server- oder Technikräume

Definition und Ausgangslage

Unberechtigter physischer Zugriff bezeichnet das Eindringen von Personen ohne entsprechende Autorisierung in sicherheitskritische Bereiche wie Serverräume oder Technikräume. Solche Zugriffe können zu Datenverlust, Sabotage, Diebstahl oder Manipulation der IT-Infrastruktur führen und stellen ein erhebliches Sicherheitsrisiko dar.

Präventive Maßnahmen

Zutrittskontrolle:
Einsatz von Schlüsselkarten, biometrischen Systemen oder PIN-Codes.
SCHULTRÄGER

Videoüberwachung:
Kameraüberwachung der Innenbereiche des Serverraums. Zutritte und Außenbereiche ggf. kritisch: Datenschutz beachten.
SCHULTRÄGER

Protokollierung:
Elektronische Erfassung und Überwachung aller Zutritte (Zutrittsprotokolle).
SCHULTRÄGER

Zutrittsbeschränkung:
Zugang nur für autorisierte Personen, keine Sammelzutritte.
SCHULTRÄGER SCHULLEITUNG

Tür-/Schlossüberwachung:
Alarm bei unbefugtem Öffnen oder gewaltsamem Zugriff.
SCHULTRÄGER

Begleitpflicht:
Externe Personen (z. B. Techniker) nur mit interner Begleitung.
SCHULTRÄGER SCHULLEITUNG

Schulung der Mitarbeitenden:
Sensibilisierung für physische Sicherheit und mögliche Gefahren.
SCHULTRÄGER SCHULLEITUNG

Kennzeichnung und Abschottung:
Technikräume klar kennzeichnen und baulich absichern (z. B. Brandschutztüren, keine Fenster).
SCHULTRÄGER

Regelmäßige Audits:
Kontrolle der Zutrittsberechtigungen und der technischen Schutzmaßnahmen.
SCHULTRÄGER

Verhalten im Schadensfall

Zugriffsversuch oder Vorfall melden:
Sofortige Information an IT-Security und ggf. staatliche Behörden.
SCHULLEITUNG

Zutritt dokumentieren:
Zeitpunkt, beteiligte Personen, ggf. Kameraaufzeichnungen sichern.
SCHULTRÄGER SCHULLEITUNG

Betroffene Systeme prüfen:
Überprüfung auf Manipulation, Datenverlust oder Schadsoftware.
SCHULTRÄGER

Zugang sperren:
Temporäres Sperren von Zugangsberechtigungen bei Verdacht.
SCHULTRÄGER

Externe Stellen informieren:
Je nach Vorfall ggf. Datenschutzbeauftragten oder Behörden einschalten.
SCHULTRÄGER SCHULLEITUNG

Nachbereitung:
Ursachenanalyse und Verbesserung der Schutzmaßnahmen.
SCHULTRÄGER SCHULLEITUNG

Unberechtigter Zugriff auf IT-Systeme

Definition und kurze Erläuterung der Bedrohung

Unberechtigter Zugriff bezeichnet den Versuch oder die erfolgreiche Handlung, sich ohne entsprechende Berechtigung Zugang zu einem IT-System, Netzwerk oder Rechenzentrum zu verschaffen. In Schulen kann dies durch externe Angreifer (z. B. Hacker) oder interne Personen (z. B. Schüler und Schülerinnen oder Mitarbeitende ohne entsprechende Rechte) geschehen. Ziel solcher Zugriffe kann das Ausspähen, Manipulieren oder Löschen sensibler Daten sein – etwa Schülerakten, Prüfungsunterlagen oder Verwaltungsdaten. Auch die Störung des Schulbetriebs durch Sabotage oder Schadsoftware zählt zu den Risiken.

Präventive Maßnahmen

Zero-Trust:
Modernes Sicherheitskonzept nach dem Prinzip „Vertraue niemandem – überprüfe alles".
JEDER

Netzwerkzugangskontrolle (NAC):
Authentifizierung und Autorisierung aller User/Geräte, die mit dem Netzwerk verbunden sind.
SCHULTRÄGER

Netzwerksegmentierung:
Aufteilung des Netzwerks in verschiedene Segmente verhindert die unkontrollierte Ausbreitung von Bedrohungen.
SCHULTRÄGER

Firewall & IDS/IPS:
Zur Kontrolle und Analyse des Datenverkehrs auf Bedrohungen
SCHULTRÄGER

Patch-Management:
Regelmäßige Software-Updates schließen Sicherheitslücken und halten die Systeme stabil
SCHULTRÄGER

Starke Authentifizierungsverfahren:
Mindestens sichere Passwörter, besser Multi-Faktor-Authentifizierung
SCHULTRÄGER

Endpoint-Security:
Maximale Absicherung der Endgeräte, um unberechtigte Zugriffe durch kompromittierte Geräte zu vermeiden
JEDER

Sensibilisierung & Schulung:
Regelmäßige Aufklärung und Schulung aller Nutzer über mögliche Sicherheitsrisiken
SCHULTRÄGER SCHULLEITUNG

Audits & Pen-Tests:
Durch regelmäßige Audits und Penetrationstest Schwachstellen erkennen, bevor sie ausgenutzt werden
SCHULTRÄGER

Verhalten im Schadensfall

Vorfall melden:
an IT-Security und ggf. staatliche Behörden
SCHULTRÄGER SCHULLEITUNG

Betroffene Systeme isolieren:
um weitere Ausbreitung zu verhindern
SCHULTRÄGER

Vorfall dokumentieren:
Zeitpunkt, betroffene Systeme/Geräte/User, vermutete Ursachen, erste Maßnahmen
SCHULTRÄGER

Forensische Analyse:
um Ursache und Umfang des unberechtigten Zugriffs zu ermitteln
SCHULTRÄGER

Verbesserung der Schutzmaßnahmen:
Anpassung der Sicherheitsstrategie aus den Erkenntnissen der Analyse
SCHULTRÄGER SCHULLEITUNG

Externe Störfaktoren für den IT-Betrieb: Risiken und Auswirkungen auf die Infrastruktur durch externe Faktoren

Definition und Ausgangslage

Die IT-Infrastruktur ist die Grundlage zum Betrieb jedweder Anwendungssoftware, die in einer Schule genutzt wird. Sie umfasst Teile der Gebäude, die Hardware vom Server bis zu den Endgeräten, das Netzwerk und die Software. Störungen des Betriebs können durch Beeinträchtigungen in all diesen Bereichen auftreten, hier werden die häufigsten extern verursachte Störungen – mit Ausnahme von Cyberangriffen – beleuchtet.

- Wegen fehlender oder zu wenig installierter USV zieht selbst ein „kurzer“ Stromausfall den Zusammenbruch des IT- Systems und somit den Stillstand der Schule nach sich.

- Ist die Internetanbindung der Schule durch z. B. Erdarbeiten gestört, betrifft dies häufig auch die VoIP-Telefonanlage. Eine Erreichbarkeit der Schule, insbesondere im Notfall, ist dann nicht mehr gegeben.
- Wasserschäden durch Starkregen oder Überflutungen, nicht nur im IT-Raum, können die Verfügbarkeit erheblich einschränken.
- Ausfall der Kühlung und Klimatisierung in wichtigen IT-Räumen. Kleine oder schlecht gewählte Räume („gewachsene Struktur“, z. B. Dachboden), eine unterdimensionierte Klimaanlage, durch Laub und Pollen verschmutzte Anlagen, können bei vermehrt auftretenden heißen Tagen zu Ausfällen führen.

Präventive Maßnahmen

Allgemein:
Automatische Überwachung der Infrastruktur, Temperatur, Strom, Luftfeuchte, Leckage im Serverraum, Einsatz einer Gefahrenmeldeanlage.
SCHULTRÄGER

Brandschutz:
Eigener Brandabschnitt, Brandmeldeanlage, Brandfrüherkennung, Löschsystem, Reduzierung der Brandlast im Serverraum, Minimierung von Brandgefahren aus Nachbarbereichen.
SCHULTRÄGER

Stromversorgung:
Einsatz einer oder mehrerer USVs, Implementierung eines Notstromaggregats, Überwachung der Stromversorgung. Ein weiterer anders geführter Stromanschluss.
SCHULTRÄGER

Blitz:
Grob- und Mittelschutz in den Verteilungen, Überspannungsschutz im Serverschrank
SCHULTRÄGER

Wasser:
Einfache Lecküberwachung der Wasserleitungen, z. B. auch in den Nachbarbereichen.
SCHULTRÄGER

Kühlung/Klimatisierung:
Überwachung Betriebszustand, regelmäßige Wartung. Hier auch die über die Zeit gewachsenen Anforderungen einbeziehen. Können bei den betroffenen Räumen z. B. Fassaden beschattet werden?
SCHULTRÄGER

Test:
Regelmäßige Durchführung von Funktionstests der technischen Infrastruktur und der Meldewege.
SCHULTRÄGER

Zusätzlich zum Serverraum:
Vermeidung von Leitungen mit gefährdenden Flüssigkeiten oder Gasen im Serverraum, Schutz von Zuleitungen vor versehentlicher Beschädigung, Schutz vor Schäden durch Brand und Rauchgase.
SCHULTRÄGER

Kommunikationsleitungen:
Eine zweite Leitung, eventuell über einen anderen Provider als Back-Up für die Telefonie und das Internet bereitstellen, alternativ mobilfunkfähige Geräte als Reserve anschaffen.
SCHULTRÄGER

Generell Redundanzen der Systeme schaffen:
Bei Auswahl und Beschaffung der Geräte auf Redundanzen achten. Doppelte Strom-/Netzwerkanbindung, Gerätestandardisierung, Lastverteilungen auf

verschiedene Systemkomponenten. Vermeidung von Single-Point-of-Failure-Strukturen, dies verhindert Kettenreaktionen und damit den Ausfall der gesamten Infrastruktur.

SCHULTRÄGER

Verhalten im Schadensfall

- Redundanzweg oder -gerät in Betrieb nehmen
- Alle oben beschriebenen Gefahren und deren Eintritt können im Einzelfall mit erheblichen Risiken beim Wiedereinschalten verbunden sein; sei es aus versicherungstechnischen Gründen oder weil nach Eintritt der Gefahrensituation die eigentliche Funktionstüchtigkeit der Systeme nicht klar ist. Deshalb ist das Vorhandensein von Schutzsystemen sowie deren regelmäßige Prüfung unerlässlich.

Verantwortliche Stellen beim Schulträger

- Planer
- Haustechnik
- IT-Sicherheitsbeauftragte/IT-Verantwortlicher für die Abschätzung der Gefahrenabwehr und -erkennung, sowie den benötigten Schutzbedarf oder -grad für die IT-Systeme

Ausfall des Betriebs durch interne Faktoren

Definition und kurze Erläuterung der Bedrohung

Durch Fehler in der internen Abwicklung kann es zu Ausfällen einzelner Programme oder ganzer Systeme kommen, z. B. wenn nicht rechtzeitig notwendige Updates installiert werden.

Mögliche Folgen

- Datenverlust durch automatische Löschung von Programmzugängen infolge fehlender oder nicht verlängerter Lizenzen.
- Erhöhte Gefahr erfolgreicher Angriffe durch nicht geschlossene Sicherheitslücken, da Updates nicht installiert wurden oder Systeme nicht mehr updatefähig sind.
- Unzureichende oder fehlende Sicherheitseinstellungen in Systemen, wenn durch mangelhafte Dokumentation bei Mitarbeiterwechseln relevantes Wissen verloren geht.

Präventive Maßnahmen

Aufstellung einer Gesamtübersicht aller eingesetzten Systeme und Programme mit Laufzeit, Lizenzstand, aktueller Version und ggfs. zusätzlicher Anforderungen (z. B. Zertifikate).

SCHULTRÄGER

Umgehendes Handeln bei gravierenden Gefahren (ablaufende Lizenzen, veraltete Versionen).

SCHULTRÄGER SCHULLEITUNG

Erweiterung der Aufstellung um die Dokumentation der tatsächlichen Sicherheitseinstellungen (ggfs. Abgleich mit frei verfügbaren Vorschlägen).

SCHULTRÄGER

Abgleich der eigenen Updateversion mit der vom Hersteller zur Verfügung gestellten Version und ggfs. Update einspielen.

SCHULTRÄGER

Aufstellung der (möglichen) Backup-Systeme für die in den verschiedenen Systemen gespeicherten Daten; wenn nicht vorhanden: Backup-Konzept initiieren.

SCHULTRÄGER SCHULLEITUNG

Einführung einer Testumgebung zur Prüfung von Software und Updates vor der Installation im System.

SCHULTRÄGER

Information an alle Nutzer zur eigenverantwortlichen Datensicherung (mit Anleitungen).

SCHULTRÄGER SCHULLEITUNG

Hoch relevante und sensible Daten müssen auf administrierten Speicherorten gesichert werden, damit im Zweifelsfall weitere Personen Zugriff erhalten können.

SCHULTRÄGER SCHULLEITUNG

Verhalten im Schadensfall

Abschaltung von Geräten, Systemen und Netzen im Angriffsfall.

SCHULTRÄGER SCHULLEITUNG

Sofortige Installation von aktuellen Programmversionen und Sicherheitsupdates.

SCHULTRÄGER SCHULLEITUNG

Verhandlung mit den Herstellern bez. Lizenzverlängerungen.

SCHULTRÄGER

Prüfen ob Backups zum Wiedereinspielen vorhanden sind.

SCHULTRÄGER

Transparente Information an alle Nutzer herausgeben.

SCHULTRÄGER SCHULLEITUNG

Verlust oder Diebstahl von Hardware

Definition und Ausgangslage

Der Verlust oder Diebstahl von Hardware – etwa Laptops, Tablets, Smartphones oder Speichermedien – stellt ein erhebliches Sicherheitsrisiko dar. Neben dem materiellen Schaden droht vor allem der Verlust sensibler Daten, die auf den Geräten gespeichert sind. Besonders kritisch ist dies bei unverschlüsselten Geräten oder fehlender zentraler Verwaltung. Schulen sind durch offene Gebäude, wechselnde Nutzergruppen und mobile Endgeräte besonders gefährdet.

Typische Szenarien sind der Diebstahl von Tablets oder Laptops aus Klassen- oder Lehrerzimmern, der Verlust von USB-Sticks mit Schülerdaten, die Entwendung von Geräten bei Einbruch in Schulgebäude sowie das unbeaufsichtigte Zurücklassen von Geräten, die von Dritten mitgenommen werden.

Wir empfehlen, alle nachfolgenden Punkte in ihrer Gesamtheit zu berücksichtigen. Nur so kann sichergestellt werden, dass bei Diebstahl und Verlust keine gravierenden Folgeschäden auftreten.

Präventive Maßnahmen

Geräteverwaltung & Mobile Device Management (MDM):
Zentrale Verwaltung aller Endgeräte inkl. Fernlöschung und Standortverfolgung.

SCHULTRÄGER IT-VERANTWORTLICHE

Verschlüsselung:
Alle Geräte sollten mit starker Verschlüsselung ausgestattet sein.

SCHULTRÄGER IT-VERANTWORTLICHE

Zugriffsrechte:
Gerätezugang nur mit sicheren Passwörtern oder biometrischer Authentifizierung.
SCHULTRÄGER SCHULLEITUNG

Sensibilisierung: Schulung von Lehrenden und Lernenden zum sicheren Umgang mit Geräten.
SCHULTRÄGER SCHULLEITUNG

Kennzeichnung:
Geräte eindeutig als Schuleigentum durch Inventar-Aufkleber oder Gravuren markieren.
SCHULTRÄGER

Sicherer Aufbewahrungsort:
Geräte außerhalb der Unterrichtszeit in abschließbaren Schränken oder Räumen lagern, idealerweise im Obergeschoss und auf genügend Lagerfläche achten.
SCHULLEITUNG

Verhalten im Schadensfall

Sofortige Meldung:
Verlust oder Diebstahl umgehend der Schulleitung und dem IT-Team melden.
SCHULLEITUNG

Gerät sperren oder löschen:
Fernlöschung über MDM oder Sperrung des Zugangs.
IT-VERANTWORTLICHE

Dokumentation:
Zeitpunkt, Ort, betroffene Daten und Maßnahmen erfassen.
SCHULLEITUNG IT-VERANTWORTLICHE

Datenschutzbeauftragte/Datenschutzaufsichtsbehörde informieren:
Bei Verlust personenbezogener Daten (Art. 33 DSGVO) ist grundsätzlich eine Meldung an die Datenschutzbehörde erforderlich.
SCHULTRÄGER SCHULLEITUNG

Polizei einschalten:
Bei Diebstahl Anzeige erstatten.
SCHULTRÄGER SCHULLEITUNG

Herausforderung: Fehlende IT-Kompetenzen und personelle Engpässe im Schulbetrieb

In vielen Schulen fehlt es nicht nur an IT-Fachkräften, sondern auch an Unterstützung beim Aufbau grundlegender digitaler Kompetenzen. Eine einzelne Lehrkraft steht beispielsweise oft vor der Herausforderung, digitale Tools im Unterricht zu nutzen, ohne dafür ausreichend geschult zu sein. IT-Sicherheit ist dabei meist kein Bestandteil ihrer Ausbildung oder Fortbildung. Das führt dazu, dass Passwörter unsicher gewählt, Geräte falsch konfiguriert oder sensible Daten ungeschützt gespeichert werden.

Die meisten Nutzer sind mit Phishing-Mails, Malware oder dem sicheren Umgang mit Cloud-Diensten wenig vertraut. Sie erkennen Bedrohungen nicht oder reagieren falsch – nicht aus Fahrlässigkeit, sondern weil ihnen das nötige Wissen fehlt. Gleichzeitig sind sie für die digitale Infrastruktur ihrer Klasse verantwortlich, ohne permanente technische Unterstützung oder klare Sicherheitsrichtlinien.

Ein konkreter Fall zeigt, wie anfällig Schulen für Cyberangriffe sein können, wenn Nutzer

nicht ausreichend im Bereich IT-Sicherheit geschult sind. Ein Lehrer erhielt eine täuschend echt wirkende E-Mail, die angeblich von der Schulleitung stammte. In der Nachricht wurde er aufgefordert, ein geteiltes Dokument zu öffnen. Ohne Verdacht zu schöpfen, klickte der Lehrer auf den Link und gab seine Zugangsdaten auf einer gefälschten Login-Seite ein. Die Angreifer nutzten den Zugriff auf sein E-Mail-Konto, um weitere Phishing-Mails an Kollegen und Eltern zu versenden.

Typische Szenarien:

- Fehlende IT-Schulung bei Schulpersonal führt zu unsicherem Umgang mit digitalen Tools
- Nutzung privater Geräte ohne Sicherheitsvorgaben
- Speicherung sensibler Schülerdaten ohne Verschlüsselung
- Unkenntnis über Phishing, Malware und sichere Passwörter
- Fehlende Reaktion auf verdächtige E-Mails oder Systemwarnungen

Grundsätzliche präventive Maßnahmen (Verantwortlichkeiten)

Übergeordnetes Konzept zur Weiterbildung der Lehrkräfte.
SCHULLEITUNG BILDUNGSMINISTERIUM

Regelmäßige IT-Sicherheitsschulungen für Schulpersonal.
SCHULLEITUNG

Einführung verbindlicher IT-Richtlinien für Schulen.
SCHULTRÄGER

Bereitstellung sicherer, zentral verwalteter Geräte.
SCHULTRÄGER BUNDESLAND

Sensibilisierung für Datenschutz und sichere Kommunikation.
SCHULTRÄGER SCHULLEITUNG

Einbindung von IT-Fachpersonal zur Unterstützung im Alltag.
BUNDESLAND SCHULLEITUNG SCHULTRÄGER

Verhalten im Schadensfall (Verantwortlichkeiten)

Keine eigenständige Löschung oder Weiterleitung verdächtiger Inhalte.
JEDER

Sofortige Meldung an die Schulleitung und IT-Verantwortliche.
JEDER

Trennung betroffener Geräte vom Netzwerk.
JEDER

Dokumentation des Vorfalls (Zeitpunkt, Art, betroffene Daten).
SCHULTRÄGER

Unterstützung durch externe IT-Experten einholen.
SCHULTRÄGER

Hinweis:

Zur näheren tiefen technischen Betrachtung empfehlen wir auch das Paper von PD: **Einführung in die Informationssicherheit für Schulen**

IT-SICHERHEIT: TOP 10 SOFORTMASS-NAHMEN FÜR SCHULEN – CHECKLISTE FÜR DEN DIGITALEN SCHULALLTAG

Um Schulen beim Aufbau einer belastbaren IT-Sicherheitsstruktur zu unterstützen, wurde eine Checkliste mit den 10 effektivsten Sofortmaßnahmen entwickelt. Sie bietet eine Hilfestellung für Schulträger und IT-Verantwortliche, um mit überschaubarem Aufwand ein hohes Maß an Schutz und Resilienz zu erreichen. Die Maßnahmen sind nach dem Prinzip „geringer Aufwand – hoher Ertrag“ priorisiert und fokussieren sich auf schnell umsetzbare Schritte mit unmittelbarer Wirkung auf die Sicherheit der schulischen IT-Infrastruktur.

Die Checkliste umfasst sowohl technische als auch organisatorische Aspekte und adressiert zentrale Handlungsfelder wie Benutzersensibilisierung, Zugriffsschutz, Datensicherung und Netzwerksegmentierung.

Ziel ist es, Schulen und Schulträgern eine klare und umsetzbare Grundlage an die Hand zu geben, um die IT-Sicherheit nachhaltig zu verbessern und Risiken aus dem digitalen Schulbetrieb effektiv zu minimieren.

Wirkung ***
Aufwand *

Awareness-Schulungen für Mitarbeitende und Schüler

- Sensibilisierung für Phishing, sichere Passwörter und Datenschutz.
- Regelmäßige Schulungen mit Zertifikat, Infoseiten, Testumgebungen und ggf. Evaluation.

  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Faktor-Mensch/Awareness/awareness_node.html

  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Management_Blitzlicht/Management_Blitzlicht_Awareness.html
- **VERANTWORTLICHKEIT:**

  SCHULLEITUNG SCHULTRÄGER

***
**

Aktualisierung & Patch-Management

- Betriebssysteme, Anwendungen und Netzwerkgeräte **regelmäßig updaten**. Deshalb am besten eine Liste aller Dienste erstellen und Termine im Kalender eintragen.
- Abhängigkeiten zwischen Software Paketen und Plugins müssen bereits in der Architektur berücksichtigt werden.

  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/04_OPS_Betrieb/OPS_1_1_3_Patch_und_Aenderungsmanagement_Edition_2023.pdf?__blob=publicationFile&v=3
- **VERANTWORTLICHKEIT:**

  SCHULTRÄGER

***
**

Starke Passwortrichtlinien & Multi-Faktor-Authentifizierung (MFA)

- Durchsetzung sicherer Passwörter (Länge, Komplexität).
- Einsatz von MFA, insbesondere für Admin-Konten und Cloud-Dienste.

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

  https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheits-empfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html
- **VERANTWORTLICHKEIT:**

  SCHULTRÄGER

Wirkung * * *
Aufwand * *

Physische und digitale Zugriffsrechte nach dem Prinzip der minimalen Rechte (Zero Trust)

- Nur notwendige Berechtigungen vergeben.
- Regelmäßige Überprüfung und Anpassung der bestehenden Zugriffsrechte, falls sich diese Rechte in den Schulen verselbstständigen.
- **VERANTWORTLICHKEIT:**

  SCHULTRÄGER

* *
*

Antiviren- und Endpoint-Schutzlösungen

- Einsatz von aktuellen Antivirenprogrammen auf allen Endgeräten. Mindestens sollten die im Betriebssystem inkludierten Tools aktiviert werden.
- Beschränkung der Nutzung externer Datenträger.

  https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheits-empfehlungen/Virenschutz-Firewall/Virenschutzprogramme/virenschutzprogramme_node.html

- **VERANTWORTLICHKEIT:**

  SCHULTRÄGER SCHULLEITUNG
  BYOD (BRING YOUR OWN DEVICE): INKLUSIVE NUTZER

* * *
* * *

Firewall- und Netzwerkschutz

- Einsatz einer professionellen Firewall (z. B. mit DPI, Webfilter, VPN).
- Trennung von Netzwerken (VLAN für z. B. Schulnetz, Gastnetz, Verwaltungsnetz, Druckernetz, Gebäudemanagement).

  https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheits-empfehlungen/Virenschutz-Firewall/Firewall/firewall.html

- **VERANTWORTLICHKEIT:**

  SCHULTRÄGER

Wirkung * * *
Aufwand * *

Sicheres Backup- und Wiederherstellungskonzept

- Regelmäßige, automatisierte Backups offline oder unveränderbar in der Cloud speichern.
- Wiederherstellung regelmäßig testen (Disaster Recovery Tests). Das beste Backup nützt nichts, wenn es nicht wieder hergestellt werden kann.
- Backup heute statt Sicherheitsvorfall morgen

  https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheits-empfehlungen/Daten-sichern-verschluesseln-und-loeschen/Datensicherung-und-Datenverlust/datensicherung-und-datenverlust_node.html

- **VERANTWORTLICHKEIT:**

  SCHULLEITUNG SCHULTRÄGER

* * *
* * *

Sicherheitskonzepte & IT-Richtlinien

- Erstellung eines IT-Sicherheitskonzepts einschließlich Notfallplänen. Ergänzend einfache Checklisten und klare Ansprechpartner für die häufigsten Fälle.
- Festlegung von Regeln zur Nutzung von Geräten, Internet, USB-Sticks im Verwaltungsnetzwerk.
- Diese müssen bekannt sein und im Alltag Beachtung finden.
- Jederzeit offline und physisch verfügbar sein. Gegebenenfalls Anpassung vorhandener Richtlinien an den Anforderungen des Schulbereichs.

  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/Massnahmenkatalog/massnahmenkatalog.html

  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-Notfallmanagement/7_Notfaellebewaeltigen/4_Notfallhandbuch/Notfallhandbuch_node.html

- **VERANTWORTLICHKEIT:**

  SCHULLEITUNG SCHULTRÄGER

Wirkung ***
Aufwand ***

Logging, Monitoring & Alarme

- Protokollierung sicherheitsrelevanter Ereignisse (z. B. Login-Versuche). Klärung der aktiven Zuständigkeit.
- Überwachung und automatisierte Alarme bei Anomalien. Hier können KI-Systeme unterstützen.

  Monitoring und Anomalie Erkennung in Produktionsnetzwerken

- **VERANTWORTLICHKEIT:**

  SCHULTRÄGER

***
**

Geräteverwaltung & Mobile Device Management (MDM)

- Die zentrale Verwaltung umfasst Updates, Richtlinien und Fernlöschung, insbesondere für mobile Geräte. Für private Geräte im Schulnetz sollten klare Regelungen und Zugangskriterien definiert werden.
- Siehe Leitfäden auf der nächsten Seite.

  https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Mobile_Device_Management/Mobile_Device_Management_node.html

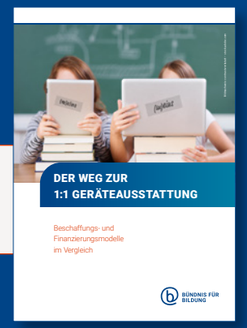
- **VERANTWORTLICHKEIT:**

  SCHULLEITUNG SCHULTRÄGER BUNDESLAND

Ausführliche Informationen erhalten Sie mit unseren zum Download bereitgestellten Leitfäden:

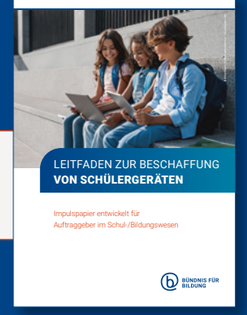
Leitfaden

Der Weg zur 1:1 Geräteausstattung



Leitfaden

Leitfaden zur Beschaffung von Schülergeräten



Leitfaden

Leitfaden zur Beschaffung von Lehrerdienstgeräten

VERANTWORTLICHKEITEN UND ZUSTÄNDIGKEITEN IN DER SCHUL-IT: WER TRÄGT WELCHE ROLLE?

Sichere Schul-IT beginnt mit Verantwortung – und Bewusstsein

Die digitale Infrastruktur in Schulen wird zunehmend komplexer. Neben dem pädagogischen Netz für den Unterricht und dem Verwaltungsnetz für die Schulorganisation treten heute viele weitere IT-Systeme und Netzbereiche auf den Plan – vom Gebäudemanagement über sicherheitsrelevante Technik bis hin zu Lösungen von Drittanbietern. Damit steigt nicht nur der Bedarf an leistungsfähiger Technologie, sondern vor allem an klaren Zuständigkeiten und gegenseitigem Verständnis.

Wer ist wofür verantwortlich?

Sachsen hat als einziges Bundesland die besondere Stellung der Schulträger im Informationssicherheitsrecht explizit anerkannt und geregelt. Im SächsISichG heißt es in § 4 Absatz 3: „Die Verantwortung für die Informationssicherheit [...] trägt die jeweilige Leiterin oder der jeweilige Leiter der staatlichen oder nicht-staatlichen Stelle, bei Schulen der jeweilige Schulträger“.

Die anderen Bundesländer behandeln Schulträger implizit über allgemeine Bestimmungen für öffentliche Stellen oder Kommunen, sodass auch dort Schulträger grundsätzlich die übergreifende Verantwortung für die IT-Sicherheit an ihren Schulen tragen. Über Verwaltungsvorschriften, Dienstanweisungen oder Organisationsvereinbarungen kann ein Schulträger seine Verantwortung strukturieren, und gegenüber anderen Beteiligten wie Schulleitern, Lehrkräften und Landesvertretungen abgrenzen.

Wer das System aufbaut, muss auch sicherstellen, dass es sicher ist. Sofern nicht anders vereinbart, liegt die Verantwortung für die Sicherheit der eigenen IT-Systeme bei der Amtsleitung des Schulträgers. Diese ist gut beraten, eine kompetente Stelle für die Informationssicherheit einzurichten, die mit ausreichend zeitlichen Ressourcen für diese Aufgabe ausgestattet wird.

In der Praxis existieren oft parallele Verantwortlichkeiten: Die Schulleitung denkt an pädagogische Software, der Schulträger an

Gebäudeautomation, der IT-Dienstleister an Netzwerktechnik – doch wer kennt die Anforderungen der jeweils anderen? An den Schnittstellen entstehen schnell Unsicherheiten und im schlimmsten Fall unbemerkte Sicherheitslücken.

Vier zentrale Gruppen tragen Verantwortung für sichere Schul-IT:

1. **Der Schulträger/Sachaufwandsträger**
   Als Betreiber der Schulgebäude kümmert er sich um die Netzwerkinfrastruktur sowie um zentrale IT-Komponenten wie IDM und MDM, von der Stromversorgung über VoIP-Systeme bis hin zu Schließanlagen und WLAN. Oft fällt auch die Koordination externer IT-Dienstleister in seinen Aufgabenbereich.

2. **Die Schulgemeinde/Schulfamilie**
   Schulleitung, Lehrkräfte, Schülerinnen und Schüler sowie schulische IT-Beauftragte nutzen das pädagogische Netz – oft auch über Klassenzimmer hinaus: in Bibliotheken, Mensen, Fachräumen oder außerschulischen Lernorten. Die Anforderungen variieren stark, die Zuständigkeiten sind häufig nicht klar abgegrenzt.

3. **Externe Dienstleister und Anbieter**
   Sie betreuen einzelne IT-Komponenten oder ganze Systeme – etwa die MDM-Plattform, das Netzwerk oder Bezahlsysteme. Sie benötigen klar definierte Schnittstellen, damit keine Lücken im Betrieb oder der Sicherheit entstehen.

4. **Das Bundesland**
   Es stellt zentrale Dienste bereit und ist in diesen Fällen für die IT verantwortlich (z. B. Lehrkräfte-Endgeräte).

Exkurs: Das Problem mit der Weisungsbefugnis

Grundsätzlich gilt: Schulträger statten die in ihrem Zuständigkeitsbereich liegenden Schulen mit der nötigen Infrastruktur aus, die Schulfamilie nutzt diese für den Unterricht oder die nötigen Verwaltungstätigkeiten. Das gilt für die gesamte digitale Infrastruktur, für Netze, Hardware und Software.

Dabei haben die Schulträger in der Regel als kommunale Körperschaften auch Beauftragte, die sich nach den jeweiligen Vorgaben um Richtlinien und deren Einhaltung in den Bereichen Datenschutz und Informationssicherheit kümmern (DSB und ISB). Diese Richtlinien gelten für alle Mitarbeitenden als Vorgabe und sind einzuhalten, anderenfalls können auch dienstrechtliche Konsequenzen die Folge sein.

Im schulischen Kontext ergibt sich damit jedoch folgende Problematik: Mit Ausnahme des kommunalen Schulwesens in Bayern sind die Mitarbeitenden an den Schulen i.d.R. Landesbedienstete und damit nicht der kommunalen Verwaltung weisungsgebunden. Rein formal gelten dienstliche Vorgaben der Kommune daher nicht für Schulleitungen und Lehrkräfte. In der Theorie sind sie folglich nicht verpflichtet, kommunale Richtlinien für den Einsatz digitaler Systeme einzuhalten. Gleiches gilt beispielsweise für die Teilnahme an vom Schulträger geforderten Fortbildungsveranstaltungen wie Awareness-Schulungen.

Diese Regelungslücke muss für ein funktionierendes Sicherheitssystem geschlossen werden. Dies geschieht einerseits durch die bisher genannten technischen Maßnahmen. Das Thema Weisungsbefugnis sollte jedoch beispielsweise durch Nutzungsbedingungen

oder -vereinbarungen mit den betroffenen Personen abgedeckt werden.

Viele Netze – viele Anforderungen – viele Risiken

Die digitale Schule von heute ist ein komplexes Ökosystem aus voneinander abhängigen IT-Strukturen – und jede einzelne davon bringt eigene Anforderungen, Verantwortlichkeiten und Sicherheitsrisiken mit sich.

Das pädagogische Netz, in dem Lernende und Lehrkräfte arbeiten und auf digitale Unterrichtsressourcen zugreifen.

Das Verwaltungsnetz, das die schulische Organisation, Verwaltung und alle damit verbundenen Prozesse unterstützt.

Die Gebäudetechnik, die Heizung, Beleuchtung, Solaranlagen sowie Sicherheitslösungen wie Kameras, Alarm- und Schließsysteme umfasst.

Die Kommunikationssysteme, die VoIP-Telefonie, Gäste-WLAN und digitale Zugangskontrollen bereitstellen.

Die Sonderbereiche, die den Betrieb von Mensen, Bibliotheken oder Sporthallen digital unterstützen.

Die Drittsysteme, über die zum Beispiel Bezahldienste oder Verwaltungssoftware in den Schulalltag integriert werden.

Die externen Netze, die von Vereinen oder Dienstleistern betrieben werden und dennoch mit der schulischen Infrastruktur interagieren.

Technisch sind viele dieser Systeme vernetzt. Organisatorisch jedoch nicht immer abgestimmt. Die Folge: Ungesicherte Schnittstellen, unklare Verantwortlichkeiten, Sicherheitslücken. Wer darf eigentlich welches Gerät ins Netz einbinden? Wer schützt die Nutzerdaten? Wer trägt die Verantwortung bei einem Ausfall oder Angriff?

Zero Trust als technisches und organisatorisches Prinzip

Ein modernes Sicherheitskonzept basiert auf dem Ansatz „Zero Trust“: Niemand erhält automatisch Zugriff – jede Verbindung muss authentifiziert, autorisiert und nachvollziehbar sein, und es wird nur Zugriff auf Ressourcen gewährt, die für die Erfüllung der Aufgabe notwendig sind. Nicht zwingend benötigte Zugriffe werden gesperrt, da sie ein Sicherheitsrisiko darstellen. Das bedeutet einen höheren Pflegeaufwand. Dafür braucht es:

- Segmentierte Netzwerke
- Gesteuerte Remote-Zugänge (VPN/SSE)
- Differenzierte Rechtevergabe
- Klare Rollenzuweisungen
- Einheitliche Sicherheitsrichtlinien

Doch: Technik allein genügt nicht. Zero Trust funktioniert nur, wenn sich alle Beteiligten abstimmen und ihre Aufgaben kennen. **Sicherheit entsteht durch Kommunikation**. Viele Beteiligte agieren bislang isoliert – quasi in ihrer „Schublade“:

- Medienbeauftragte kümmern sich um Unterrichtsgeräte
- Schulträger-IT betreibt die Infrastruktur

- Facility Management um Gebäudeautomation
- Externe Anbieter um einzelne Tools

Die Fragen lauten: Wann sitzen alle einmal an einem Tisch?

Wer kennt die Verantwortlichen in den anderen Bereichen?

Welche Systeme greifen ineinander – technisch wie organisatorisch?

Nur wer die Gesamtsituation versteht, kann mitdenken, mitverantworten und mitgestalten.

Sicherheit ist ein gemeinsamer Prozess

Eine Firewall ersetzt keine Kommunikation.

Ein starkes WLAN ersetzt keine klare Rollenverteilung.

Ein sicheres Passwort ersetzt keine funktionierende Abstimmung.

Digitale Sicherheit in Schulen entsteht nicht durch Einzelmaßnahmen, sondern durch ein gemeinsames Verständnis. Zuständigkeiten müssen definiert, Abläufe abgestimmt, Verantwortlichkeiten dokumentiert werden – z. B. im Geschäftsverteilungsplan der Kommune.

Sichere Schul-IT ist Teamarbeit.

Und sie beginnt mit der Bereitschaft, gemeinsam Verantwortung zu übernehmen.

DIE KOMMUNIKATION IM KRISENFALL

Ein gut durchdachtes Kommunikationskonzept ist in Sicherheitsvorfällen ebenso wichtig wie die technische Reaktion. Schnelle und klare Informationen können Schaden begrenzen, Vertrauen aufrechterhalten und unnötige Panik vermeiden. Es muss auch klar definiert sein, wie und bei wem Krisenfälle durch die Nutzende gemeldet werden müssen. Beispielsweise sollte es für Sicherheitsvorfälle eine eigene Notfallnummer geben, die Rufnummer einer IT-Hotline wäre hier nicht zielführend. Im Vorfeld muss zwingend ein Krisenstab gebildet werden.

Informationen darüber, an wen sich Nutzende wenden sollen, sollten deshalb Lerninhalt der oben genannten Schulungen sein.

Grundsätze der Kommunikation

- Vordefinierte Kommunikationskanäle: Legen Sie vorab fest, welche Kanäle genutzt werden (beispielsweise: E-Mail, Intranet, Messenger-Dienste, ggf. öffentliche Kanäle).
- Klare Rollen und Zuständigkeiten: Bestimmen Sie, wer wann mit wem kommuniziert. Wer informiert die Schulleitung, wer die Eltern und Schüler, wer die Behörden?
- Wahrheit und Transparenz: Kommunizieren Sie offen und ehrlich, auch wenn die Situation unsicher ist. Spekulationen schaden mehr als ein offenes Wort.
- Faktengestützte Informationen: Verlassen Sie sich auf Informationen aus verlässlichen Quellen wie dem IT-Team (Schulträger/Dienstleister) oder dem ISB (Informationssicherheitsbeauftragter).
- Einfache Sprache: Verzichten Sie auf technische Fachbegriffe, um Missverständnisse zu vermeiden.

Ablauf bei einem Sicherheitsvorfall

Phase 1: Sofortige Reaktion

- Der (sensibilisierte) Nutzer informiert das IT-Team beim Schulträger sofort beim Feststellen eines Vorfalls über bekannte Notfallnummern.
- Das IT-Team informiert umgehend den ISB und den Krisenstab und versucht, den Schaden zu minimieren.
- Je nach Sachlage werden Schulleitung und Schulträger alarmiert.

Phase 2: Lagebewertung

- Krisenstab (bestehend aus Schulleitung, Schulträger und IT-Experten) bewertet das Ausmaß des Vorfalls.
- Erster Entwurf einer internen Mitteilung wird erstellt.

Phase 3: Externe Kommunikation

- Wenn notwendig, werden Eltern, Schüler und die Öffentlichkeit über vordefinierte Kanäle informiert.
- Eine offizielle Mitteilung wird an relevante Behörden (Schulamt, ggf. Polizei) gesendet.

Phase 4: Nachbereitung

- Das Kommunikationskonzept wird evaluiert und bei Bedarf angepasst.
- Erkenntnisse aus dem Vorfall werden dokumentiert und für zukünftige Fälle genutzt.

IT- Notfallkarte

Hier können Sie sich die IT-Notfallkarte downloaden.

Die IT-Notfallkarte „Verhalten bei IT-Notfällen“ ist ein neues Hinweisschild, analog zum bekannten Format „Verhalten im Brandfall“. Beschäftigten in Organisationen werden wichtige Verhaltenshinweise bei IT-Notfällen aller Art an die Hand gegeben. Die aufgeführten Maßnahmen ermöglichen es Organisationen, vom ersten Moment an die richtigen Entscheidungen treffen zu können. Die Notfallkarte soll an zentralen Orten platziert werden und erzeugt einen unmittelbaren Beitrag zur Security Awareness in Ihrer Organisation.

Der jeweilige Ansprechpartner für IT-Notfälle im eigenen Wirkungsbereich ist individuell zu ermitteln.

Mitglieder des Krisenteams

Rolle/Funktion	Aufgabe im Krisenstab
Schulträger / Verwaltung	Strategische Entscheidungen, Ressourcen-bereitstellung, externe Kommunikation
IT-Leitung / IT-Sicherheitsbeauftragte	Technische Analyse, Sofortmaßnahmen, Wiederherstellung der Systeme
Datenschutzbeauftragte/r	Bewertung datenschutzrechtlicher Risiken, Meldung von Datenpannen
Kommunikationsverantwortliche/r	Krisenkommunikation intern/extern, Medienarbeit
Rechtsbeistand / Juristische Beratung	Rechtliche Einschätzung, Unterstützung bei Meldungen
Krisenmanager/in oder Koordinator/in	Organisation, Dokumentation, Moderation der Sitzungen
Externe IT-Dienstleister (optional)	Technische Unterstützung, Forensik
Schulleitung	Operative Entscheidungen, Kommunikation mit Schulträger und Behörden, sowie Schulgemeinde
Vertreter der Elternschaft (optional)	Transparente Kommunikation mit Eltern
Vertreter der Lehrkräfte / Personalrat (optional)	Kommunikation mit Kollegium, interne Unterstützung
Polizei / Datenschutzbehörde (optional)	Bei schwerwiegenden Vorfällen, rechtliche Begleitung
Psychologische Beratung (optional)	Unterstützung bei emotional belastenden Situationen

Bei Netzwerkausfall, Stromausfall oder ähnliches (Telefonie VoIP), sollte ein Off-Line-Medium als Ausweich-Kanal zur Verfügung stehen.

Kommunikationsmatrix

Wer kommuniziert?	Mit wem?	Über welchen Kanal?	Wann?	Kontakt-daten
IT-Team	**ISB, Schulträger, Schulleitung**	**Telefon / Sicheres Chat-System**	**Sofort nach Feststellung**	
Schulleitung	**Schulträger**	**Telefon / E-Mail**	**Nach Abstimmung mit IT-Team**	
Schulträger	**Schulleitung (intern)**	**E-Mail-Verteiler / Intranet**	**Nach Freigabe durch Krisenstab**	
Schulträger	**Relevante Behörden**	**E-Mail / Offizielles Schreiben**	**Nach Abstimmung mit Krisenstab (innerhalb von 24h bei Datenvorfällen)**	
Schulträger	**Presse / Öffentlichkeit (extern)**	**Presse-mitteilung / Social Media**	**Nach Freigabe durch Krisenstab**	
Schulleitung / Schulträger	**Eltern / Erziehungs-berechtigte**	**Elternbrief / E-Mail / Schul-App**	**Nach interner Abstimmung und Freigabe**	
IT-Team / Schulleitung / Krisenstab	**Dokumentation**	**Protokoll / Ticket-System / Bericht**	**Parallel zur Kommunikation oder direkt danach**	
Schulleitung / Schulträger	**Schul-gemeinschaft (Feedback)**	**Intranet / Elternabend / Schülerver-tretung/ Rundmail**	**Nach Abschluss der Maßnahmen**	

Die oben genannten Angaben können von Bundesland zu Bundesland und von Kommune zu Kommune variieren und sind entsprechend anzupassen.

DOKUMENTATION PRÄVENTIVER MASSNAHMEN

KONTINUIERLICHE AKTUALISIERUNG DES KRISENPLANS

Ein zentraler Bestandteil einer ganzheitlichen IT-Sicherheitsstrategie im schulischen Umfeld ist die regelmäßige Überprüfung und Erprobung möglicher Cybersecurity-Bedrohungsszenarien, um im Ernstfall vorbereitet zu sein. Durch strukturierte Penetrationstests und Simulationen von Angriffen können potenzielle Sicherheitslücken frühzeitig identifiziert und gezielt geschlossen werden. Diese praxisnahen Tests dienen nicht nur der technischen Härtung der Systeme, sondern auch der Sensibilisierung und Schulung des IT-Personals sowie der Anwenderinnen und Anwender. Hier bietet sich die externe Einbindung eines Dienstleisters an.

Ebenso essenziell ist die **systematische Dokumentation der präventiven Sicherheitsmaßnahmen und definierten Handlungswege**. Eine klare und nachvollziehbare Dokumentation schafft Transparenz über Zuständigkeiten, Kommunikationsketten und Abläufe im Ernstfall und stellt sicher, dass alle beteiligten Akteure im Krisenfall handlungsfähig bleiben. Hierzu gehören neben technischen Schutzmaßnahmen (z. B. Firewalls, Endpoint-Protection, Backup-Strategien) auch organisatorische Prozesse wie die Zugangskontrolle, Krisenpläne, Kommunikationsrichtlinien. Die Entscheidung muss getroffen werden, welche Dokumente für den Ernstfall in ausgedruckter Form vorliegen müssen, um handlungsfähig zu bleiben.

Da sich das Bedrohungsumfeld im Bereich der IT-Sicherheit fortlaufend verändert, ist eine **regelmäßige Aktualisierung des Krisen- und Notfallplans** zwingend erforderlich. Neue Angriffsmethoden, Software-Updates und veränderte schulische Strukturen müssen kontinuierlich in die Sicherheitsarchitektur integriert werden. Eine jährliche Überprüfung, ergänzt durch anlassbezogene Anpassungen nach Vorfällen oder Systemänderungen, gewährleistet die dauerhafte Wirksamkeit des Sicherheitskonzepts und stärkt die Resilienz der gesamten Schul-IT-Infrastruktur.

FAZIT

SICHERHEIT ALS FUNDAMENT DIGITALER BILDUNG

In einer Zeit, in der digitale Technologien das Lehren und Lernen tiefgreifend prägen, ist Informationssicherheit kein technisches Detail, sondern eine zentrale Säule der pädagogischen Qualität. Moderne Bildung basiert auf Daten – deren Schutz ist eine rechtliche Pflicht und die Voraussetzung für das Vertrauen von Lehrkräften, Eltern sowie Schülerinnen und Schülern.

Sicherheit als Gemeinschaftsaufgabe
Damit dieser Anspruch Realität wird, müssen Schulträger und Schulen Informationssicherheit als gemeinsame Aufgabe begreifen.
Ein koordiniertes Handeln erfordert klare Verantwortlichkeiten:

- **Schulträger:** Tragen die Verantwortung für die technische Infrastruktur (Netzwerke, Server, Cloud-Angebote) sowie zentrale Sicherheitsmechanismen (Firewalls, MDM, Updates).

- **Schulen:** Sind verantwortlich für die sichere Nutzung im Alltag, organisatorische Maßnahmen (Zugriffsregelungen) und die Sensibilisierung der Schulgemeinschaft.

Prävention durch Technik und Organisation
IT-Sicherheit erfordert das Ineinandergreifen von technischen und organisatorischen Maßnahmen. Erst die Kombination aus Verschlüsselung, Zwei-Faktor-Authentifizierung und Netzwerksegmentierung mit klaren Dienstvereinbarungen und Notfallplänen schafft ein robustes Sicherheitsniveau.

Kontinuierliche Entwicklung und „Faktor Mensch“: Digitale Sicherheit ist kein statischer Zustand, sondern ein fortlaufender Prozess. Da sich Bedrohungslagen ständig ändern, müssen Sicherheitsstrategien regelmäßig evaluiert werden. Das größte Risiko sind oft nicht technische Lücken, sondern alltägliche Fehler. Daher sind zwei Faktoren entscheidend:

1. **Qualifiziertes Personal:** Schulträger müssen intern oder extern Expertise für die Administration vorhalten.

2. **Awareness:** Die fortlaufende Schulung von Lehrkräften und Schulleitungen ist essenziell, um Wissenslücken zu schließen und die „menschliche Firewall“ zu stärken.

Krisenmanagement: Handlungsfähig im Ernstfall
Trotz maximaler Prävention bleibt ein Restrisiko. Ein professionelles Krisenmanagement entscheidet dann über das Ausmaß des Schadens. Gemeinsam entwickelte Notfallpläne, klare Meldewege und eine transparente Kommunikationsstrategie stellen sicher, dass im Ernstfall jeder Akteur sofort weiß, was zu tun ist.

Nachhaltige Informationssicherheit entsteht durch eine gelebte Sicherheitskultur. Die vorliegende Handlungsempfehlung bietet Schulträgern und Schulen eine praxisnahe Orientierung, um IT-Sicherheit schrittweise zu verbessern und Prioritäten sinnvoll zu setzen. Nur durch verlässliche Strukturen und eine enge Kooperation schaffen wir einen geschützten Raum für die digitale Bildung der Zukunft.

GLOSSAR

ALPHABETISCH

Datenschutz, Datenschutzbeauftrager (DSB)
Datenschutz bezieht sich auf den Schutz personenbezogener Daten. Er folgt gesetzlichen Vorgaben (z. B. DSGVO) und schützt die Privatsphäre sowie die Rechte betroffener Personen. Der Datenschutzbeauftragte unterstützt bei der Beantwortung von Fragen zum Schutz der personenbezogenen Daten und übernimmt Aufgaben nach der DSGVO, insbesondere Überwachung der Einhaltung der Vorhaben von Datenschutzvorschriften (angelehnt an Art. 38, 39 DSGVO).

Datensicherheit
Umfasst technische und organisatorische Maßnahmen, die Daten jeglicher Art vor Verlust, Manipulation und unbefugtem Zugriff schützen. Sie ist ein Teilbereich der Informationssicherheit.

DPI (Deep Packet Inspection)
Technik zur Analyse des Datenverkehrs, bei der nicht nur die Header, sondern auch die Inhalte von Datenpaketen untersucht werden.

Endpoint
Bezeichnet ein Endgerät in einem Netzwerk, z. B. Laptop, Smartphone oder Tablet, das gesichert und verwaltet werden muss.

Firewall
Ein Netzwerksicherheitsgerät, das ein- und ausgehenden Datenverkehr überwacht und anhand definierter Regeln blockiert oder zulässt.

IDS (Intrusion Detection System)
System, das verdächtige Aktivitäten im Netzwerk erkennt und Warnungen ausgibt.

Incident Response Teams
Teams aus Fachleuten, die Sicherheitsvorfälle erkennen, analysieren und koordinierte Maßnahmen zur Eindämmung, Behebung und Wiederherstellung ergreifen.

Informationssicherheit, Informationssicherheitsbeauftragter (ISB)
Informationssicherheit umfasst den Schutz aller Informationen – digital, analog oder mündlich – vor unbefugtem Zugriff. Der Informationssicherheitsbeauftragte **(ISB) ist verantwortlich für die Planung, Umsetzung und Überwachung der Informationssicherheit**.

IPS (Intrusion Prevention System)
Erkennt verdächtige Aktivitäten im Netzwerk und blockiert diese aktiv, um Angriffe zu verhindern.

IT-Sicherheit
Konzentriert sich auf den Schutz von IT-Systemen, Netzwerken und digitalen Daten vor Angriffen, Ausfällen und Missbrauch.

IT-Team
Operatives technisches Personal (Schule, Schulträger, Dienstleister), das für den IT-Betrieb und die Umsetzung technischer Sicherheitsmaßnahmen zuständig ist.

MDM (Mobile Device Management)
Software zur zentralen Verwaltung, Überwachung und Absicherung mobiler Endgeräte wie Smartphones und Tablets.

Penetrationstest
Geplanter, simulierter Angriffsversuch auf IT-Systeme, um Schwachstellen aufzudecken, bevor echte Angreifer sie ausnutzen können.

Phishing
Methode, bei der Angreifer sich als vertrauenswürdige Absender ausgeben, um sensible Daten wie Passwörter oder Bankinformationen zu stehlen.

Ransomware
Schadsoftware, die Daten verschlüsselt und anschließend Lösegeld für deren Entschlüsselung fordert.

SSE – Security Service Edge
Cloudbasierte Sicherheitsdienste, die Nutzer beim Zugriff auf Internet, Cloud und Unternehmensanwendungen schützen, egal wo sie sich gerade befinden.

Staging-Umgebung
Testumgebung, die die Produktionsumgebung realistisch nachbildet. Dort werden Funktionen, Updates oder Konfigurationen vor dem Livegang geprüft.

USV (Unterbrechungsfreie Stromversorgung)
Gerät, das bei Stromausfällen Notstrom bereitstellt, um kritische Systeme weiter betreiben zu können.

VLAN (Virtual Local Area Network)
Netzsegment innerhalb eines physischen Netzes. Es trennt physische Netze in Teilnetze auf.

VPN (Virtual Private Network)
Ermöglicht eine sichere, verschlüsselte Verbindung über ein unsicheres Netzwerk wie das Internet.

Zero-Trust-Architektur
Sicherheitskonzept, das grundsätzlich keinem Benutzer oder Gerät vertraut – weder innerhalb noch außerhalb des Netzwerks –, bis deren Identität und Berechtigungen überprüft wurden.

www.bfb.org

Bündnis für Bildung e.V.
Oranienburger Str. 32
10117 Berlin

info@b-f-b.net
www.bfb.org

BÜNDNIS FÜR BILDUNG