

RATGEBER FÜR CYBERSICHERHEIT

SICHERE DIGITALE INFRASTRUKTUREN

IN SCHULEN UND NON-FORMALEN EINRICHTUNGEN



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Éducation nationale,
de l'Enfance et de la Jeunesse



Kofinanziert von der
Europäischen Union





HAFTUNGSAUSSCHLUSS

Dieser Ratgeber dient als allgemeine Orientierungshilfe und enthält grundlegende Empfehlungen zur Sicherheit in Grundschulen und Einrichtungen für Kinder und Jugendliche. Es erhebt keinen Anspruch auf Vollständigkeit und ersetzt weder gesetzliche Vorgaben noch eine individuelle Risikoanalyse oder die Beratung durch zuständige Fachstellen.

Jede Einrichtung ist selbst dafür verantwortlich, ihre spezifischen Risiken zu bewerten, geeignete Sicherheitsmaßnahmen umzusetzen sowie die zuständigen Behörden oder Fachstellen bei Bedarf einzubeziehen.

Die Umsetzung der in diesem Ratgeber beschriebenen Maßnahmen bietet keine Garantie, dass Sicherheitsvorfälle verhindert werden. Der Herausgeber übernimmt auch keine Haftung für Schäden oder Folgen, die aus der Anwendung oder Nichtanwendung der Inhalte entstehen.

INFO FÜR DAS PÄDAGOGISCHE PERSONAL

Dieser Leitfaden konzentriert sich auf technische und organisatorische Sicherheitsmaßnahmen. Für Lehrpersonen und Erzieher bietet BEE SECURE zusätzlich den Ratgeber „Im digitalen Zeitalter ein Vorbild sein“ an. Die Publikation enthält praktische Empfehlungen für einen verantwortungsvollen und sicheren Umgang mit digitalen Werkzeugen im beruflichen und privaten Alltag.



Herausgeber: Service national de la jeunesse (SNJ)
Service national de la jeunesse - B.P. 707 L-2017 Luxembourg
www.snj.lu | www.bee-secure.lu

© 2026 Service national de la jeunesse (SNJ) – Initiative BEE SECURE



Die Creative-Commons-Lizenz dieser Publikation nachlesen:
www.creativecommons.org/licenses/by-nc-sa/4.0/deed.de

Ratgeber für Cybersicherheit
Sichere digitale Infrastrukturen in Schulen
und non-formalen Einrichtungen
09.2026

ISBN 978-2-919846-71-9
Elektronische Ressource

Initiiert von:



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Durchgeführt von:



Service national
de la jeunesse



Kofinanziert von:



Kofinanziert von der
Europäischen Union

In Zusammenarbeit mit:



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Éducation nationale,
de l'Enfance et de la Jeunesse

Hinweise:

- KI-Tools wurden für die Formatierung und die sprachliche Überarbeitung der Texte eingesetzt. Der Text wurde anschließend vom Team von BEE SECURE geprüft und freigegeben.
- Um die Lesbarkeit dieser Publikation zu erleichtern, wurde die männliche Form als neutrales Geschlecht verwendet, um die gesamte Bevölkerung zu bezeichnen.

INHALTSVERZEICHNIS

EINLEITUNG	3
1. GRUNDLAGEN EINER SICHEREN DIGITALEN UMGEBUNG	4
2. GERÄTE UND SOFTWARE SICHER VERWALTEN	6
3. NETZWERKE UND INFRASTRUKTUR SCHÜTZEN	10
4. DATENSCHUTZ UND VERTRAULICHKEIT STÄRKEN	13
5. DATEN SICHERN UND WIEDERHERSTELLEN	16
6. KINDER UND JUGENDLICHE SCHÜTZEN	19
7. AUF SICHERHEITSVORFÄLLE VORBEREITET SEIN	22
8. PRAXISBEISPIELE	24
NÜTZLICHE LINKS	27
BIBLIOGRAFIE	27

EINLEITUNG

Digitale Medien begleiten Kinder und Jugendliche heute in nahezu allen Lebensbereichen. Ob in der Schule, Kinderbetreuungsstrukturen, einem Jugendhaus oder einer Wohnstruktur – überall kommen Geräte, Plattformen und Online-Dienste zum Einsatz. Damit wächst auch die Verantwortung, diese digitalen Umgebungen sicher zu gestalten und junge Menschen vor Risiken im Netz zu schützen.

Dieser Leitfaden richtet sich an Einrichtungen, die ihre digitale Infrastruktur sicher gestalten und verantwortungsvoll betreiben möchten. Er enthält praktische Empfehlungen zu Benutzerkonten, Geräten, Netzwerken, Datenschutz, Datensicherung sowie zum Schutz von Kindern und Jugendlichen im digitalen Raum.

Die Empfehlungen wenden sich in erster Linie an Personen, die für die technische Infrastruktur einer Einrichtung verantwortlich sind. Dazu zählen beispielsweise interne oder externe Informatiker, Techniker, Mitarbeitende von Gemeindeverwaltungen, Personal von Trägerorganisationen sowie administratives Leitungspersonal. Einzelne Hinweise richten sich zudem an das pädagogische Personal und sind entsprechend gekennzeichnet.

Die in diesem Leitfaden vorgestellten Maßnahmen helfen dabei, digitale Risiken zu verringern, technische Ressourcen zu schützen und Kindern sowie Jugendlichen eine sichere digitale Umgebung zu bieten.

1. GRUNDLAGEN EINER SICHEREN DIGITALEN UMGEBUNG

Bereits mit wenigen organisatorischen und technischen Grundmaßnahmen lassen sich zahlreiche Sicherheitsprobleme vermeiden. Dazu gehören unter anderem ein sorgfältiger Umgang mit Benutzerkonten, klar geregelte Zugriffsrechte und die regelmäßige Überprüfung wichtiger Systemeinstellungen.

1.1 Benutzerkonten absichern

Benutzerkonten bilden die Grundlage für den Zugang zu Geräten, Netzwerken und digitalen Diensten einer Einrichtung. Sie ermöglichen Mitarbeitenden den Zugriff auf Arbeitsgeräte, E-Mail-Konten, Lernplattformen, Server oder Verwaltungsprogramme und tragen gleichzeitig dazu bei, Zugriffe einzelnen Personen eindeutig zuzuordnen.

Viele Sicherheitsvorfälle beginnen mit kompromittierten Zugangsdaten. Wer Zugriff auf ein Benutzerkonto erhält, kann je nach Berechtigungen auf Geräte, Netzwerke oder sensible Informationen zugreifen. Entsprechend wichtig ist ein sorgfältiger Umgang mit Benutzerkonten.

Deshalb empfiehlt sich die Einführung klarer Regeln für die Erstellung und Verwaltung von Zugangsdaten. Dazu gehören die Verwendung von langen, individuellen Passsätzen oder komplexen Passwörtern sowie die Sensibilisierung der Nutzer für bewährte Sicherheitspraktiken.

Passsätze bieten gegenüber klassischen Passwörtern den Vorteil, dass sie sowohl sicher als auch leichter zu merken sind. Sie bestehen aus mehreren zufällig gewählten Wörtern und sollen zusätzlich durch Sonderzeichen oder Zahlen ergänzt werden.

Beispiel:

Wählen Sie einen Satz, den Sie sich gut merken können und der keine persönlichen Informationen enthält. Ein Beispiel wäre:

„In die MR kommen 225 Kinder.“

Daraus kann beispielsweise folgender Passsatz entstehen:

In.die.MR.kommen.225.Kinder

Oder – noch kompakter – ein Passwort aus den Anfangsbuchstaben eines Satzes:

„In unsere große MR kommen jeden Tag 225 glückliche Kinder!!“

IugMRkjT225gK!!

Mit dem Passworttest von BEE SECURE können Sie anschließend überprüfen, wie sicher Ihr Passwort oder Passsatz ist.

Für die sichere Aufbewahrung von Zugangsdaten können Passwortmanager eine sinnvolle Unterstützung darstellen. Besonders wirksam ist die Aktivierung der Multi-Faktor-Authentifizierung (MFA). Dabei wird neben dem Passwort oder Passsatz eine zusätzliche Bestätigung verlangt, beispielsweise über eine App oder einen Sicherheitscode. Diese Maßnahme erschwert den Missbrauch kompromittierter Zugangsdaten erheblich.



EMPFEHLUNGEN

- Verwenden Sie für jedes Benutzerkonto ein individuelles Passwort oder einen individuellen Passsatz.
- Vermeiden Sie einfache Passwörter wie „123456“, „Passwort2025“, „ABC“, „QWERT“ oder leicht vorhersehbare Tastaturmuster.
- Ein starkes Passwort besteht aus mindestens 12 zufälligen Klein- und Großbuchstaben, Ziffern und Sonderzeichen.
- Lange und individuelle Passsätze erhöhen die Sicherheit und bleiben häufig leichter merkbar.
- Aktivieren Sie die Multi-Faktor-Authentifizierung, wenn verfügbar.
- Nutzen Sie einen Passwortmanager zur sicheren Verwaltung Ihrer Zugangsdaten.

1.2 Individuelle Benutzerkonten und Administratorrechte

Jede Person sollte nach Möglichkeit über ein eigenes Benutzerkonto verfügen. Individuelle Konten erleichtern die Nachvollziehbarkeit von Aktivitäten und reduzieren Risiken, die durch gemeinsam genutzte Zugangsdaten entstehen können. Letztere erschweren die Zuordnung von Änderungen oder Vorfällen und erhöhen das Risiko eines unbeabsichtigten oder missbräuchlichen Zugriffs auf Daten und Systeme.

Ebenso empfiehlt sich die konsequente Trennung zwischen regulären Benutzerkonten und Administratorkonten.

Für alltägliche Aufgaben genügt ein Standardkonto; Administratorrechte kommen nur dann zum Einsatz, wenn Änderungen an Systemen, Software oder Sicherheitseinstellungen erforderlich sind.

Administratorkonten zählen zu den besonders schützenswerten Zugängen einer Einrichtung. Ihre Absicherung durch Multi-Faktor-Authentifizierung bietet einen zusätzlichen Schutz vor unbefugten Zugriffen.



EMPFEHLUNGEN

- Richten Sie für jede Person ein eigenes Benutzerkonto ein.
- Verwenden Sie Administratorkonten ausschließlich für IT-Verwaltungsaufgaben.
- Arbeiten Sie im Alltag mit einem Standardkonto.
- Aktivieren Sie die Multi-Faktor-Authentifizierung für Administratorkonten.

2. GERÄTE UND SOFTWARE

SICHER VERWALTEN

In den meisten Einrichtungen kommen heute zahlreiche digitale Geräte zum Einsatz – von Computern und Tablets bis hin zu Smartphones oder interaktiven Bildschirmen. Damit diese Werkzeuge zuverlässig genutzt werden können, verdienen ihre Verwaltung und ihre Absicherung besondere Aufmerksamkeit.

2.1 Software bewusst auswählen

Nicht jede Software ist gleich vertrauenswürdig. Welche Programme eingesetzt werden, beeinflusst unmittelbar die Sicherheit einzelner Geräte und der gesamten IT-Infrastruktur. Programme aus unbekannten Quellen oder nicht unterstützte Anwendungen können Sicherheitslücken enthalten oder Schadsoftware verbreiten.

Deshalb empfiehlt sich die Nutzung von Software aus offiziellen Quellen, wie den Websites der Hersteller oder vertrauenswürdigen App-Stores. Vor der Einführung neuer Programme lohnt sich zudem die Prüfung, ob diese weiterhin vom Hersteller gepflegt und regelmäßig mit Sicherheitsupdates versorgt werden.

EMPFEHLUNGEN

- Beziehen Sie Software ausschließlich aus offiziellen Quellen oder vertrauenswürdigen App-Stores.
- Prüfen Sie vor der Installation, ob die Anwendung weiterhin vom Hersteller unterstützt wird.
- Benutzen Sie keine modifizierten Programme oder Raubkopien.



2.2 Installation kontrollieren

Jede zusätzliche Anwendung erweitert die digitale Angriffsfläche eines Geräts. Aus diesem Grund empfiehlt sich ein bewusster Umgang mit Softwareinstallationen.

Die Installation neuer Programme soll auf Personen beschränkt sein, die für die Verwaltung der Geräte zuständig sind. Dadurch lässt sich das Risiko verringern, dass ungeprüfte oder ungeeignete Anwendungen auf dienstlichen Geräten genutzt werden.

Ebenso sinnvoll ist die regelmäßige Überprüfung bereits installierter Programme. Anwendungen, die nicht mehr benötigt werden, sollen entfernt werden, um die Übersichtlichkeit und Sicherheit der Geräte zu erhöhen.

Auf Geräten, die von Kindern und Jugendlichen genutzt werden, können zusätzlich Jugendschutz- oder Alterseinstellungen aktiviert werden. Kapitel 6 enthält weitere Informationen zu diesem Thema.

EMPFEHLUNGEN

- Beschränken Sie Softwareinstallationen auf autorisierte Personen.
- Entfernen Sie Anwendungen, die nicht mehr benötigt werden.
- Aktivieren Sie auf Geräten für Kinder und Jugendliche geeignete Jugendschutzfunktionen.



2.3 Updates automatisieren

Sicherheitslücken werden regelmäßig entdeckt und durch Updates geschlossen. Geräte und Anwendungen, die nicht aktualisiert werden, können leichter Ziel von Cyberangriffen werden.

Automatische Updates sorgen dafür, dass Betriebssysteme, Anwendungen und Treiber ohne zusätzlichen Aufwand immer auf dem neusten Stand sind. Dies betrifft nicht nur Computer, sondern auch Tablets, Smartphones, Drucker, Server, Router und andere vernetzte Geräte.

EMPFEHLUNGEN

- Aktivieren Sie automatische Updates für Betriebssysteme, Programme und Firmware auf allen Nutzergeräten, Servern und Netzwerkgeräten.



2.4 Antivirenschutz einsetzen

Antivirenprogramme erkennen und blockieren viele bekannte Bedrohungen, bevor ein Schaden entstehen kann. Sie stellen daher einen wichtigen Bestandteil eines mehrschichtigen Sicherheitskonzepts dar. Auf Arbeitsgeräten empfiehlt sich ein aktueller Virenschutz, der regelmäßig aktualisiert wird und laufend neue Bedrohungen erkennen kann.

Viele Betriebssysteme verfügen bereits über integrierte Schutzmechanismen. Dennoch bleibt es wichtig, regelmäßig zu überprüfen, ob sie auf dem neusten Stand sind, und sicherzustellen, dass die Schutzfunktionen aktiv sind. Auch Server oder andere zentrale Systeme können von einem zusätzlichen Schutz profitieren.

EMPFEHLUNGEN

- ◆ Aktivieren Sie den Virenschutz auf allen Arbeitsgeräten.
- ◆ Aktualisieren Sie die Virensignaturen durch regelmäßige Updates.

2.5 Systemprotokollierung aktivieren

Systemprotokolle – auch als „Logging“ bezeichnet – dokumentieren wichtige Ereignisse auf Geräten und in Netzwerken. Dazu gehören beispielsweise Anmeldeversuche, Systemänderungen oder sicherheitsrelevante Vorfälle.

Eine aktivierte Protokollierung erleichtert die Analyse technischer Probleme und unterstützt die Nachvollziehbarkeit von Sicherheitsvorfällen. Im Fall eines Cyberangriffs können Protokolle wichtige

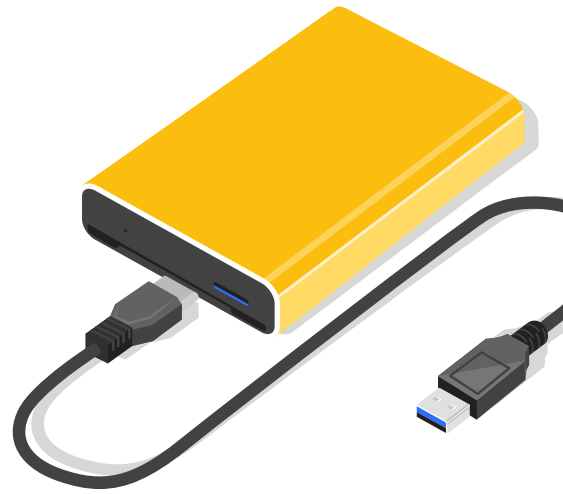
Hinweise liefern, um Ursachen und Schwachstellen zu identifizieren und geeignete Gegenmaßnahmen einzuleiten.

Je nach eingesetztem Betriebssystem und der vorhandenen Infrastruktur stehen unterschiedliche Protokollierungswerkzeuge zur Verfügung. Für Windows-Systeme kann beispielsweise die erweiterte Protokollierung mit dem Dienst Sysmon¹ zusätzliche Informationen erfassen.

EMPFEHLUNGEN

- ◆ Aktivieren Sie die Systemprotokollierung auf verwalteten Nutzergeräten und Servern.
- ◆ Dokumentieren Sie sicherheitsrelevante Ereignisse nachvollziehbar.

¹<https://learn.microsoft.com/de-de/sysinternals/downloads/sysmon>



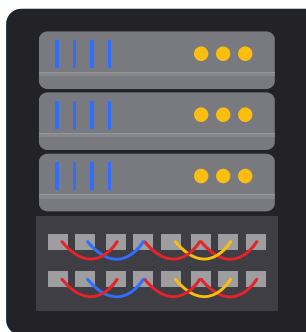
2.6 Externe Datenträger vermeiden

USB-Sticks, externe Festplatten oder andere Speichermedien können eine praktische Möglichkeit zum Datentransfer darstellen. Gleichzeitig erhöhen sie das Risiko eines Datenverlusts oder sogar eines unbeabsichtigten Datenlecks, da solche Medien leicht verloren gehen oder entwendet werden können. Daher wird generell von der Nutzung von externen Speichermedien abgeraten.

Zudem stellen fremde oder unbekannte Speichermedien, insbesondere USB-Sticks, ein Einfallstor für Schadsoftware dar. Vor ihrer Nutzung empfiehlt sich immer eine Überprüfung mit einem aktuellen Antivirenprogramm. Zusätzlich wird

angeraten, die Funktionen „AutoRun“ und „AutoPlay“ zu deaktivieren. Dadurch wird verhindert, dass Programme beim Anschließen eines Datenträgers automatisch ausgeführt werden.

Wo gesicherte und datenschutzkonforme Server- oder Cloud-Lösungen zur Verfügung stehen (z. B. interne Dateiserver), können diese eine sichere Alternative zum Austausch von Dateien über physische Datenträger darstellen. Auch bei der Nutzung von Cloud-Diensten tragen geeignete Sicherheitsmaßnahmen – beispielsweise klar geregelte Zugriffsrechte und eine Multi-Faktor-Authentifizierung – zum Schutz der Daten bei.



TIPP

Sensibilisieren Sie Lehrpersonen, Erzieher sowie alle weiteren Mitarbeitenden für den sicheren Umgang mit externen Datenträgern. Fremde oder unbekannte USB-Sticks sollten grundsätzlich nicht an dienstliche Geräte angeschlossen werden. Empfehlen Sie stattdessen den Austausch von Dateien über die von der Einrichtung vorgesehenen Server- oder Cloud-Lösungen.

EMPFEHLUNGEN

- Verwenden Sie nur Datenträger aus vertrauenswürdigen Quellen.
- Deaktivieren Sie „AutoRun“ und „AutoPlay“.
- Nutzen Sie sichere Server oder Cloud-Lösungen für den Dateiaustausch.



3. NETZWERKE UND

INFRASTRUKTUR SCHÜTZEN

Eine stabile und sichere Netzwerkinfrastruktur bildet die Grundlage für den zuverlässigen Betrieb digitaler Dienste. Netzwerke verbinden Geräte, Nutzer und Anwendungen miteinander und spielen deshalb eine zentrale Rolle für den Schutz von Daten und Systemen.

3.1 Firewalls

Eine Firewall überwacht den Datenverkehr zwischen Netzwerken und entscheidet, welche Verbindungen zugelassen oder blockiert werden. Sie bildet eine wichtige Schutzschicht zwischen dem Internet und den internen Systemen einer Einrichtung.

Viele Router verfügen bereits über integrierte Firewall-Funktionen. In komplexeren Umgebungen oder bei gemeinsam genutzten Infrastrukturen

kann eine dedizierte Firewall zusätzliche Sicherheitsvorteile bieten. Besonders dann, wenn mehrere Organisationen oder Dienste dieselbe Internetanbindung nutzen, empfiehlt sich eine klare Trennung und Absicherung der einzelnen Netzwerke.

EMPFEHLUNGEN

- Stellen Sie sicher, dass die Firewall auf Routern, Servern und Arbeitsgeräten aktiviert ist.
- Überprüfen Sie die Notwendigkeit einer zusätzlichen Abtrennung Ihres internen Netzwerks.



3.2 Netzwerke trennen

Nicht alle Geräte und Nutzer benötigen den Zugriff auf dieselben Daten, Dateien und Ordner. Eine klare Trennung verschiedener Netzwerke erhöht die Sicherheit und erleichtert die Verwaltung.

So kann beispielsweise zwischen einem Netzwerk für das Personal, einem Netzwerk für Kinder und Jugendliche sowie einem Gastnetzwerk unterschieden werden.

Jedes dieser Netzwerke kann eigene Zugriffsrechte und Schutzmechanismen erhalten. Durch eine solche Segmentierung lässt sich verhindern, dass ein Sicherheitsvorfall in einem Bereich automatisch Auswirkungen auf andere Bereiche hat.

Beispiel:

Eine Einrichtung kann folgende Netzwerke vorsehen:

- ◆ Personalnetzwerk mit Zugriff auf interne Dateien, Dienste und Drucker
- ◆ Netzwerk für Kinder und Jugendliche mit zusätzlichen Schutzmaßnahmen
- ◆ Gastnetzwerk mit ausschließlich Internetzugang



EMPFEHLUNGEN

- ◆ Beschränken Sie den Zugriff auf interne Dienste auf berechtigte Personen.
- ◆ Trennen Sie gemeinsam genutzte Netzwerke voneinander.

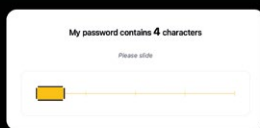
3.3 WLAN-Sicherheit

Drahtlose Netzwerke ermöglichen einen flexiblen Zugang zum Internet und zu internen Diensten. Gleichzeitig stellen sie einen potenziellen Angriffspunkt dar, wenn sie nicht ausreichend geschützt sind. Moderne Verschlüsselungsverfahren wie WPA3 bieten einen höheren Schutz als ältere Standards. Wo dies technisch möglich ist, empfiehlt sich die Nutzung von WPA3.

WLAN-Zugangsdaten verdienen denselben Schutz wie andere Zugangsdaten. Sie sollten nur berechtigten Personen zugänglich sein und regelmäßig überprüft

werden. Zugangsdaten für Personal- oder Gastnetzwerke sollten nicht öffentlich ausgehängt oder an Orten sichtbar sein, an denen Kinder, Jugendliche oder unbefugte Personen sie einsehen können. Insbesondere bei Gastnetzwerken kann darauf geachtet werden, dass keine Verbindung zu internen Systemen besteht und dass gegebenenfalls zusätzliche Schutzmaßnahmen eingerichtet werden.

HOW STRONG IS YOUR PASSWORD?



TIPP

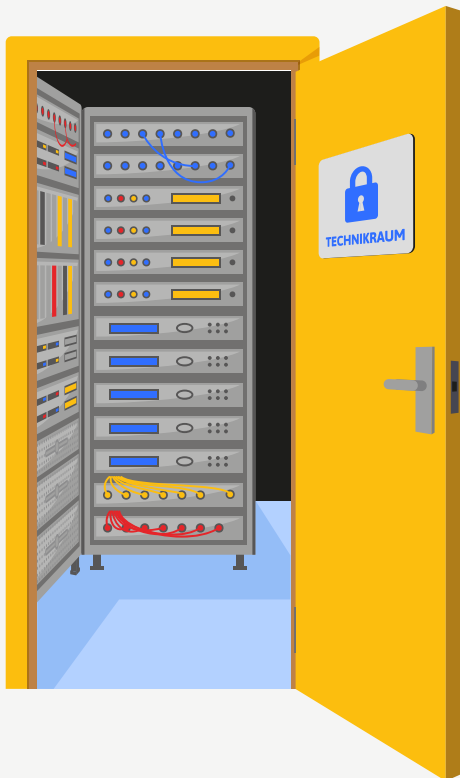
Vorhersehbare WLAN-Passwörter wie Jahreszahlen, Namen der Einrichtung oder einfache Zahlenfolgen bieten nur einen begrenzten Schutz. Lange und individuelle Passsätze erhöhen die Sicherheit deutlich.

Mit dem Passworttest von BEE SECURE können Sie überprüfen, wie sicher ein Passwort oder Passsatz ist: pwdtest.bee-secure.lu



EMPFEHLUNGEN

- ◆ Aktivieren Sie WPA3 oder mindestens WPA2.
- ◆ Trennen Sie Gastnetzwerke vom internen Netzwerk.
- ◆ Sichern Sie Netzwerke (auch das Gastnetzwerk) mit einem Passwort.



3.4 Zutrittskontrolle und physische Sicherheit

Digitale Sicherheit beginnt nicht erst am Bildschirm. Auch der physische Zugang zu Geräten, Dokumenten und technischen Anlagen spielt eine wichtige Rolle.

Server, Netzwerktechnik und andere zentrale Komponenten enthalten häufig sensible Informationen oder ermöglichen den Zugriff auf kritische Systeme. Daher empfiehlt sich eine angemessene Zugangskontrolle für technische Räume und Infrastrukturen.

Ebenso sollen vertrauliche Dokumente, Datenträger und mobile Geräte vor unbefugtem Zugriff geschützt aufbewahrt werden. Die Vergabe von Schlüsseln, Zugangskarten oder Badges sollte nachvollziehbar dokumentiert werden. So lässt sich jederzeit erkennen, wer über welche Zugangsberechtigung verfügt.

EMPFEHLUNGEN

- Beschränken Sie den Zugang zu Serverräumen auf autorisierte Personen.
- Bewahren Sie mobile Geräte und Datenträger bei Nichtgebrauch in abschließbaren Schränken oder Schubladen auf.
- Führen Sie eine Liste der ausgegebenen Schlüssel, Badges und Zutrittskarten.
- Sperren Sie Ihren Bildschirm, wenn Sie den Arbeitsplatz unbeaufsichtigt lassen.
- Schließen Sie Ihr Büro beim Verlassen ab.



4. DATENSCHUTZ UND VERTRAULICHKEIT STÄRKEN

Im Alltag von Schulen und non-formalen Einrichtungen werden zahlreiche personenbezogene Daten verarbeitet. Dazu gehören beispielsweise Fotos, Gesundheitsinformationen oder Kontaktdaten. Der sorgfältige Umgang mit diesen Informationen trägt wesentlich zum Schutz der Privatsphäre aller Beteiligten bei.

4.1 DSGVO-konforme Dienste auswählen

Viele digitale Werkzeuge erleichtern den Arbeitsalltag von Schulen und anderen Einrichtungen. Gleichzeitig verarbeiten diese Dienste häufig personenbezogene Daten.

Vor der Einführung neuer Anwendungen empfiehlt sich deshalb eine Prüfung ihrer Vereinbarkeit mit

der europäischen Datenschutz-Grundverordnung (DSGVO). Dabei können insbesondere die Art der verarbeiteten Daten, die Speicherorte sowie die Datenschutzbestimmungen des Anbieters berücksichtigt werden.



TIPP

Nicht jede praktische Anwendung erfüllt automatisch die Anforderungen an Datenschutz und Informationssicherheit. Prüfen Sie neue Dienste deshalb bereits vor ihrer Einführung auf ihre Vereinbarkeit mit der DSGVO und den internen Richtlinien Ihrer Einrichtung.

Eine Übersicht der zugelassenen oder empfohlenen Dienste erleichtert dem Personal die Auswahl geeigneter Werkzeuge und trägt zu einer einheitlichen Nutzung innerhalb der Einrichtung bei.

EMPFEHLUNGEN

- Prüfen Sie neue Anwendungen vor ihrer Einführung auf ihre Vereinbarkeit mit der DSGVO.
- Erstellen und pflegen Sie eine Liste der von Ihrer Einrichtung freigegebenen digitalen Dienste. Orientieren Sie sich dabei nach Möglichkeit an den Empfehlungen zuständiger Stellen, beispielsweise des MENJE oder des CGIE.
- Informieren Sie das Personal darüber, welche Anwendungen genutzt werden dürfen.



4.2 Vertraulichkeit gewährleisten

Im Rahmen ihrer Tätigkeit erhalten viele Mitarbeitende Zugang zu sensiblen Informationen über Kinder, Jugendliche, Familien oder Kollegen. Ein verantwortungsvoller Umgang mit diesen Daten trägt wesentlich zum Schutz der Privatsphäre bei.

Besonders Personen mit erweiterten Zugriffsrechten, beispielsweise Informatiker, Administratoren oder externe Dienstleister, verfügen häufig über Einblicke in Systeme, Dateien oder Protokolle. Der Zugriff auf solche Informationen sollte sich auf jene Inhalte beschränken, die für die jeweilige Aufgabe erforderlich sind.

Gleichzeitig empfiehlt es sich, Mitarbeitenden nur Zugriff auf jene Ordner, Dateien oder Systeme zu gewähren, die sie für ihre tägliche Arbeit tatsächlich benötigen. Dadurch wird das Risiko eines unbeabsichtigten Zugriffs auf sensible Informationen reduziert.

Vertraulichkeitsvereinbarungen können dazu beitragen, Erwartungen und Verantwortlichkeiten transparent festzuhalten und das Bewusstsein für den Schutz sensibler Daten zu stärken.



WAS IST EINE VERTRAULICHKEITSVEREINBARUNG?

Eine Vertraulichkeitsvereinbarung – häufig auch als „Non-Disclosure Agreement“ (NDA) bezeichnet – legt fest, dass vertrauliche Informationen ausschließlich im vereinbarten Rahmen genutzt und nicht an unbefugte Personen weitergegeben werden dürfen.

EMPFEHLUNGEN

- Beschränken Sie Zugriffsrechte auf die Personen, die diese tatsächlich benötigen.
- Schließen Sie bei Bedarf Vertraulichkeitsvereinbarungen mit externen Dienstleistern ab.
- Überprüfen Sie regelmäßig die vergebenen Berechtigungen.
- Sensibilisieren Sie Mitarbeitende für den Umgang mit vertraulichen Informationen.



4.3 Datenschutzkultur fördern

Datenschutz entsteht nicht allein durch Technik. Ebenso entscheidend ist ein bewusster und verantwortungsvoller Umgang mit personenbezogenen Daten im Arbeitsalltag. Mitarbeitende profitieren von klaren Informationen über ihre Rechte und Pflichten im Zusammenhang mit der DSGVO. Regelmäßige Sensibilisierung und Weiterbildungen können dazu beitragen, Datenschutzrisiken frühzeitig zu erkennen und angemessen zu handeln.

Zu einer gelebten Datenschutzkultur gehört außerdem die regelmäßige Überprüfung und Löschung

personenbezogener Daten, sobald diese nicht mehr benötigt werden oder gesetzliche Aufbewahrungsfristen abgelaufen sind. Dies betrifft sowohl digitale Daten – beispielsweise auf Servern, Webseiten oder in Anwendungen – als auch Papierdokumente mit personenbezogenen Informationen.

Darüber hinaus erleichtert eine Ansprechperson für Datenschutzfragen den Umgang mit Unsicherheiten oder Vorfällen. Viele Einrichtungen bestimmen hierfür einen „Data Protection Officer“ (DPO).



EMPFEHLUNGEN

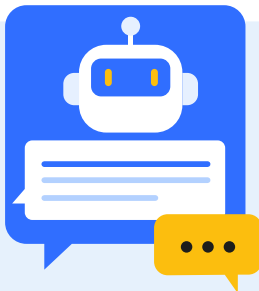
- Benennen Sie eine Ansprechperson für Datenschutzfragen und fördern Sie einen offenen Umgang mit Fragen oder Unsicherheiten.
- Planen Sie regelmäßige Sensibilisierungsmaßnahmen.

4.4 Künstliche Intelligenz verantwortungsvoll nutzen

KI-gestützte Werkzeuge und Chatbots gehören inzwischen in vielen Einrichtungen zum Arbeitsalltag. Sie können Recherchen, Übersetzungen, Texterstellung oder andere Aufgaben wesentlich erleichtern.

Gleichzeitig verdienen personenbezogene Daten bei der Nutzung solcher Dienste besondere Aufmerksamkeit. Je nach Plattform können eingegebene Informationen verarbeitet, gespeichert oder zur Weiterentwicklung der Systeme verwendet werden.

Bei der Nutzung öffentlicher KI-Anwendungen empfiehlt sich deshalb ein zurückhaltender Umgang mit personenbezogenen Daten. Namen, Adressen, Telefonnummern, Gesundheitsdaten oder andere sensible Informationen über Kinder, Jugendliche, Eltern oder Mitarbeitende gehören grundsätzlich nicht in öffentliche KI-Systeme.



TIPP

Personenbezogene Angaben können vor der Nutzung von KI-Anwendungen durch Platzhalter ersetzt oder vorab anonymisiert werden. Anstelle von Namen können beispielsweise Formulierungen wie „Schüler A“, „Mitarbeiter B“ oder „Person X“ verwendet werden.



EMPFEHLUNGEN

- Geben Sie keine personenbezogenen Daten in öffentliche KI-Anwendungen ein.
- Verwenden Sie möglichst anonymisierte oder fiktive Beispiele.
- Informieren Sie Mitarbeitende über Chancen und Risiken von KI-Anwendungen.

INFO FÜR DAS PÄDAGOGISCHE PERSONAL

Lehrer, Erzieher und Betreuer finden auf der Seite [KI-Kompass.lu](https://www.ki-kompass.lu) Orientierung, Material und Weiterbildungsangebote für den sicheren und verantwortungsvollen Einsatz von KI im pädagogischen Alltag.

5. DATEN SICHERN UND WIEDERHERSTELLEN

Der Verlust von Daten hat oft ganz alltägliche Ursachen und ist nicht ausschließlich die Folge von Cyberangriffen. Häufig sind es alltägliche Situationen – ein defektes Gerät, ein versehentlich gelöscht Dokument oder ein verlorenes Smartphone –, die dazu führen, dass wichtige Informationen unzugänglich sind. Eine durchdachte Strategie zur Speicherung und Sicherung von Daten trägt dazu bei, Ausfallzeiten zu reduzieren und wichtige Informationen im Bedarfsfall wiederherstellen zu können.

5.1 Speicherorte bewusst wählen

Der Ort, an dem Daten gespeichert werden, hat einen direkten Einfluss auf deren Sicherheit und Verfügbarkeit. Werden Dateien ausschließlich auf einzelnen Geräten gespeichert, besteht das Risiko, dass sie bei einem Defekt, Verlust oder Diebstahl nicht mehr verfügbar sind. Gemeinsame Speicherorte erleichtern dagegen die Zusammenarbeit und verringern die Abhängigkeit von einzelnen Geräten.

Wo geeignete Lösungen zur Verfügung stehen, können zentrale Dateiserver, vertrauenswürdige Cloud-Dienste oder andere gemeinsam verwaltete Speicherorte eine sinnvolle Alternative darstellen. Physische Datenträger wie USB-Sticks oder externe Festplatten können für bestimmte Zwecke weiterhin nützlich sein, gehen jedoch mit zusätzlichen Risiken einher. Sie können verloren gehen, beschädigt werden oder in falsche Hände geraten.

EMPFEHLUNGEN

- Speichern Sie wichtige Dateien möglichst in einem gemeinsam verwalteten Speichersystem.
- Vermeiden Sie die ausschließliche Speicherung auf nur einem Gerät.



5.2 Geräteortung nutzen

Mobile Geräte wie Smartphones oder Tablets enthalten häufig berufliche Daten und ermöglichen den Zugriff auf verschiedene Dienste und Benutzerkonten. Geht ein Gerät verloren oder wird es gestohlen, können Ortungs- und Kontrollfunktionen dabei helfen, es wiederzufinden oder aus der Ferne zu sperren. Viele Betriebssysteme verfügen bereits über entsprechende Funktionen wie „Wo ist?“ oder „Mein Gerät finden“.

Zusätzlich kann ein Verzeichnis der eingesetzten Mobilgeräte die Verwaltung erleichtern. Dazu gehören beispielsweise Gerätetypen, Seriennummern oder die „International Mobile Equipment Identity“ (IMEI) von Mobiltelefonen. Diese Informationen können im Verlustfall hilfreich sein und die Zusammenarbeit mit Polizei oder Mobilfunkanbietern erleichtern.



WAS IST DIE IMEI?

Die „International Mobile Equipment Identity“ (IMEI) ist eine eindeutige Identifikationsnummer für Mobiltelefone. Sie kann unter anderem bei Verlust oder Diebstahl eines Geräts hilfreich sein. Die IMEI befindet sich in der Regel auf der Verpackung des Geräts und kann bei vielen Mobiltelefonen auch direkt über die Eingabe des Codes `*#06#` in der Telefon-App angezeigt werden.

EMPFEHLUNGEN

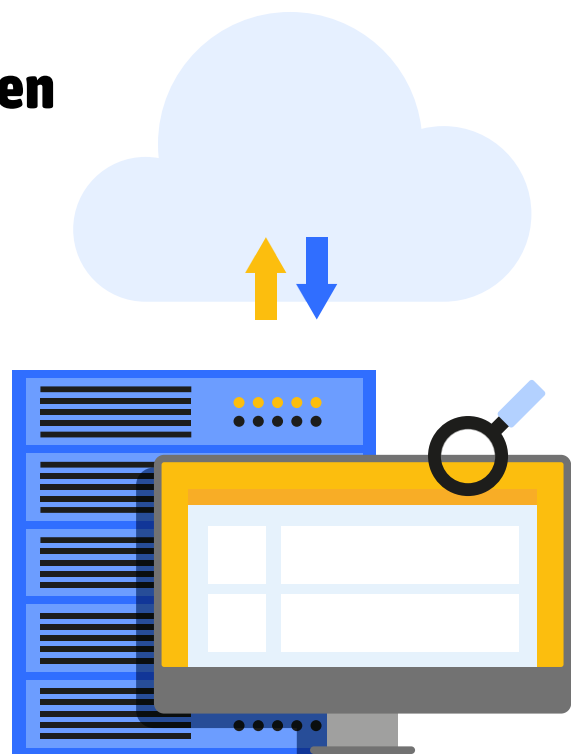
- Aktivieren Sie Ortungsfunktionen auf mobilen Dienstgeräten.
- Dokumentieren Sie Gerätetypen, Seriennummern und IMEI.
- Legen Sie einen Ablauf für den Verlust oder Diebstahl mobiler Geräte fest.
- Sperren oder löschen Sie verlorene Geräte möglichst zeitnah aus der Ferne.



5.3 Back-ups planen und testen

Back-ups gehören zu den wichtigsten Maßnahmen zum Schutz vor Datenverlust. Sie ermöglichen die Wiederherstellung wichtiger Informationen nach technischen Störungen, Cyberangriffen oder menschlichen Fehlern.

Zu Beginn empfiehlt sich eine Übersicht aller Speicherorte innerhalb der Einrichtung. Dazu können Arbeitscomputer, mobile Geräte, Dateiserver, Cloud-Dienste oder andere Speichersysteme gehören. Für jeden Speicherort kann anschließend festgelegt werden, wie häufig eine Sicherung erfolgen soll und wie viel Datenverlust im Ernstfall akzeptabel wäre.



Eine bewährte Orientierung bietet die sogenannte 3-2-1-0-Regel:

3 Kopien der Daten

Neben den Originaldaten existieren mindestens zwei zusätzliche Sicherungskopien.

2 unterschiedliche Speichermedien

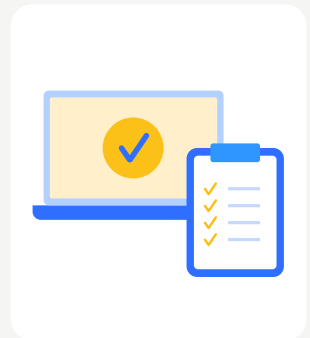
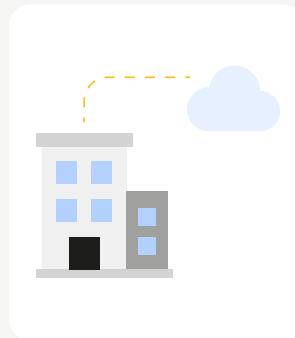
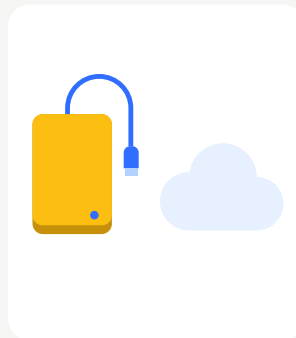
Die Sicherungen werden auf mindestens zwei verschiedenen Speichermedien oder -lösungen gespeichert, beispielsweise auf einer externen Festplatte und in einer Cloud-Lösung.

1 externe Kopie

Mindestens eine Sicherung befindet sich außerhalb der Einrichtung, um auch bei Brand, Wasserschaden oder anderen schwerwiegenden Vorfällen verfügbar zu bleiben.

0 Fehler bei der Wiederherstellung

Back-ups werden regelmäßig getestet, damit beschädigte oder unvollständige Sicherungen frühzeitig erkannt und behoben werden können.



INFO FÜR DAS PÄDAGOGISCHE PERSONAL

Auch die Lehrpersonen und das pädagogische Fachpersonal sollten sich bewusst sein, wie wichtig die regelmäßige Sicherung ihrer Arbeitsdaten ist. Unterrichtsmaterialien, Dokumentationen oder andere beruflich genutzte Dateien sollten regelmäßig in den von der Einrichtung vorgesehenen Speicherlösungen gesichert werden und nicht ausschließlich auf lokalen oder privaten Geräten gespeichert sein.

EMPFEHLUNGEN

- Erstellen Sie regelmäßig Back-ups aller wichtigen Daten.
- Nutzen Sie die 3-2-1-0-Regel als Orientierung.



6. KINDER UND

JUGENDLICHE SCHÜTZEN

Kinder und Jugendliche bewegen sich heute viel in digitalen Räumen. Sie lernen, spielen, kommunizieren und informieren sich online. Gleichzeitig stoßen sie dabei nicht immer auf Inhalte oder Angebote, die ihrem Alter und ihrer Entwicklung entsprechen. Technische Schutzmaßnahmen können helfen, Risiken zu begrenzen und einen sicheren Rahmen für die Nutzung digitaler Angebote zu schaffen.

6.1 Inhaltsfilter einsetzen

Inhaltsfilter können den Zugang zu Webseiten und Online-Angeboten einschränken, die für Kinder und Jugendliche ungeeignet oder potenziell schädlich sind. Beispielsweise können so Inhalte für Erwachsene, Glücksspiele, Gewaltdarstellungen, Schadsoftware sowie bestimmte Formen von Online-Betrug eingeschränkt werden.

Je nach technischer Infrastruktur können solche Filter auf Netzwerkebene, auf einzelnen Geräten oder direkt in Anwendungen eingerichtet werden. Ergänzend können Kindersicherheitseinstellungen auf Mobilgeräten und in Apps genutzt werden, um den Zugriff auf altersunangemessene Inhalte weiter einzuschränken.

NÜTZLICHER HINWEIS

Für Bildungseinrichtungen und andere Organisationen stehen über RESTENA verschiedene Inhaltsfilter zur Verfügung, die den Zugang zu ungeeigneten oder potenziell schädlichen Online-Inhalten einschränken können. Gemeinden und andere interessierte Einrichtungen können sich direkt an RESTENA wenden, um Informationen zu verfügbaren Filterlösungen und deren Einrichtung zu erhalten. Da sich Online-Inhalte und Plattformen kontinuierlich verändern, empfiehlt sich eine regelmäßige Überprüfung der Filtereinstellungen.

Kontakt: restena.lu/fr/contact



WICHTIG

Kein Filtersystem kann sämtliche problematischen Inhalte zuverlässig erkennen oder blockieren. Inhaltsfilter ergänzen daher die pädagogische Begleitung oder Aufsicht der Kinder, ersetzen sie jedoch nicht.

- Richten Sie Inhaltsfilter auf der Netzwerk-, Geräte- oder Anwendungsebene ein.
- Aktivieren Sie Kindersicherheitseinstellungen auf Mobilgeräten und in Apps.



6.2 Kindgerechte Benutzerkonten

Bei Geräten, die Kindern oder Jugendlichen zur Verfügung gestellt werden, empfiehlt sich eine altersgerechte Konfiguration. Eigene Benutzerkonten ermöglichen eine bessere Anpassung von Berechtigungen, Anwendungen und Sicherheitseinstellungen. Gleichzeitig erleichtern sie die Trennung zwischen den Zugängen des Personals und jenen der Kinder oder Jugendlichen.

Wenn Computer oder Tablets bereitgestellt werden, empfiehlt sich die Nutzung persönlicher Benutzerkonten für jedes Kind. In Schulen kann dies beispielsweise über die IAM-Konten erfolgen. Individuelle Konten erleichtern die Verwaltung von Zugriffsrechten und fördern einen verantwortungsvollen Umgang mit digitalen Werkzeugen.

Wenn keine persönlichen Benutzerkonten für jedes einzelne Kind eingerichtet werden können, empfiehlt sich zumindest eine Trennung zwischen den Konten

des Personals und jenen der Kinder oder Jugendlichen. Neben dem Hauptkonto für Erwachsene kann dafür ein separates Benutzerkonto für Kinder oder Jugendliche eingerichtet werden. Dieses Konto sollte über eingeschränkte Berechtigungen verfügen und insbesondere keine Administratorrechte besitzen. Zusätzliche Jugendschutz- oder Parental-Control-Funktionen können die Verwaltung und Begleitung durch Erwachsene unterstützen.

Kindgerechte Konten können beispielsweise verhindern, dass Software installiert, Sicherheitseinstellungen verändert oder ungeeignete Inhalte aufgerufen werden. Bereits vorinstallierte Anwendungen und Lernangebote erleichtern zudem die sichere Nutzung der Geräte und reduzieren die Notwendigkeit zusätzlicher Installationen.

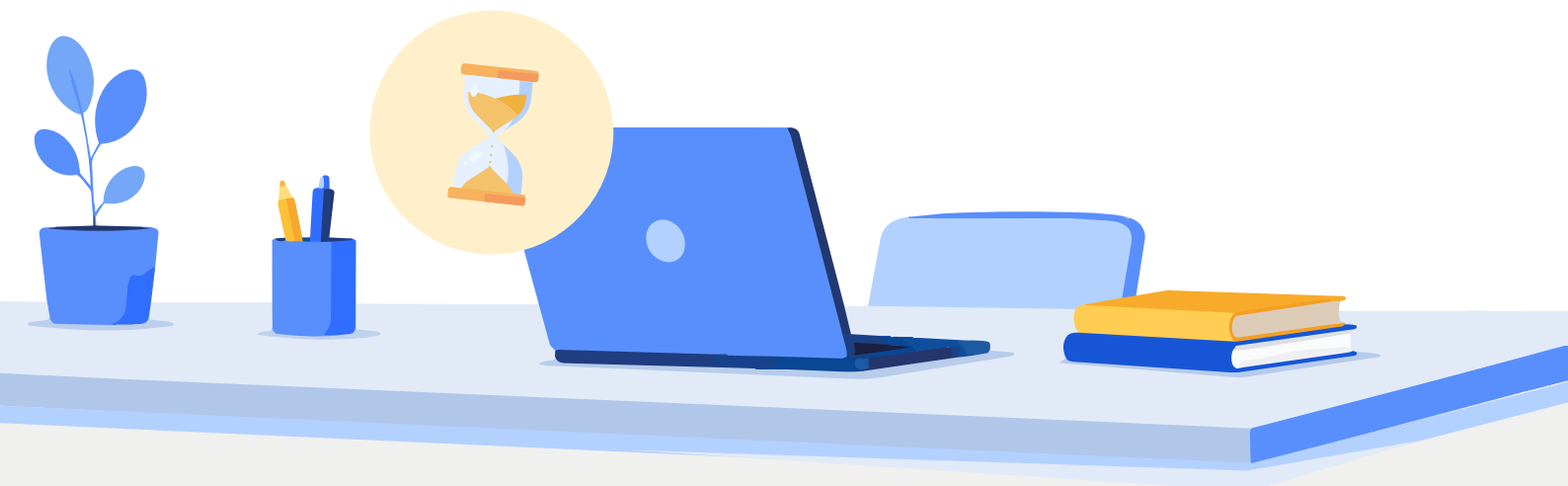
INFO FÜR DAS PÄDAGOGISCHE PERSONAL

Auch vernetztes Spielzeug, digitale Lernplattformen oder KI-gestützte Anwendungen verdienen besondere Aufmerksamkeit. Vor ihrem Einsatz empfiehlt sich eine Prüfung der Datenschutz- und Sicherheitseinstellungen sowie der Altersempfehlung.

EMPFEHLUNGEN

- Richten Sie nach Möglichkeit für jedes Kind ein persönliches Benutzerkonto ein.
- Verwenden Sie für Kinder ausschließlich Standardkonten ohne Administratorrechte.
- Nutzen Sie Jugendschutz- oder Parental-Control-Funktionen.





6.3 Nutzungszeiten festlegen

Je nach Einrichtung kann es sinnvoll sein, den Zugang zum Internet auf bestimmte Zeitfenster zu beschränken. Dies betrifft insbesondere Wohnstrukturen, Internate oder andere Einrichtungen, in denen Kinder und Jugendliche auch außerhalb von Unterrichts- oder Betreuungszeiten Zugang zu digitalen Geräten haben.

Zeitlich gesteuerte WLAN-Netzwerke oder eine technisch festgelegte Bildschirmzeit können dabei helfen, Nutzungszeiten an die Bedürfnisse der jeweiligen Einrichtung anzupassen. Solche Maßnahmen tragen dazu bei, unbeaufsichtigte oder exzessive Nutzungsphasen zu reduzieren, und unterstützen einen ausgewogenen Umgang mit digitalen Medien.

INFO FÜR DAS PÄDAGOGISCHE PERSONAL

Zeitliche Einschränkungen können einen Rahmen setzen. Besonders wirksam werden sie jedoch in Kombination mit Gesprächen über Mediennutzung, Schlafgewohnheiten und digitale Balance.

EMPFEHLUNGEN

- Legen Sie altersgerechte Nutzungszeiten für gemeinsam genutzte Geräte fest.
- Nutzen Sie technische Möglichkeiten zur zeitlichen Steuerung des Internetzugangs.



7. AUF SICHERHEITSVORFÄLLE VORBEREITET SEIN

Auch gut geschützte Einrichtungen bleiben nicht von technischen Störungen oder Sicherheitsvorfällen verschont. Entscheidend ist deshalb nicht nur die Prävention, sondern auch die Vorbereitung auf Situationen, in denen etwas schief läuft.

7.1 Weiterbildung

Digitale Technologien entwickeln sich kontinuierlich weiter. Gleichzeitig entstehen neue Sicherheitsrisiken, Betrugsformen und Angriffsmethoden.

Regelmäßige Weiterbildungen helfen dabei, aktuelle Entwicklungen zu verfolgen und bestehende Kenntnisse aufzufrischen. Dies betrifft nicht nur

technisch Verantwortliche, sondern auch Personen, die digitale Werkzeuge im Berufsalltag nutzen. Je nach Aufgabenbereich können Themen wie Cybersicherheit, Datenschutz, Cyberhygiene, Medienkompetenz oder der Umgang mit künstlicher Intelligenz relevant sein.

INFO FÜR DAS PÄDAGOGISCHE PERSONAL

Auch Lehrpersonen und Erzieher profitieren von regelmäßigen Weiterbildungen in Bereichen wie digitale Medien und aktuelle Online-Trends. Dies erleichtert die Begleitung von Kindern und Jugendlichen im digitalen Alltag. Nutzen Sie die vielfältigen Weiterbildungsangebote, beispielsweise vom *Institut national d'administration publique*, dem *Institut de Formation de l'Éducation Nationale*, der *Plattform*, dem *Digital Learning Hub* oder dem *Lifelong Learning Centre*.

EMPFEHLUNGEN

- Planen Sie regelmäßige Weiterbildungen für IT-Verantwortliche und weitere Mitarbeitende.
- Informieren Sie das Personal über aktuelle Betrugsmaschen und neue Sicherheitsrisiken.

7.2 Kontaktlisten bereithalten

Im Fall eines Sicherheitsvorfalls zählt häufig jede Minute. Eine aktuelle Kontaktliste erleichtert die rasche Kommunikation und unterstützt die Koordination der notwendigen Maßnahmen.

Je nach Einrichtung können in der Liste interne und externe Ansprechpersonen erfasst werden. Dazu

gehören beispielsweise technisch Verantwortliche, Datenschutzbeauftragte, externe Dienstleister oder zuständige Meldestellen. Auch die Kontaktdaten des zuständigen *Computer Emergency Response Teams* können Teil einer solchen Übersicht sein. Die Liste sollte regelmäßig überprüft und bei personellen oder organisatorischen Änderungen aktualisiert werden.



WAS IST EIN CERT?

Ein „Computer Emergency Response Team“, kurz CERT, unterstützt Organisationen bei der Bewältigung von Cybervorfällen und technischen Sicherheitsproblemen. Eine Liste aller in Luxemburg ansässigen CERTs finden Sie unter cert.lu.

7.3 Reaktionspläne vorbereiten

Wenn ein Sicherheitsvorfall eintritt, stehen Verantwortliche häufig unter Zeitdruck. Ein vorbereiteter Reaktionsplan kann helfen, wichtige Schritte systematisch abzuarbeiten. Der Plan kann festlegen, wer informiert wird, welche Sofortmaßnahmen vorgesehen sind und wie Entscheidungen dokumentiert werden. Dadurch wird vermieden, dass wichtige Aufgaben übersehen werden.

Je nach Art des Vorfalls können erste Maßnahmen beispielsweise darin bestehen, betroffene Geräte vom Netzwerk zu trennen, Zugangsdaten zu ändern oder zuständige Fachpersonen zu informieren. Regelmäßige Übungen oder Besprechungen können dazu beitragen, Abläufe bekannt zu machen und die Handlungsfähigkeit im Ernstfall zu stärken.



RUHE BEWAHREN

Ein Sicherheitsvorfall erfordert ein rasches, aber besonnenes Handeln. Vermeiden Sie vorschnelle Entscheidungen und arbeiten Sie den vorbereiteten Reaktionsplan Schritt für Schritt ab. Klare Abläufe und festgelegte Zuständigkeiten helfen dabei, die Situation systematisch zu bewerten, geeignete Maßnahmen einzuleiten und weitere Schäden möglichst zu begrenzen.

EMPFEHLUNGEN



- Erstellen Sie eine aktuelle Kontaktliste für Sicherheitsvorfälle und erfassen Sie interne und externe Ansprechpersonen.
- Erarbeiten Sie einen Reaktionsplan für Sicherheitsvorfälle.
- Legen Sie Verantwortlichkeiten und Kommunikationswege fest.
- Dokumentieren Sie Sofortmaßnahmen für unterschiedliche Szenarien.
- Üben Sie den Ablauf regelmäßig gemeinsam mit den beteiligten Personen.

8. PRAXISBEISPIELE

Jede Einrichtung verfügt über unterschiedliche technische Voraussetzungen und organisatorische Rahmenbedingungen. Die folgenden Beispiele zeigen, wie verschiedene Sicherheitsmaßnahmen in typischen Alltagssituationen umgesetzt werden können. Die beschriebenen Maßnahmen dienen als Orientierung und können an die jeweiligen Bedürfnisse der Einrichtung angepasst werden.

Fallbeispiel 1 Datensicherung in einer Grundschule

AUSGANGSSITUATION

Eine Grundschule möchte sicherstellen, dass wichtige Daten auch nach einem technischen Defekt oder einem Sicherheitsvorfall verfügbar bleiben.

HERAUSFORDERUNGEN

- unterschiedliche Speicherorte identifizieren
- Datenverluste vermeiden
- Wiederherstellung ermöglichen

MÖGLICHE MAßNAHMEN

• Bestandsaufnahme der Speicherorte

Berücksichtigt werden können unter anderem Arbeitscomputer, Server, Cloud-Dienste und mobile Geräte.

• Back-up-Strategie festlegen

Die 3-2-1-0-Regel bietet eine bewährte Orientierung für die Erstellung von Sicherungskopien. Mehr dazu im Kapitel 5.3.

• Wiederherstellung testen

Regelmäßige Tests helfen dabei, die Funktionsfähigkeit der Back-ups zu überprüfen.

INFO FÜR DAS PÄDAGOGISCHE PERSONAL

Auch Unterrichtsmaterialien, Dokumentationen, Fotos oder andere beruflich genutzte Dateien verdienen eine angemessene Sicherung, unabhängig davon, auf welchem Gerät sie gespeichert sind.

Werden für berufliche Zwecke private Geräte genutzt, empfiehlt sich besondere Vorsicht. Auf diesen Geräten gelten unter Umständen nicht dieselben Sicherheitsmaßnahmen wie auf den Geräten der Einrichtung. Speichern Sie berufliche Daten deshalb möglichst in den von der Einrichtung vorgesehenen Speicherlösungen und vermeiden Sie die ausschließliche Ablage auf privaten Geräten.

Fallbeispiel 2 Internetzugang in einer Wohnstruktur oder einem Internat

AUSGANGSSITUATION

In einer Wohnstruktur nutzen Kinder und Jugendliche das Internet täglich – für Hausaufgaben, Unterhaltung oder den Kontakt mit Familie und Freunden. Die Einrichtung möchte diese Nutzung ermöglichen und gleichzeitig einen angemessenen Schutz gewährleisten.

HERAUSFORDERUNGEN

- Zugang zu ungeeigneten Inhalten vermeiden
- unterschiedliche Nutzergruppen berücksichtigen
- unbeaufsichtigte Nutzung während der Nacht reduzieren
- Netzwerksicherheit gewährleisten

MÖGLICHE MAßNAHMEN

• Inhaltsfilter

Die Nutzung von Inhaltsfiltern kann dazu beitragen, den Zugang zu ungeeigneten oder potenziell schädlichen Inhalten einzuschränken. RESTENA bietet hierfür verschiedene Filterlösungen an.

• Getrennte Netzwerke

Separate Netzwerke für Personal, Bewohner und Gäste erleichtern die Verwaltung und erhöhen die Sicherheit.

• Zeitliche Steuerung des Internetzugangs

Je nach Konzept der Einrichtung kann das Abschalten des Internetzugangs außerhalb der vorgesehenen Nutzungszeiten, also zum Beispiel zur Schlafenszeit, sinnvoll sein.

Fallbeispiel 3 Computerarbeitsplätze in einer Maison relais

AUSGANGSSITUATION

Eine Maison relais stellt Kindern Computer für Hausaufgaben, Lernangebote oder kreative Aktivitäten zur Verfügung.

HERAUSFORDERUNGEN

- altersgerechte Nutzung ermöglichen
- ungewollte Änderungen an Geräten verhindern
- sichere Internetnutzung fördern

MÖGLICHE MAßNAHMEN

• Benutzerkonten einrichten

Separate Konten für Kinder und Erwachsene erleichtern die Verwaltung von Berechtigungen und Sicherheitseinstellungen. Kindgerechte Benutzerkonten profitieren von eingeschränkten Berechtigungen. Dadurch können Kinder und Jugendliche beispielsweise keine Programme oder Spiele selbst installieren und keine sicherheitsrelevanten Systemeinstellungen verändern.

• Geeignete Anwendungen bereitstellen

Vorinstallierte Lernprogramme und ausgewählte Anwendungen können die sichere Nutzung unterstützen.

• Netzwerk absichern

Getrennte Netzwerke für Kinder und Personal erhöhen die Sicherheit und vereinfachen die Verwaltung. Eine eindeutige Benennung der Netzwerke erleichtert die Orientierung und reduziert das Risiko von Verwechslungen. So könnten beispielsweise Bezeichnungen wie „MR_WLAN_Kids“ und „MR_WLAN_Staff“ verwendet werden.

• Inhaltsfilter einsetzen

Filter können den Zugang zu ungeeigneten Inhalten einschränken und die sichere Nutzung fördern.

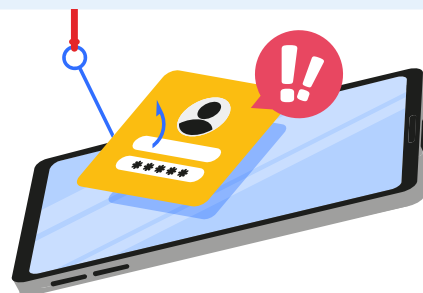
DAS ERGEBNIS

Die Geräte sind für die vorgesehenen Aktivitäten nutzbar, während gleichzeitig wichtige Sicherheitsmaßnahmen berücksichtigt werden.

Fallbeispiel 4 Reaktion auf einen Phishing-Vorfall

AUSGANGSSITUATION

Eine Mitarbeiterin oder ein Mitarbeiter erhält eine E-Mail mit einem Link zu einer vermeintlichen Microsoft-Teams-Seite. Nach der Anmeldung entsteht der Verdacht, dass es sich um einen Phishing-Versuch gehandelt hat.



HERAUSFORDERUNGEN

- möglichen Missbrauch des Benutzerkontos verhindern
- zuständige Stellen informieren

● Weitere Konten berücksichtigen

Wurde dasselbe Passwort an anderer Stelle verwendet, empfiehlt sich auch dort eine Änderung der Zugangsdaten.

MÖGLICHE MAßNAHMEN

● Zuständige Stellen kontaktieren

Informieren Sie so schnell wie möglich interne IT-Verantwortliche sowie gegebenenfalls das Centre de gestion informatique de l'éducation (CGIE) oder andere Fachstellen.

● Zugangsdaten ändern und Sicherheit überprüfen

Ändern Sie umgehend das betroffene Passwort, gegebenenfalls mit Unterstützung von Fachstellen. Überprüfen Sie, ob noch offene Anmeldesitzungen bestehen und beenden Sie sie. Aktivieren Sie die Multi-Faktor-Authentifizierung.

● Vorfall dokumentieren und melden

Zeitpunkt, betroffene Plattform und möglicherweise preisgegebene Informationen werden festgehalten. Liegt ein wesentlicher Vorfall vor, der einer gesetzlichen Meldepflicht unterliegt, melden Sie ihn den zuständigen Datenschutz- oder Cybersicherheitsbehörden.

NÜTZLICHE LINKS

BEE SECURE Im digitalen Zeitalter ein Vorbild sein

bee-secure.lu/de/publikation/erzieher-und-lehrer-im-umgang-mit-medien-und-technologien/

CGIE

cgie.lu

CIRCL

circl.lu

CNPD

cnpd.public.lu

Fondation RESTENA – DNS Server

restena.lu/fr/service/serveurs-dns

Guide pratique – Mettre en place la sécurité de l'information : les étapes clés pour bien débiter

anssi.extranet.etat.lu/fr/actualites/2026/approche-securite-information

Microsoft – What is incident response

microsoft.com/de-de/security/business/security-101/what-is-incident-response

BIBLIOGRAFIE

Cyber fundamentals SMALL

atwork.safeonweb.be/tools-resources/cyberfundamentals-framework

Microsoft Phishing

support.microsoft.com/de-de/windows/sch%C3%BCtzen-sie-sich-vor-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44

Was ist die 3-2-1-1-0-Backup-Regel?

zmanda.com/de/blog/understanding-the-3-2-1-1-0-backup-rule/

Weitere Informationen finden Sie unter

BEE-SECURE.LU