F 7.10

Datenschutz

Datenschutzgerechte Passwortstrategien – Ein Leitfaden für sichere digitale Schulwelten

Carsten Arntz, Oberstudiendirektor i. K.

© Carsten Arntz, 2023, Passwortlogin, generiert mit DALL-E innerhalb ChatGPT-4 Plus

Dieser Beitrag beschäftigt sich mit den Herausforderungen und Lösungsansätzen beim Umgang mit digitalen Daten in Bildungseinrichtungen, insbesondere durch die Anwendung von Passwortsicherheitsmaßnahmen und Verschlüsselungstechniken. Er betont die Notwendigkeit, das Bewusstsein und die Praktiken im Umgang mit Passwörtern zu verbessern sowie die Bedeutung der Implementierung fortgeschrittener Verschlüsselungsmethoden zum Schutz vor unautorisierten Zugriffen. Dabei wird auf die Rolle der Schulleitung in diesem Prozess und die technische Unterstützung zur Erhöhung der digitalen Sicherheit hingewiesen.

KOMPETENZPROFIL

Zielgruppe:	Schulleitungen
Schlüsselbegriffe:	Passwörter, Datenschutz, Compliance, Cybersecurity
Einsatzfeld:	Schulleitung, Schulleitungsteams
Thematische Bereiche:	KI, Schulentwicklung

Inhaltsverzeichnis

1. Das Passwort-Paradoxon: Bequemlichkeit versus Sicherheit 3
2. Die Rolle der Verschlüsselungstechnologie 5
3. Wie sichere Passwörter die Privatsphäre schützen können 8
4. Erkennung und Vermeidung von Phishing-Angriffen 10
5. Schutz vor Malware und Ransomware 12
6. Einhaltung von Datenschutz- und Compliance-Anforderungen in der Schulleitung am Beispiel der Stellenplanung 14
7. Cloud-Sicherheit 17
8. Zukünftige Trends in der Cybersicherheit mit Künstlicher Intelligenz 19

Literatur 22

1. Das Passwort-Paradoxon: Bequemlichkeit versus Sicherheit

Das weitverbreitete Phänomen der Nachlässigkeit von Menschen im Umgang mit Passwörtern im Alltag stellt ernsthafte Sicherheitsrisiken für Einzelpersonen und den Schulbetrieb dar. In einer Welt, in der digitale Technologien fest in unseren Alltag integriert sind, bilden sichere Passwörter die erste Schutzlinie gegen unautorisierten Zugriff auf persönliche und berufliche Daten. Trotz dieser Bedeutung zeigen Studien und Beobachtungen, dass viele Menschen beim Erstellen von Passwörtern äußerst nachlässig sind, was zu Datenverlust, Identitätsdiebstahl oder finanziellen Verlusten führen kann.

Sehr einfach, schlicht und oft leicht zu merken. Das sind die Merkmale vieler Passwörter, die Menschen wählen, wie „123456", „password" oder „123456789".[1] Diese Simplizität hat jedoch ihren Preis, da solche Passwörter schnell und einfach von Cyberkriminellen geknackt werden können. Eine Studie von Security.org[2] aus dem Jahr 2023 zeigt, dass ein überraschend hoher Prozentsatz der Nutzer immer noch einfache Sequenzen oder leicht zu erratende Wörter als Passwörter verwendet: Teile davon beinhalten oftmals das eigene Geburtsdatum, den Namen des Haustiers oder das Lieblingsreiseziel. Dies erleichtert Angreifern den Zugang zu Daten, da solche Passwörter oft bei Wörterbuchangriffen und Brute-Force-Methoden[3] zum Einsatz kommen.

Die 10 beliebtesten und unsichersten Passwörter des Jahres 2023 sind:[4]

1. 123456789
2. 12345678
3. hallo
4. 1234567890
5. 1234567
6. passwort
7. password1

Hasso Plattner Institut (2023, 19. Dezember).

Security.org (2023, 13. September).

„Brute-Force-Methoden" sind eine Art von Cyberangriff, bei dem ein Angreifer versucht, ein Passwort oder einen Schlüssel durch systematisches Ausprobieren jeder möglichen Kombination von Buchstaben, Zahlen und Symbolen zu erraten. Ziel ist es, Zugang zu einem verschlüsselten Konto, einer Datei oder einem Netzwerk zu erlangen. Dieser Ansatz ist im Wesentlichen ein Versuch-und-Irrtum-Verfahren, das keine Kenntnis des tatsächlichen Passworts oder Schlüssels voraussetzt. *(Definition generiert von ChatGPT-3)*

Hasso Plattner Institut (2023, 19. Dezember).

8. target123
9. iloveyou
10. qwerty123[5]

Ein weiteres Problem ist die Wiederverwendung von Passwörtern über verschiedene Konten hinweg. Aus Bequemlichkeit verwenden viele Menschen dasselbe Passwort für unterschiedliche Dienste, von sozialen Medien bis zu Bankkonten. Dieses Verhalten kann verheerende Folgen haben, wenn ein Passwort kompromittiert wird, da Angreifer dann potenziell Zugang zu mehreren Konten des Opfers erhalten können. Ein Bericht von Verizon[6] aus dem Jahr 2022 zeigt, dass eine erhebliche Anzahl von Datenschutzverletzungen auf die Wiederverwendung von Passwörtern zurückzuführen ist. Ein prominentes Beispiel hierfür ist der LinkedIn-Datenverstoß[7] aus dem Jahr 2016, bei dem Millionen von Passwörtern gestolzen wurden. Obendrein nachlässigen viele Nutzer die regelmäßige Aktualisierung ihrer Passwörter. Auch, wenn Dienste empfehlen, Passwörter regelmäßig zu ändern, ignorieren viele diese Hinweise, was sie langfristig potenziellen Sicherheitsrisiken aussetzt. Experten empfehlen daher, Passwörter regelmäßig zu ändern (mindestens einmal im Monat), insbesondere nach einer bekannt gewordenen Sicherheitsverletzung. Ein Paradebeispiel für nachlässiges Verhalten ist das Teilen von Passwörtern mit anderen. Dies geschieht oft in Arbeitsumgebungen, sozialen Kreisen oder selbst innerhalb von Familien, partnerschaftlichen Beziehungen und im Freundeskreis, um diesen Menschen den Zugang zu diversen Online- und Streaming-Diensten zu erleichtern.

Viele Menschen unterschätzen den Nutzen der Zwei-Faktor-Authentifizierung (2FA)[8] als zusätzliche Sicherheitsebene, da er ihnen zu umständlich und zeitaufwendig ist. Obwohl 2FA die Sicherheit von Online-Konten erheblich verbessern kann, zögern viele Nutzende, diese Funktion zu aktivieren. Die Konsequenzen der Nachlässigkeit im Umgang mit Passwörtern können gravierend

[5] Das Passwort „qwerty123" leitet sich von den ersten sechs Buchstaben der oberen Tastenreihe einer QWERTY-Computertastatur ab, gefolgt von einer einfachen, aufsteigenden Zahlenreihe.

[6] Verizon (2022).

[7] LinkedIn (2016) und Bundeskriminalamt (2020, 12. November).

[8] „Zwei-Faktor-Authentifizierung (2FA)" ist eine Sicherheitsmaßnahme, die einen zweiten Schritt zur Verifizierung der Identität eines Benutzers beim Zugriff auf ein Online-Konto oder System hinzufügt, zusätzlich zum herkömmlichen Benutzernamen und Passwort. Durch die Einführung einer zusätzlichen Authentifizierungsebene (gewöhnlicherweise die Zusendung eines sechsstelligen Zahlencodes per SMS oder E-Mail) wird es für unbefugte Personen wesentlich schwieriger, Zugang zu sensiblen Informationen oder Diensten zu erlangen, selbst, wenn sie das Passwort kennen. *(Definition generiert von ChatGPT-3)*

sein, von persönlichem Stress und Verlust der Privatsphäre hin zu finanziellen Schäden und Reputationsverlust für Unternehmen oder Schulen.

Das mangelnde Bewusstsein und Wissen über Passwortsicherheit ist ein grundlegendes Problem. Viele Menschen wissen schlichtweg nicht, wie man ein starkes Passwort erstellt und sicher verwaltet. Bildungsinitiativen und Informationskampagnen[9] sind entscheidend, um das Bewusstsein zu schärfen und Nutzer über die besten Praktiken für Passwortsicherheit zu informieren.

2. Die Rolle der Verschlüsselungstechnologie

Für Schulleitungen stellt sich die Herausforderung, ein sicheres digitales Umfeld zu schaffen, in dem die personenbezogenen Daten von Schülern, Lehrern und anderen Mitarbeitern geschützt sind. Die Rolle der Verschlüsselung in Schulen erstreckt sich von der Sicherung der Kommunikation bis zum Schutz sensibler Informationen und ist ein zentrales Element in der Strategie zur Abwehr von Cyberbedrohungen.

Verschlüsselungstechnologien ermöglichen die Umwandlung von Informationen oder Daten in einen Code, um unbefugten Zugriff zu verhindern. Diese Technologien sind besonders im Schulkontext von Bedeutung, wo neben der Sicherheit von personenbezogenen Daten auch die Integrität von Prüfungsmaterialien (z. B. Zentralabitur, DiVa-BK: Digitale Vorprüfung am Berufskolleg in Nordrhein-Westfalen) gewährleistet sein muss. Schulleitungen stehen vor der Aufgabe, die angemessene Implementierung von Verschlüsselungstechnologien zu überwachen und sicherzustellen, dass sowohl die Kommunikation als auch die gespeicherten Daten gegen Cyberangriffe geschützt sind.

Ein grundlegendes Beispiel[10] für die Anwendung von Verschlüsselung in der Schule ist die sichere Übermittlung von Noten und persönlichen Informationen zwischen Lehrkräften und der Schulverwaltung. Durch die Verwendung

[9] Vgl. Deutscher Bundestag – Ausschuss für Digitales (2023, 19. Januar) oder SoSafe (2023).
[10] Bildungsland NRW (2021, 14. Januar).

von Ende-zu-Ende-Verschlüsselung[11] können E-Mails und andere elektronische Kommunikationsformen so gesichert werden, dass nur der beabsichtigte Empfänger den Inhalt entschlüsseln und lesen kann. Diese Maßnahme schützt vor dem Abfangen sensibler Informationen durch Unbefugte, ein Szenario, das zu Datenschutzverletzungen und anderen Sicherheitsrisiken führen kann. Ferner spielt die Verschlüsselung eine entscheidende Rolle beim Schutz digitaler Lernmaterialien. Mit der zunehmenden Verbreitung von E-Learning und digitalen Ressourcen müssen Schulleitungen sicherstellen, dass auch diese Inhalte geschützt sind. Verschlüsselung kann verhindern, dass urheberrechtlich geschützte Lehrmaterialien illegal kopiert oder verändert werden. Zudem garantiert sie, dass Prüfungen und Tests sicher gespeichert und übertragen werden, wodurch die Integrität des Bewertungsprozesses gewahrt bleibt. Leider ist es heutzutage immer noch gang und gäbe, dass Prüfungsklausuren oder Notenlisten ohne Verschlüsselung per E-Mail innerhalb des Kollegiums versandt werden.

Ein weiterer wichtiger Aspekt ist der Schutz von digitalen Endgeräten und Netzwerken. Viele Schulen stellen Schülern und Lehrern Tablets, Laptops oder andere digitale Geräte zur Verfügung. Die Verschlüsselung dieser Endgeräte ist essenziell, um sicherzustellen, dass bei Verlust oder Diebstahl keine sensiblen Daten kompromittiert werden. Dies schließt auch die Verschlüsselung von Speichermedien ein, auf denen möglicherweise sensible Informationen gespeichert sind. Ebenso wichtig ist die Verschlüsselung des Datenverkehrs innerhalb des Schulnetzwerks, um die Datenübertragung vor potenziellen Lauschangriffen zu schützen. Für Schulleitungen besteht die Herausforderung darin, ein Gleichgewicht zwischen der Implementierung effektiver Sicherheitsmaßnahmen und der Gewährleistung einer benutzerfreundlichen Umgebung für Lernende und Lehrkräfte zu finden. Die Einführung von Verschlüsselungstechnologien erfordert eine sorgfältige Planung und Schulung aller Beteiligten, um sicherzustellen, dass diese korrekt angewendet werden und keine unnötigen Hindernisse für den Lehr- und Lernprozess schaffen. Als Folge

[11] „Ende-zu-Ende-Verschlüsselung" (E2EE) ist ein Verfahren, bei dem Nachrichten oder Daten so verschlüsselt werden, dass sie nur vom Sender und Empfänger gelesen werden können. Dies schützt die Daten vor dem Zugriff durch Dritte, einschließlich der Anbieter der Kommunikationsplattform. E2EE verwendet eine Form der „Public-Key-Verschlüsselung", die zwei Schlüssel verwendet: einen öffentlichen Schlüssel für die Verschlüsselung und einen privaten Schlüssel für die Entschlüsselung von Daten. Dies stellt sicher, dass nur der beabsichtigte Empfänger die Nachricht entschlüsseln und lesen kann. *(Definition generiert von ChatGPT-3)* Ein gelungenes Beispiel dafür war die bundesweite Energiepreispauschale für Studierende sowie Fachschüler" im Jahr 2023, die einen einmaligen Zuschuss für die gestiegenen Energiekosten in Höhe von 300 Euro brutto enthielt.
Vgl. Bundesregierung (2023, 4. Oktober).

davon ist ein wichtiger Faktor für den Erfolg von Verschlüsselungsinitiativen in Schulen die fortlaufende Bildung und Sensibilisierung. Schulleitungen müssen Lehrkräfte, Schüler und Eltern über die Bedeutung von Datenschutz und Cybersicherheit informieren und Anleitungen zur sicheren Nutzung digitaler Ressourcen bereitstellen. Dies schließt die Aufklärung über die Risiken von Phishing-Angriffen, die Bedeutung starker Passwörter und die Verwendung von Zwei-Faktor-Authentifizierung mit ein.

Die Implementierung einer robusten Verschlüsselungsstrategie in Schulen erfordert zudem die Zusammenarbeit mit IT-Experten, um sicherzustellen, dass die ausgewählten Verschlüsselungstechniken den neuesten Sicherheitsstandards entsprechen und gleichzeitig mit den bestehenden Systemen und Prozessen der Schule kompatibel sind. Die Auswahl der richtigen Verschlüsselungslösungen kann komplex sein, da sie von mehreren Faktoren abhängt, einschließlich der Art der zu schützenden Daten, den verwendeten Geräten und der vorhandenen IT-Infrastruktur. Ein Beispiel für eine Best-Practice-Implementierung von Verschlüsselung in Schulen könnte die Einführung verschlüsselter virtueller privater Netzwerke (VPNs)[12] sein, um die sichere Fernkommunikation und den Fernzugriff auf das Schulnetzwerk zu ermöglichen. Diese Maßnahme ist besonders relevant, da das Fernlernen und die Fernarbeit zunehmend an Bedeutung gewinnen. Durch die Einrichtung eines VPNs können Lehrkräfte und Schüler sicher auf interne Ressourcen zugreifen, ohne befürchten zu müssen, dass ihre Daten während der Übertragung abgefangen werden. Während der Coronapandemie empfahl sich die Verwendung von VPNs beim Lernen auf Distanz als vorbildliches datenschutzkonformes Vorgehen. Zusätzlich können Schulen verschlüsselte Cloud-Speicherdienste nutzen, um Lehrmaterialien und Schülerarbeiten sicher zu speichern und zu teilen. Die Wahl eines Cloud-Dienstes, der starke Verschlüsselungsstandards sowohl für die Speicherung

[12] Ein virtuelles privates Netzwerk (VPN)" ist eine Technologie, die die sichere Verbindung eines Geräts über ein öffentliches Netzwerk, wie das Internet, zu einem privaten Netzwerk einer Schule ermöglicht. Dabei wird die Verschlüsselung des Datenverkehrs zwischen dem Gerät des Nutzers und dem VPN-Server der Schule werden die Daten geschützt, sodass Unbefugte sie schwer einsehen oder abfangen können. Diese Sicherheitsmaßnahme ist besonders wichtig, wenn Schüler, Lehrer oder Verwaltungspersonal über unsichere Netzwerke, beispielsweise öffentliches WLAN, auf schulinterne digitale Ressourcen zugreifen.
VPNs werden in Bildungseinrichtungen genutzt, um Lehrkräften und Schülern den Fernzugriff auf das Schulnetzwerk zu ermöglichen. Dies erlaubt ihnen, von zu Hause oder anderen Standorten aus, als wären sie direkt in der Schule, auf Lernmaterialien und interne Informationen zuzugreifen. Darüber hinaus helfen VPNs, die Privatsphäre der Nutzer bei ihrer Online-Arbeit zu schützen und ermöglichen den Zugang zu Lehrmaterialien, die eventuell wegen geografischer Beschränkungen blockiert sind. *(Definition generiert von ChatGPT-3)*

als auch für die Übertragung von Daten auf einem Serverstandort innerhalb Deutschlands anbietet, ist entscheidend für den Schutz vor unbefugtem Zugriff und Datenlecks.

Die Implementierung und Verwaltung von Verschlüsselungstechnologien stellt Schulleitungen jedoch vor viele Herausforderungen. Dazu gehört die Notwendigkeit, sich kontinuierlich über Entwicklungen in der Verschlüsselungstechnologie zu informieren, die Sicherstellung der Kompatibilität mit bestehenden Technologien (z. B. digitales Lernplattformen wie Moodle) und die Überwindung möglicher Widerstände innerhalb der Schulgemeinschaft gegenüber neuen Systemen. Auch die Einführung neuer Sicherheitsmaßnahmen erfordert häufig eine Anfangsinvestition, sowohl in finanzieller Hinsicht als auch in Bezug auf Zeit und Ressourcen für die Schulung des Personals. Zur Unterstützung der Schulleitungen bei der Bewältigung dieser Herausforderungen könnten professionelle Entwicklungsprogramme und Partnerschaften mit Technologieanbietern von Nutzen sein. Diese können wertvolle Ressourcen und Expertise bieten, um sicherzustellen, dass Schulen die für ihre spezifischen Bedürfnisse am besten geeigneten Verschlüsselungslösungen auswählen und implementieren.

3. Wie sichere Passwörter die Privatsphäre schützen können

Die Schulleitung trägt bei der Gewährleistung der Datensicherheit, die durch die Implementierung und Aufrechterhaltung starker Passwortsicherheitsmaßnahmen erreicht werden kann, eine große Verantwortung. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat hierzu umfassende Richtlinien entwickelt, die als Grundlage für die Erstellung und Verwendung sicherer Passwörter dienen.[13] Diese Richtlinien sind nicht nur für den individuellen Schutz essenziell, sondern tragen auch dazu bei, eine robuste digitale Sicherheitskultur innerhalb der Schulgemeinschaft zu fördern.

Die Komplexität und Einzigartigkeit von Passwörtern spielen eine zentrale Rolle bei der Verhinderung unbefugten Zugriffs auf sensible Informationen.

Laut BSI sollten sichere Passwörter folgende Kriterien erfüllen:[14]

- Die Länge eines Passwortes sollte acht Zeichen nicht unterschreiten; denn: Ich ist länger immer besser.

[13] Bundesamt für Sicherheit in der Informationstechnik (BSI) (a) und (b).

[14] Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI) (a) und (b).

- Bei Anwendungen, die anfällig für Offline-Attacken sind, wie z. B. WPA2- oder WPA3-geschützte WLANs, sollte das Passwort idealerweise zwischen 20 und 25 Zeichen lang sein.
- Es ist möglich, eine breite Palette von Zeichen zu verwenden, einschließlich Groß- und Kleinbuchstaben, Zahlen und einer Vielzahl von Sonderzeichen.
- Die Kombination unterschiedlicher Zeichentypen, darunter Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen, trägt signifikant zur Passwortsicherheit bei.
- Auf den Gebrauch von Umlauten sollte verzichtet werden, da diese auf internationalen Tastaturen möglicherweise nicht verfügbar sind.
- Einfache Zahlenreihen oder die Hinzufügung gängiger Sonderzeichen an einem ansonsten einfachen Passwort reichen für eine sichere Passwortgestaltung nicht aus.
- Leicht erratbare persönliche Informationen, wie die Namen von Angehörigen, Geburtsdaten oder Ähnliches, sollten bei der Passworterstellung vermieden werden.

Diese Empfehlungen sind das Fundament für die Entwicklung von Passwörtern, die selbst durch ausgefeilte Brute-Force- oder Wörterbuchangriffe nur schwer zu entschlüsseln sind. Die Strategie, starke Passwörter zu generieren und sich zu merken, kann jedoch eine Herausforderung darstellen. Das BSI schlägt vor, kreative Methoden wie die Bildung von Passwörtern aus den ersten Buchstaben eines Satzes zu verwenden oder zufällig gewählte Wörter durch Leerzeichen getrennt zu nutzen, um sowohl Sicherheit als auch Merkbarkeit zu gewährleisten. Beispielsweise ergäbe jeden **A**bend **s**chaue **i**ch **m**ir **d**ie **v**ielen **S**terne **a**m **H**immel **a**n“ dieser ergäbe dann das Passwort: JAsimdv*aHa.[15]

Die Implementierung einer solchen Passwortpolitik in einem schulischen Umfeld erfordert eine proaktive Herangehensweise der Schulleitung. Es ist nicht nur wichtig, dass die Schulleitung selbst starke Passwörter verwendet, sondern auch, dass sie das Bewusstsein und die Bildung innerhalb der Schulgemeinschaft fördert. Überdies ist der Einsatz von Passwort-Managern eine effektive Strategie zur Verwaltung starker, einzigartiger Passwörter für multiple Konten. Passwort-Manager speichern Passwörter in einer verschlüsselten Datenbank, die durch ein einzelnes, starkes Masterpasswort geschützt ist. Diese Werkzeuge können nicht nur dazu beitragen, die Sicherheit zu erhöhen, indem sie die Verwendung einzigartiger Passwörter für jeden Account

[15] Beispiel entnommen aus: Arntz, Carsten; Kämper, Stephan (2021).

erleichtern, sondern auch die Benutzerfreundlichkeit verbessern, indem sie die Notwendigkeit eliminieren, sich zahlreiche komplexe Passwörter merken zu müssen. Die Einführung und Nutzung von Passwort-Managern erfordert jedoch eine sorgfältige Auswahl und Konfiguration, um sicherzustellen, dass die verwendeten Lösungen den höchsten Sicherheitsstandards entsprechen. Die Schulleitung muss daher in der Lage sein, fundierte Entscheidungen über die Auswahl von Passwort-Managern zu treffen, die sowohl eine starke Verschlüsselung bieten als auch eine benutzerfreundliche Oberfläche für Lehrer, Schüler und Verwaltungspersonal haben. Der Platzhirsch unter den Passwort-Managern, die Software 1Password, erlaubt z. B. maximal 100 Zeichen pro Passwort sowie die Einbindung von Zahlen und Zeichen. Als „starke Passwörter" werden jedoch innerhalb der Software bereits Kennwörter mit 13 Zeichen als sicher definiert.

Durch die Einhaltung der vom BSI empfohlenen Richtlinien für die Erstellung sicherer Passwörter und die Implementierung von Passwort-Managern können Schulleitungen einen signifikanten Beitrag zur Erstärkung der digitalen Sicherheit leisten. Dies erfordert ein fortlaufendes Engagement für die Sensibilisierung und Ausbildung der Schulgemeinschaft (inklusive des Sekretariats) bezüglich der Bedeutung von Passwortsicherheit sowie eine strategische Planung und Implementierung von Technologien, die die Verwaltung von Passwörtern vereinfachen und sicherer machen. **Die Schulleitung definiert die Datensicherheit innerhalb der Schule.** Die Schaffung einer starken Sicherheitskultur in Schulen erfordert nicht nur die Auswahl technologischer Lösungen, sondern auch die Förderung eines Bewusstseins, das über die Schule hinausgeht und Schüler auf ein Leben in einer digital vernetzten Welt vorbereitet. Die Schulleitung muss dabei eine Vorbildfunktion einnehmen und durch kontinuierliche Bildungsinitiativen und gegebenenfalls die Integration von Cybersicherheitsthemen den Lehrplan (z. B. im Fach Medienpädagogik) die Grundlage für eine nachhaltige digitale Sicherheit legen.

4. Erkennung und Vermeidung von Phishing-Angriffen

Heutzutage ist die Wahrung der Sicherheit und Privatsphäre von personenbezogenen Daten von essenzieller Bedeutung. Auch Bildungseinrichtungen greifen zunehmend auf digitale Plattformen und Ressourcen zu und sollten sich daher auch auf die Erkennung und Vermeidung von sogenannten Phishing-Angriffen konzentrieren. „Phishing" (engl. betrügerisches Entlocken sensibler Daten) ist eine weitverbreitete Methode, die von Cyberkriminellen eingesetzt wird, um sensible Informationen zu erlangen. Phishing, eine Technik, die da-

rauf abzielt, Individuen dazu zu verleiten, persönliche oder finanzielle Informationen preiszugeben, bedroht die Integrität und Vertraulichkeit von Daten in Bildungseinrichtungen. Es ist daher unerlässlich, Strategien zu entwickeln, die nicht nur die Erkennung solcher Versuche verbessern, sondern auch das Bewusstsein und die Widerstandsfähigkeit der Nutzer gegenüber diesen betrügerischen Praktiken stärken.

Phishing-Angriffe sind in ihrer Natur besonders hinterhältig, da sie häufig vertrauenswürdige Identitäten, wie die von Banken, Online-Versandhändlern, sozialen Netzwerken oder sogar Bildungseinrichtungen imitieren. Diese Angriffe können in verschiedenen Formen auftreten, einschließlich, aber nicht beschränkt auf E-Mail-Phishing, Spear-Phishing und Smishing, wobei jeder Typ spezifische Techniken verwendet, um an das gewünschte Ziel zu gelangen. Beispielsweise zielt E-Mail-Phishing auf breite Nutzergruppen ab (z. B. die bekannten Mails: „Lieber Freund, ich habe geerbt und verschenke 5 Millionen Dollar an Sie"), während Spear-Phishing spezifische Individuen oder Organisationen mit maßgeschneiderten Nachrichten angreift (z. B. Lehrkräfte mit derselben Schulemailkennung). Smishing nutzt SMS-Nachrichten als Vehikel für den Betrug (Beispiel: „Ihr Sparkonto wurde gesperrt! Bitte klicken Sie auf folgenden Link.").

Die Erkennung von Phishing-Versuchen erfordert ein tiefgehendes Verständnis der charakteristischen Merkmale solcher Angriffe. Oft enthalten Phishing-Nachrichten verdächtige Links, die zu gefälschten Webseiten führen oder sie fordern den Empfänger auf, persönliche Daten preiszugeben. Eine weitere verbreitete Taktik ist das Erzeugen eines Gefühls der Dringlichkeit oder Angst (z. B. die Meldung, dass das eigene Konto gehackt worden ist), um den Empfänger zu einer unüberlegten Handlung zu bewegen. Diese Merkmale sind Indikatoren, die Nutzer alarmieren sollten.

Um Phishing effektiv zu vermeiden, ist eine umfassende Strategie erforderlich, die Bildung und technologische Lösungen kombiniert. Auf der Bildungsseite ist es entscheidend, dass sowohl Lehrpersonal als auch Schüler über die Risiken und Kennzeichen von Phishing informiert werden. Auch hier können regelmäßige Schulungen und Sensibilisierungskampagnen das Bewusstsein schärfen und dazu beitragen, dass potenzielle Ziele skeptischer gegenüber verdächtigen Nachrichten werden. Es ist ebenso wichtig, klare Richtlinien für den Umgang mit potenziellen Phishing-Versuchen zu etablieren, wie die Nichtweitergabe persönlicher Informationen ohne vorherige Überprüfung und das sofortige Melden verdächtiger Aktivitäten an die zuständigen Stellen.

Technologische Lösungen spielen ebenfalls eine entscheidende Rolle bei der Prävention von Phishing. Fortschrittliche E-Mail-Filter, die in der Lage sind, Phishing-Versuche zu erkennen und zu blockieren, bevor sie den Nutzer erreichen, sind ein wesentliches Werkzeug. Zusätzlich können Web-Browser-Erweiterungen, die verdächtige Links und Webseiten identifizieren, eine weitere Sicherheitsebene hinzufügen. Die Implementierung von Multi-Faktor-Authentifizierung (MFA)[16] kann ebenfalls dazu beitragen, die Sicherheit zu erhöhen, indem sie eine zusätzliche Hürde für Angreifer darstellt, wenngleich sie in den Besitz von Anmeldedaten gelangen sollten.

Interaktive Schulungsmodule[17], die realistische Phishing-Szenarien simulieren, haben sich als besonders wirksam erwiesen. Durch die aktive Teilnahme an diesen Simulationen können Kollegen lernen, verdächtige E-Mails zu erkennen, ohne einem echten Risiko ausgesetzt zu sein. Feedback und Analyse nach jeder Simulationssession bieten wertvolle Einblicke in individuelle Stärken und Schwächen, was die Entwicklung gezielter Verbesserungsstrategien ermöglicht.

5. Schutz vor Malware und Ransomware

Malware- und Ransomware-Bedrohungen stellen ebenfalls eine erhebliche Herausforderung dar. Solche Schadsoftware kann verheerende Auswirkungen auf den Bildungssektor haben, indem sie den Zugang zu wichtigen digitalen Ressourcen blockiert, sensible Daten gefährdet oder den Lehrbetrieb erheblich stört. Daher ist es von großer Bedeutung, angemessene Sicherheitsmaßnahmen zu ergreifen und ein tiefgehendes Bewusstsein für diese Bedrohungen zu verbreiten, um die digitale Infrastruktur und Daten von Bildungseinrichtungen wirksam zu schützen.

„Malware" (engl. schädliche Software, Schadprogramm) umfasst Software, die darauf ausgelegt ist, einem Computersystem ohne Autorisierung Schaden zu-

[16] Die „Multi-Faktor-Authentifizierung (MFA)" stellt ein Sicherheitsverfahren dar, bei dem Benutzer aufgefordert werden, mehrere Bestätigungsschritte zu absolvieren, bevor sie Zugriff auf Online-Konten, Systeme oder Netzwerke erhalten. Diese Bestätigungsmethoden können aus verschiedenen Kategorien stammen, wie Kenntnisse des Benutzers (wie Passwörter oder PINs), im Besitz des Benutzers befindliche Gegenstände (wie ein Smartphone oder Sicherheitstoken) oder biometrische Merkmale des Benutzers (wie Fingerabdrücke). Der Kerngedanke der MFA liegt darin, die Sicherheit durch die Anforderung mehrfacher, voneinander unabhängiger Nachweise zu verstärken, wodurch es für Unbefugte deutlich erschwert wird, alle für den Zugriff notwendigen Informationen zu erlangen. *(Definition generiert von ChatGPT-3)*

[17] ODoherty, Conor (2024).

zufügen oder auf dieses zuzugreifen, einschließlich Computerviren, Würmern, Trojanern und Spyware. „Ransomware“ (engl. Erpressungsschadsoftware, Lösegeldsoftware) ist eine spezielle Form der Malware aus der Kryptovirologie, die damit droht, die Daten des Opfers zu veröffentlichen oder den Zugang dazu zu blockieren, es sei denn, ein Lösegeld wird gezahlt. Diese Art von Cyberangriff hat in den vergangenen Jahren rapide zugenommen und gilt nun als eine ernsthafte Bedrohung für Institutionen jeder Größe, einschließlich des Bildungssektors.

Ransomware-Angriffe finden in hoher Zahl statt (Schätzungen nach alle 11 Sekunden) und selbst Weltunternehmen sind davor nicht immer gefeit.[18] Der erste Schritt zum Schutz ist die Implementierung robuster Sicherheitssysteme, einschließlich aktualisierter Antivirensoftware und Firewalls, die bekannte Malware identifizieren und blockieren, bevor sie Schaden anrichten kann. Es muss jedoch verstanden werden, dass keine Sicherheitssoftware perfekten Schutz bietet. Cyberkriminelle entwickeln kontinuierlich neue Methoden, um Sicherheitsvorkehrungen zu umgehen, was die Notwendigkeit einer mehrschichtigen Sicherheitsstrategie unterstreicht. Ein solcher Ansatz sollte auch die systematische Datensicherung aller kritischen Daten umfassen. Backup-Lösungen, die Daten zu geplanten Zeitintervallen automatisch sichern, können im Falle eines Ransomware-Angriffs von entscheidender Bedeutung sein. Sie reduzieren die möglichen Folgen eines Angriffs, indem sie die Wiederherstellung der Systeme ohne Lösegeldzahlung ermöglichen. Backups sollten außerhalb des Hauptnetzwerks erstellt werden, damit sie nicht auf ähnliche Weise kompromittiert werden können.

Eine weitere Schlüsselkomponente im Kampf gegen Malware und Ransomware ist die Durchsetzung von Zugriffsrechten und die Reduzierung von Privilegien. Der Grundsatz des geringstmöglichen Privilegs, bei dem Nutzern nur die minimal notwendigen Rechte für ihre Aufgaben zugewiesen werden, spielt dabei eine zentrale Rolle. Es ist außerdem von äußerster Wichtigkeit, regelmäßige Software- und Betriebssystemupdates durchzuführen, um Sicherheitslücken zu schließen, die von Malware ausgenutzt werden könnten. Hersteller veröffentlichen regelmäßig Patches und Updates, um bekannte Sicherheitsschwachstellen zu beheben. Ein Versäumnis bei der Installation dieser Updates öffnet Angreifern Tür und Tor.

[18] Kaspersky (2021).

Trotz aller Vorsichtsmaßnahmen kann es dennoch zu einer Infektion kommen. In solchen Fällen ist eine schnelle und koordinierte Reaktion entscheidend, um den Schaden zu begrenzen und die Wiederherstellung zu beschleunigen. Dies erfordert einen vorab entwickelten Incident-Response-Plan[19] mit klaren Richtlinien für das Vorgehen im Falle einer Infektion. Ein solcher Plan sollte die Identifizierung und Isolierung betroffener Systeme, die Benachrichtigung relevanter Stakeholder und die Schritte zur Wiederherstellung der Systeme umfassen.

6. Einhaltung von Datenschutz- und Compliance-Anforderungen in der Schulleitung am Beispiel der Stellenplanung

Die Einhaltung von Compliance-Anforderungen in der Schulleitung, insbesondere im Bereich der Stellenplanung, wo persönliche und arbeitsvertragliche Daten verarbeitet werden, ist eine komplexe Herausforderung, die eine gründliche Berücksichtigung gesetzlicher und organisatorischer Aspekte erfordert. In diesem Kontext spielen sowohl das Verständnis der grundlegenden Prinzipien von Compliance und Datenschutz[20] als auch deren praktische Umsetzung eine zentrale Rolle. „Compliance" (*engl.* Regelbefolgung, Regelkonformität) bezieht sich auf die Einhaltung von Gesetzen, Richtlinien und ethischen Standards durch Unternehmen und ihre Mitarbeiter. Es umfasst eine Vielzahl von Bereichen, einschließlich des sozialen Umgangs, der Fairness, der internen Kommunikation und der Fehlerkultur. Ebenso ist die Berücksichtigung der Interessen verschiedener Interessengruppen (Schulaufsicht, Schulträger, Eltern, Kooperationspartner) von Bedeutung. Die gesetzliche Grundlage für die Compliance in Deutschland wird durch eine Reihe von Gesetzen und Verordnungen gebildet.[21]

---

[19] Ein „Incident-Response-Plan" (engl. Plan zur Reaktion auf Sicherheitszwischenfälle) ist eine systematische Anleitung, die Organisationen darauf vorbereitet, auf Vorfälle wie Cyberattacken, Datenverlust oder andere sicherheitsrelevante Ereignisse effizient zu reagieren. Dieses Dokument definiert spezifische Abläufe und Verantwortlichkeiten, um im Falle einer Sicherheitsbedrohung schnell handeln zu können. Das Hauptziel besteht darin, die Auswirkungen solcher Vorfälle zu begrenzen, die Sicherheit und Funktionalität betroffener Systeme rasch wiederherzustellen und durch gründliche Analyse präventive Maßnahmen für die Zukunft zu entwickeln. Bei Schulen sollte dieser Incident-Response-Plan immer mit dem zuständigen Datenschutzbeauftragten abgesprochen sein. *(Definition generiert von ChatGPT-3)*

[20] Consulting Check (2024).

[21] Vgl. Das Aktiengesetz (AktG), das Gesetz betreffend die Gesellschaften mit beschränkter Haftung (GmbH-Gesetz) und spezifische Regelungen zum Beispiel im Bereich der Korruptionsbekämpfung.

Ein wesentlicher Bestandteil der Compliance in der Schulleitung ist der Schutz personenbezogener Daten, der durch die Datenschutz-Grundverordnung (DSGVO) und das Bundesdatenschutzgesetz (BDSG) geregelt wird. Die Dokumentation und der Nachweis der Einhaltung dieser Vorschriften sind für Schulen ebenso verpflichtend wie für Unternehmen. Dies beinhaltet die Erstellung von Datenschutzrichtlinien, die Schulung der Mitarbeiter im Bereich Datenschutz und die Aufbewahrung von Aufzeichnungen über die Verarbeitung personenbezogener Daten. Ein Schulleiter kann die Einhaltung von Compliance-Anforderungen bei der Stellenplanung (bspw. der Name, Geburtsdaten, Vergütung gemäß dem Arbeitsvertrag sowie interne Bemerkungen wie Renteneintritt, Gesundheitsdaten usw. eine Rolle spielen) durch eine Kombination aus strategischer Planung, Einsatz moderner Technologien und einer klaren Organisationsstruktur sicherstellen. Grundlegend für den Prozess ist das Verständnis der Bedeutung von Compliance im Zusammenhang mit Verträgen und Personalmanagement sowie die Anwendung bewährter Verfahren zur Gewährleistung der Einhaltung gesetzlicher und ethischer Standards.

Zunächst ist es wichtig, die Vertragsverwaltung als integralen Bestandteil der Risikomanagementstrategie der Schule zu betrachten. Dies beinhaltet die regelmäßige Überprüfung bestehender Verträge, die Überwachung der Einhaltung von Vertragsklauseln und das Führen von Protokollen. Bei der Stellenplanung sollte der Schulleiter sowohl quantitative als auch qualitative Aspekte berücksichtigen. Dies umfasst die Berechnung der benötigten Mitarbeiteranzahl unter Berücksichtigung von Faktoren wie persönlichen Daten, Pensionierungen, Fluktuation und Ausfallstatistiken durch Krankheit. Gleichzeitig ist es entscheidend, die erforderlichen Qualifikationen für bestimmte Stellen zu definieren und Weiterbildungsmöglichkeiten zu planen, um die Fähigkeiten und Kompetenzen des Personals zu erweitern.

Der Einsatz einer HR-Software[22] würde erheblich zur Effizienz der Personalplanung beitragen, indem diese Daten generiert und aufbereitet, die für die Entscheidungsfindung notwendig sind. Da jedoch die meisten Schulleitungen ihre Stellenplanung – aufgrund des Mangels an einer bundesweiten einheitlichen Lösung für eine entsprechende datenschutzkonforme Software – mit

[22] HR-Software steht für „Human Resource Software" und bezieht sich auf ein System oder eine Reihe von Systemen, die zur Verwaltung menschlicher Ressourcen und verwandter Prozesse innerhalb einer Organisation eingesetzt werden. Diese Art von Software hilft Unternehmen, ihre Personalaktivitäten und -prozesse zu automatisieren, effizienter und vor allem datenschutzkonform zu gestalten und zu optimieren. *(Definition generiert von ChatGPT-3)*

simplen Excel-Dateien verarbeiten, wäre hier zumindest die Anwendung einer datenschutzsicheren Verschlüsselung sinnvoll. Und damit ist nicht die leicht zu knackende Passwortfunktion innerhalb von Excel gemeint, sondern ei externe Verschlüsselung als ZIP-Datei auf einem zusätzlich gesicherten Server innerhalb der Schule. Für die praktische Umsetzung bedeutet dies, dass die Schulleitung klare Compliance-Ziele und -Werte festlegt, eine dedizierte Compliance-Organisation einrichtet (= eine jährliche Belehrung in der ersten Lehrerkonferenz im Schuljahr und alle fünf Jahre wiederkehrende Schulungen des Kollegiums durch externe Datenschutzexperten) und Audits des Datenschutzbeauftragten durchführen lassen sollte, um die Einhaltung von Compliance-Anforderungen an der Schule zu gewährleisten und um Fehlverhalten vorzubeugen. Durch die **Schaffung einer Kultur der Integrität und Transparenz** kann die Schulleitung nicht nur rechtliche Risiken minimieren, sondern auch im Vorhinein etwaigen Anwendungsfehlern oder Fehlverhalten vonseiten des Kollegiums vorbeugen.

Die Einhaltung von Compliance-Anforderungen und Datenschutzbestimmungen in der Schulleitung ist somit kein einmaliges Projekt, sondern ein kontinuierlicher Prozess, der eine dauerhafte Aufmerksamkeit und Anpassungsfähigkeit erfordert. Die erfolgreiche Umsetzung dieser Prinzipien trägt nicht nur zur Erfüllung rechtlicher Verpflichtungen bei, sondern stärkt auch die Integrität und das Vertrauen in die Schulführung und fördert eine positive und ethisch fundierte Schulgemeinschaft.

WICHTIG: Strategien zur Einhaltung von Compliance-Anforderungen

- **Transparenz und Aufklärung:** Die Grundlage für eine rechtskonforme Datenverarbeitung ist Transparenz. Bewerber und Mitarbeiter müssen darüber informiert werden, welche ihrer Daten erhoben werden, zu welchem Zweck und aufgrund welcher rechtlichen Grundlage. Eine klare Datenschutzerklärung ist hier unerlässlich.
- **Datenminimierung und Zweckbindung:** Es dürfen nur diejenigen personenbezogenen Daten erhoben und verarbeitet werden, für einen konkreten Zweck (z. B. die Stellenplanung) erforderlich sind. Alle Datenverarbeitungsprozesse sollten regelmäßig daraufhin überprüft werden, ob sie dem Prinzip der Datenminimierung entsprechen.
- **Sicherheitsmaßnahmen:** Um den Schutz der verarbeiteten Daten zu gewährleisten, müssen technische und organisatorische Sicherheitsmaßnahmen getroffen werden. Dazu zählen insbesondere die Verschlüsselung der Daten, der Zugriffsschutz sowie regelmäßige Schulungen der Schulleitungen (und auch des Sekretariats) zum Umgang mit sensiblen Daten.
- **Verfahren bei Datenpannen:** Trotz aller Vorsichtsmaßnahmen kann es zu Datenpannen kommen. Ein definierter Prozess für den Umgang mit solchen Vorfällen ist daher unerlässlich. Dies umfasst die sofortige Benachrichtigung der zuständigen Datenschutzbehörden, dem Datenschutzbeauftragten sowie der betroffenen Personen.
- **Dokumentation und Nachweisführung:** Schulen müssen nachweisen können, dass die Datenverarbeitung im Einklang mit den geltenden Datenschutzvorschriften erfolgt. Eine akkurate Dokumentation aller Datenverarbeitungsaktivitäten ist daher unerlässlich.

Cloud-Sicherheit

Als Schulleitung steht man vor der Herausforderung, den Spagat zwischen technologischer Innovation und der Gewährleistung von Datensicherheit und Datenschutz zu meistern. Die Einführung und Nutzung von Cloud-Diensten in der Bildungslandschaft hat das Potenzial, Lehr- und Lernprozesse zu revolutionieren. Sie bietet Lehrkräften und Schülern Zugang zu einer Vielzahl von Ressourcen und Kollaborationswerkzeugen, die den Unterricht bereichern und individualisiertes Lernen fördern können. Doch mit der Verlagerung schuli-

scher Daten und Prozesse in die Cloud gehen auch berechtigte Bedenken hinsichtlich Sicherheit und Datenschutz einher. Es gilt daher, die Risiken sorgfältig gegen die Vorteile abzuwägen und beste Lösungen für sicheres Cloud-Computing zu etablieren.

Einer der größten Vorteile der Cloud-Nutzung ist die Möglichkeit, Bildungsressourcen und -werkzeuge auf flexible und skalierbare Weise bereitzustellen. Dies ermöglicht es Schulen, auf ein breites Spektrum an Anwendungen und Diensten zuzugreifen, ohne in kostspielige Hardware investieren zu müssen. Lehrkräfte können somit dynamische und interaktive Lernerfahrungen schaffen, die auf die individuellen Bedürfnisse der Schüler zugeschnitten sind. Zudem erleichtert der Cloud-Zugriff die Hausaufgaben- und Projektarbeit, indem Schüler von zu Hause aus auf die benötigten Materialien zugreifen können. Ein weiterer Vorteil ist die Verbesserung der Kollaboration. Cloud-basierte Plattformen ermöglichen es Schülern und Lehrern, in Echtzeit (z. B. an Dokumenten) zusammenzuarbeiten, unabhängig von ihrem physischen Standort. Dies fördert eine inklusive Lernumgebung, in der Ideen frei geteilt und gemeinsam an Projekten gearbeitet werden kann. Darüber hinaus können Schuladministratoren von der Effizienzsteigerung profitieren, die Cloud-Dienste bieten, indem sie administrative Prozesse automatisieren und somit mehr Zeit für pädagogische Aufgaben einsetzen. Dennoch darf auch die Sicherheit bei der Einführung von Cloud-Diensten nicht vernachlässigt werden. Die Risiken umfassen unter anderem den potenziellen Verlust der Kontrolle über schulische Daten, die Gefahr von Datenlecks und die Einhaltung gesetzlicher Datenschutzvorschriften. Es ist von entscheidender Bedeutung, dass Schulen mit Cloud-Anbietern zusammenarbeiten, die robuste Sicherheitsmaßnahmen anbieten und deren Dienste die Einhaltung der Datenschutz-Grundverordnung (DSGVO) gewährleisten.

Um ein hohes Maß an Sicherheit zu erreichen, sollten Schulen bewährte Praktiken für sicheres Cloud-Computing befolgen. Dazu gehört die sorgfältige Auswahl von in Deutschland ansässigen Cloud-Anbietern, die nicht nur starke Datenschutz- und Sicherheitsprotokolle anbieten, sondern auch Erfahrung im Bildungsbereich haben. Ein transparenter und offener Dialog mit dem Anbieter über Sicherheitsmaßnahmen und Datenschutzrichtlinien ist essenziell. Die Implementierung von Zugriffsrechten und die Schulung von Lehrkräften, Schülern und Eltern in Bezug auf sichere Online-Praktiken sind weitere wichtige Schritte. Lehrkräfte und Schüler sollten über die potenziellen Risiken der Cloud-Nutzung informiert werden und lernen, wie sie Phishing-Angriffe erkennen und vermeiden können. Zudem ist es ratsam, regelmäßige Backups

schulischer Daten durchzuführen, um im Falle eines Datenverlusts oder eines Sicherheitsvorfalls vorbereitet zu sein. Die Auswahl solcher dedizierter Bildungsplattformen, die regelmäßig auf Sicherheitslücken überprüft und aktualisiert werden, minimiert das Risiko von Cyberangriffen und Datenlecks.

Als Schulleitung ist es eine Pflicht, eine sichere digitale Lernumgebung zu schaffen, die die Vorteile der Cloud-Technologie maximiert, während gleichzeitig die Privatsphäre und Sicherheit unserer Schüler und Lehrkräfte geschützt werden. Dies erfordert eine kontinuierliche Bewertung und Anpassung unserer Sicherheitspraktiken, die Zusammenarbeit mit vertrauenswürdigen Cloud-Anbietern und die Förderung eines bewussten Umgangs mit digitalen Ressourcen innerhalb unserer Schulgemeinschaft. Durch die Umsetzung dieser Vorgehensweisen kann die digitale Transformation im Bildungswesen sicher und verantwortungsvoll vorangetrieben werden.

8. Zukünftige Trends in der Cybersicherheit mit Künstlicher Intelligenz

Im Zuge der Digitalisierung des Bildungsbereiches und der Verwaltung von Schulen gewinnen Trends in der Cybersicherheit, insbesondere die Integration von Künstlicher Intelligenz (KI), zunehmend an Bedeutung. Als Schulleitungen steht man vor der Herausforderung, Schulen nicht nur mit modernsten technologischen Werkzeugen auszustatten, sondern auch sicherzustellen, dass die Daten der Schüler und Lehrkräfte geschützt sind. Die neuesten Trends in der Cybersicherheit mit KI bieten sowohl Chancen als auch Herausforderungen für Schulen.

Einer der wichtigsten Trends für 2024 ist der Einsatz von Generativer KI (GenAI[23]), der die Cyber-Sicherheitslandschaft signifikant verändert. GenAI ermöglicht, Sicherheitsoperationen zu verstärken und gleichzeitig Herausforderungen in der Verwaltung zu bewältigen. Sicherheitsexperten sind so-

[23] „Generative Künstliche Intelligenz (GenAI)" bezeichnet einen Bereich der KI-Technologien, der darauf spezialisiert ist, Daten zu generieren, die denen ähneln, auf denen sie trainiert wurden. Diese Technologie kann beispielsweise neue Bilder, Texte, Musik oder Sprachausgaben erzeugen, die nicht ohne weiteres von Menschen geschaffenen Werken zu unterscheiden sind. GenAI-Systeme, wie GPT (Generative Pre-trained Transformer) für Texte oder verschiedene Modelle für bildgenerierende Aufgaben, lernen aus großen Datenmengen und können kreativen oder neuen Inhalt erstellen, der spezifische Anforderungen oder Vorgaben erfüllt. Der Einsatz von generativer KI reicht von der Erstellung personalisierter Inhalte über die Generierung künstlerischer Werke bis hin zu Anwendungen in der Forschung und Entwicklung, wo sie beispielsweise neue Moleküle für Medikamente designen kann. *(Definition generiert von ChatGPT-3)*

wohl von den Potenzialen als auch von den Schwierigkeiten, die GenAI mit sich bringt, in Anspruch genommen. Die Entwicklungen in der Generativen KI, wie beispielsweise große Sprachmodelle à la ChatGPT, zeigen bereits vielversprechende Anwendungen in der Sicherheitsüberwachung und bei der Anwendungssicherheit. Es wird jedoch darauf hingewiesen, dass sich die Gesellschaft noch am Anfang dieser Entwicklung befindet und kurzfristig eher mit Herausforderungen als mit signifikanten Produktivitätssteigerungen zu rechnen sollten.[24]

Die Demokratisierung der KI ist ein wichtiger Schlüsselbereich, der Schulen betrifft. Mit der Bereitstellung von leicht zugänglichen KI-Plattformen wird es auch für Schulen einfacher, KI-basierte Lösungen zu implementieren. Dies erfordert jedoch eine Anpassung der Strategien und Prozesse und einen kulturellen Wandel innerhalb der Institution. Die Vorteile liegen in der Skalierung vorhandener Ressourcen, was die betrieblichen Strategien und Entscheidungsprozesse erheblich verbessern kann.[25]

Die Fortschritte in der KI-Regulierung sind ebenfalls von Bedeutung für Schulen, insbesondere im Hinblick auf den Schutz personenbezogener Daten. Die Regulierungen werden sich mit der Reife und Verbreitung der KI weiterentwickeln, wobei ein Schwerpunkt auf Datenschutzbestimmungen wird, um wachsenden Bedenken hinsichtlich Datenschutz und Datennutzung Rechnung zu tragen. Dies wird für Schulen besonders relevant sein, da sie große Mengen an persönlichen Informationen von Schülern verarbeiten.[26]

Als Schulleitung muss man bereit sein, diese Trends anzunehmen und gleichzeitig die Sicherheit der eigenen Bildungsinstitution zu gewährleisten. Die Integration von KI in die Cybersicherheit bietet großartige Möglichkeiten, Schulen sicherer und effizienter zu gestalten, erfordert jedoch eine sorgfältige Planung und Implementierung sowie eine kontinuierliche Überprüfung und Anpassung der Sicherheitsstrategien.

[24] [illegible] Inc. (2024, 22 Februar).
[25] Cardoso, Tiago/Digitale Welt (2023, 18. Dezember).
[26] Hillemann, Dennis/Fieldfisher (2024, 08. Januar).

Zukünftige Trends von Schulen, die Künstliche Intelligenz (KI) und Cybersicherheit nutzen

- **Automatisierte Erkennung und Abwehr von Cyberbedrohungen:** KI-gesteuerte Cloud-Netzwerklösungen und Netzwerkhardware können dazu beitragen, Anomalien im Netzwerkverkehr von Schulen zu erkennen, die auf mögliche Cyberangriffe hinweisen. Diese Systeme lernen aus vergangenen Sicherheitsvorfällen und können proaktiv ungewöhnliche Aktivitäten identifizieren, um Bedrohungen wie Malware oder Phishing-Angriffe automatisch zu blockieren, bevor sie Schaden anrichten.
- **KI-gestützte Netzwerksicherheit:** Mit der zunehmenden Vernetzung von Schulsystemen und Geräten könnte KI dazu beitragen, Netzwerksicherheitslösungen zu entwickeln, die dynamisch auf Veränderungen reagieren und sich an neue Bedrohungen anpassen, um die Integrität schulischer Netzwerke zu schützen.
- **Verbesserung der Privatsphäre und des Datenschutzes:** KI kann dabei helfen, Datenschutzverletzungen zu verhindern, indem sie sicherstellt, dass personenbezogene Daten von Schülern und Lehrkräften verschlüsselt und sicher gespeichert werden. KI-Technologien könnten entwickelt werden, um Datenschutzrichtlinien automatisch durchzusetzen und Compliance zu gewährleisten.
- **Personalisierte Lernerfahrungen unter Wahrung der Sicherheit:** Durch den Einsatz von KI in Lernplattformen könnten personalisierte Lerninhalte bereitgestellt werden, während gleichzeitig die Sicherheit dieser Plattformen gewährleistet wird. KI könnte beispielsweise dazu beitragen, maßgeschneiderte Lernpfade zu erstellen, die auf den individuellen Fortschritt und die Vorlieben der Schüler abgestimmt sind, und gleichzeitig sicherstellen, dass diese Interaktionen geschützt sind.
- **Intelligente Überwachung des Online-Verhaltens von Schülern:** KI-Systeme könnten das Online-Verhalten von Schülern überwachen, um unangemessene Inhalte zu erkennen oder Cybermobbing frühzeitig zu identifizieren. Diese Systeme könnten Lehrkräften und Schulverwaltungen helfen, präventiv zu handeln und unterstützende Maßnahmen zu ergreifen.

Literatur

- **Arntz, Carsten; Kämper, Stephan (2021).** Die digitale Schulleitung und das papierlose Büro: Strategien und Praxisbeispiele für das papierlose Büro, Hamburg: Tredition, S. 128.
- **Bildungsland NRW (2021, 14. Januar).** DiVa-BK (Digitale Vorprüfung am Berufskolleg) startet in die Erprobungsphase. https://www.schulministerium.nrw/diva-bk-digitale-vorpruefung-am-berufskolleg-startet-die-erprobungsphase
- **Bundesamt für Sicherheit in der Informationstechnik (BSI) (a).** BSI-Basisschutz: Sicherheit Passwörter (Faktenblatt). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Checklisten/sichere_passwoerter_faktenblatt.pdf?__blob=publicationFile&v=4#download=1
- **Bundesamt für Sicherheit in der Informationstechnik (BSI) (b).** Sichere Passwörter erstellen. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html
- **Bundeskriminalamt (2020, 12. November),** LinkedIn-Datenschutzfolgenabschätzung gem. Art. 35 Abs. 1 der Europäischen Datenschutzgrundverordnung (DSGVO). https://www.bka.de/SharedDocs/Downloads/DE/Service/Datenschutz/LinkedIn/datenschutzfolgenabschaetzung.pdf?__blob=publicationFile&v=4
- **Bundesregierung (2023, 4. Oktober),** Energiekosten: Zuschuss von bis zu 300 Euro. https://www.bundesregierung.de/breg-de/schwerpunkte/entlastung-fuer-deutschland/energiepreispauschale-2124992
- **Cardoso, Tiago/Digitale Welt (2023, 18. Dezember),** Künstliche Intelligenz: 6 Trends und Entwicklungen in 2024. https://digitaleweltmagazin.de/kuenstliche-intelligenz-6-trends-und-entwicklungen-in-2024
- **Consulting Check (2024).** Compliance: Definition, Gesetze, Sicherstellung. https://www.consultingcheck.com/de/topics/compliance-sicherstellen-so-halten-sie-die-gesetze-ein/19336
- **Deutscher Bundestag – Ausschuss für Digitales (2023, 19. Januar).** Stellungnahme von Julia Schuetze, Projektleiterin im Bereich Cybersicherheitspolitik und Resilienz bei der Stiftung Neue Verantwortung e.V., für die öffentliche Anhörung des Ausschusses für Digitales zum Thema „Cybersicherheit – Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland". https://www.bundestag.de/resource/blob/929986/a83f11806d0c6b47cead2437e2b35b4f/Stellungnahme-Schuetze-data.pdf

- **Gartner, Inc. (2024, 22 Februar).** Gartner Identifies the Top Cybersecurity Trends for 2024. https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024
- **Hasso Plattner Institut (2023, 19. Dezember).** 123456789 ist das beliebteste Passwort 2023 in Deutschland: Das HPI hat wieder die Top Ten der meist geleakten Passwörter ausgewertet. https://hpi.de/news/jahrgaenge/2023/123456789-ist-das-beliebteste-passwort-2023-in-deutschland.html
- **Hillemann, Dennis/Fieldfisher (2024, 08. Januar).** Die Nutzung von KI im öffentlichen Sektor – 10 Prognosen für 2024, 08.01.2024. https://www.fieldfisher.com/de-de/insights/die-nutzung-von-ki-im-oeffentlichen-sektor
- **Kaspersky (2021).** Die größten Ransomware-Angriffe 2020. https://www.kaspersky.de/resource-center/threats/top-ransomware-2020
- **LinkedIn (2016).** Benachrichtigung über Datenschutzverletzung. https://www.linkedin.com/help/lms/answer/a338522/notificare-privind-bresa-de-date-mai-2016?lang=de-DE
- **ODoherty, Conor (2024).** Bewährte Praktiken für Phishing-Simulation. https://www.metacompliance.com/de/blog/cyber-security-awareness/phishing-simulation-best-practices
- **Security.org (2023, 13. September).** Password Manager Industry Report and Market Outlook (2023-2024). https://www.security.org/digital-safety/password-manager-annual-report
- **SoSafe (2023).** Stärken Sie Ihre Sicherheitskultur. https://sosafe-awareness.com/de/?gad_source=1*11aikhj*_up*MQ..&gclid=EAIaIQobChMI2ZC4ueCohQMVLkRBAx1F8AQ...YASAAEgIJZvD_BwE
- **Verizon (2022).** Data Breach Investigations Report 2008–2022. https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf

[Letzte Abrufe: 01.05.2024]

Weiterführende Literatur

- **Arntz, Carsten (2023).** Die agile Schulleitung: Inspirierend führen in unsicheren Zeiten, Ahrensburg: Tredition.
- **Arntz, Carsten; Kämper, Stephan (2022).** Digitales Schulmanagement: Schule professionell leiten und verwalten, Stuttgart: Dr. Josef Raabe Verlag.
- **Arntz, Carsten; Kämper, Stephan (2023).** ChatGPT – Wie künstliche Intelligenz den Arbeitsalltag von Schulleitungen revolutioniert. In: Schulleitung und Schulentwicklung, Ausgabe 4/2023, Stuttgart: Dr. Josef Raabe Verlag.

RAAbits Online
@RAABE

Mehr Materialien für Ihren Unterricht mit RAAbits Online

Unterricht abwechslungsreicher, aktueller sowie nach Lehrplan gestalten – und dabei Zeit sparen.
Fertig ausgearbeitet für über 20 verschiedene Fächer, von der Grundschule bis zum Abitur: Mit RAAbits Online stehen redaktionell geprüfte, hochwertige Materialien zur Verfügung, die sofort einsetz- und editierbar sind.

- Zugriff auf bis zu **400 Unterrichtseinheiten** pro Fach
- Didaktisch-methodisch und **fachlich geprüfte Unterrichtseinheiten**
- Materialien als **PDF oder Word** herunterladen und individuell anpassen
- Interaktive und multimediale Lerneinheiten
- Fortlaufend **neues Material** zu aktuellen Themen

Testen Sie RAAbits Online 14 Tage lang kostenlos!
www.raabits.de

RAAbits Online – Das Portal für Unterrichtsmaterialien und Schulorganisation