



WHITEPAPER

Digitalpakt 2.0: Die digitale Schule sicher gestalten

Wie Schulen und Schulträger Cyberrisiken begrenzen
und ihre IT nachhaltig schützen können.

Erstellt in Zusammenarbeit mit Rechtsanwalt
Dr. Andreas Daum von Noerr Partnerschaftsgesellschaft mbB

Mit dem Digitalpakt 2.0 stehen bis 2030 fünf Milliarden Euro für die digitale Weiterentwicklung der Schulen bereit. Damit eröffnet sich die Chance, IT-Sicherheit von Beginn an in Planung, Umsetzung und Betrieb einzubeziehen. Denn mit Cloud-Diensten, Lernplattformen, KI-Anwendungen und einer wachsenden Zahl vernetzter Geräte wächst auch die Angriffsfläche.

Wie es um die Cybersicherheit an deutschen Schulen tatsächlich steht, zeigt eine aktuelle Sophos-Befragung* unter 200 Verantwortlichen: Viele Einrichtungen bewerten ihren Sicherheitsstand positiv, zugleich berichten 78 Prozent von mindestens einer konkreten Bedrohung oder einem Sicherheitsvorfall innerhalb eines Jahres. Phishing steht dabei an erster Stelle. Fehlende Ressourcen, Fachkräfte und klare Strukturen erschweren einen dauerhaft wirksamen Schutz.

Dieses Whitepaper ordnet ein, was der Digitalpakt 2.0 an Fördermöglichkeiten bietet, benennt die rechtlichen Pflichten und aktuellen Risiken und zeigt an Praxisbeispielen und gängigen Angriffsszenarien, wie Schulen und Schulträger ihre IT-Sicherheit zukunftsfähig aufstellen können. Im Mittelpunkt: integrierte Sicherheitsansätze, die Verantwortliche entlasten und einen verlässlichen digitalen Schulbetrieb ermöglichen.

*Zur Befragung:

Im Auftrag von Sophos führte techconsult im Juli 2026 die Online-Befragung "Cybersicherheit an deutschen Schulen" unter 200 Verantwortlichen aus Schulen, Schulträgern und schulnahen Verwaltungen in Deutschland durch. Berücksichtigt wurden unterschiedliche Schulformen, Träger und Größenklassen.



Digitalpakt 2.0: Digitalisierung sicher gestalten

Was das Förderprogramm für Schulen und Schulträger bedeutet

Die Digitalisierung hat den Schulalltag grundlegend verändert. Das betrifft den Unterricht ebenso wie die technische Ausstattung und die Organisation. Der Digitalpakt 2.0 baut auf seinem Vorgänger auf und fördert die digitale Entwicklung der Schulen. Bund und Länder stellen dafür bis 2030 gemeinsam fünf Milliarden Euro bereit. Gefördert werden der Ausbau der digitalen Ausstattung, die Qualifizierung von Lehrkräften für digitale Medien, moderne Lehrmethoden sowie der IT-Betrieb und dessen Sicherheit.

IT-Sicherheit kann gefördert werden

Eine verlässlich funktionierende digitale Schul-Infrastruktur braucht angemessenen Schutz. IT-Sicherheit sollte deshalb bereits bei der Planung neuer Systeme berücksichtigt werden. Das betrifft jedes Netzwerk, jeden Server, jeden Computer, jedes netzwerkfähige Gerät, jede Software und jeden Cloud-Dienst.

Welche Maßnahmen und Leistungen im Einzelnen förderfähig sind, regeln die Vereinbarungsdokumente und die Förderprogramme der Länder. Je nach Förderprogramm können dazu auch Softwarelizenzen, Administration und Leistungen für den laufenden Betrieb gehören. Zudem sieht die Verwaltungsvereinbarung zwischen Bund und Ländern zu Fördergegenständen und Förderbedingungen unter dem Digitalpakt Schule 2.0 unter § 2 Abs. 4 Nr. 3 lit. a) vor, dass auch „befristete Ausgaben in unmittelbarer Verbindung mit Investitionsmaßnahmen für den Auf- und Ausbau von Strukturen für die professionelle Administration der digitalen Infrastrukturen und den professionellen Support“ förderfähig sind. Die Fußnote 1 zu dieser Regelung konkretisiert darüber hinaus, dass dies auch „Sachmittel für die Beauftragung externer Dienstleister in direkter Verbindung mit Investitionsmaßnahmen“ beinhaltet.

IT-Sicherheit von Anfang an einplanen

Mit der zunehmenden Digitalisierung wächst die Angriffsfläche. Risiken entstehen vor allem dort, wo Geräte nicht zentral verwaltet werden, Sicherheitsupdates fehlen oder Benutzerkonten unzureichend geschützt sind.

Cyberangriffe auf Bildungseinrichtungen beginnen häufig beim alltäglichen Umgang mit digitalen Systemen: im E-Mail-Postfach oder beim Zugang zu einer Lernplattform. Phishing und kompromittierte Zugangsdaten spielen dabei eine zentrale Rolle. Künstliche Intelligenz erhöht das Bedrohungspotenzial zusätzlich, weil sich betrügerische Nachrichten glaubwürdiger formulieren und gezielter auf einzelne Personen zuschneiden lassen. Aber auch die Schatten-IT (Shadow IT) trägt maßgeblich zu einer erhöhten Bedrohung bei, indem potenziell riskante Hard- und Software ungeprüft und unverwaltet im Netzwerk der Schule verwendet werden.

Schulen und Schulträger sollten ihren Sicherheitsbedarf daher frühzeitig in die Investitionsplanung aufnehmen und erfahrene Fachleute einbeziehen. So lässt sich frühzeitig festlegen, welche technischen und organisatorischen Sicherheitsmaßnahmen erforderlich sind und wie Betrieb, Support und Weiterentwicklung langfristig sichergestellt werden können.

IT-Sicherheit an Schulen: Eine Bestandsaufnahme*

Positive Selbsteinschätzung, häufige reale Vorfälle

Sophos hat im Juli 2026 insgesamt 200 Verantwortliche in schulischen Organisationen befragen lassen – über verschiedene Schulformen, Träger und Größenklassen hinweg. Beim eigenen Sicherheitsstand fällt die Einschätzung dabei positiv aus: 67,5 Prozent bewerten ihn als gut oder sehr gut. Nur 28,5 Prozent sehen deutliche Lücken und lediglich zwei Prozent sprechen von erheblichem Nachholbedarf. Weitere zwei Prozent haben keine Aussage dazu getroffen.

Dieser positiven Einschätzung steht eine hohe Zahl beobachteter Bedrohungen und Sicherheitsvorfälle gegenüber. 47,5 Prozent haben in den vergangenen zwölf Monaten Phishing-Mails an Lehrkräfte oder Verwaltung beobachtet, 31,5 Prozent Cybermobbing und 22,5 Prozent unbefugte Zugriffe auf Schulnetze oder Daten.

Jeweils 17 Prozent berichten von Ausfällen durch Angriffe und von Sicherheitsvorfällen durch Schülerinnen und Schüler. Hinzu kommen Datenschutzverletzungen, Vorfälle über Drittanbieter-Plattformen, Ransomware und kompromittierte Benutzerkonten. Nur 19,5 Prozent geben an, dass ihnen keine Vorfälle bekannt sind. Weitere 2,5 Prozent können die Frage nicht beantworten.

Damit berichten 78 Prozent von mindestens einer konkreten Bedrohung oder einem Sicherheitsvorfall im vergangenen Jahr.

Zugleich zeigt sich ein Zusammenhang mit der Selbsteinschätzung: Von den Befragten, die ihren Sicherheitsstand als deutlich lückenhaft bewerten, berichten 33,3 Prozent von unbefugten Zugriffen auf Netze oder Daten. Bei einem guten Sicherheitsstand sind es 18,3 Prozent.

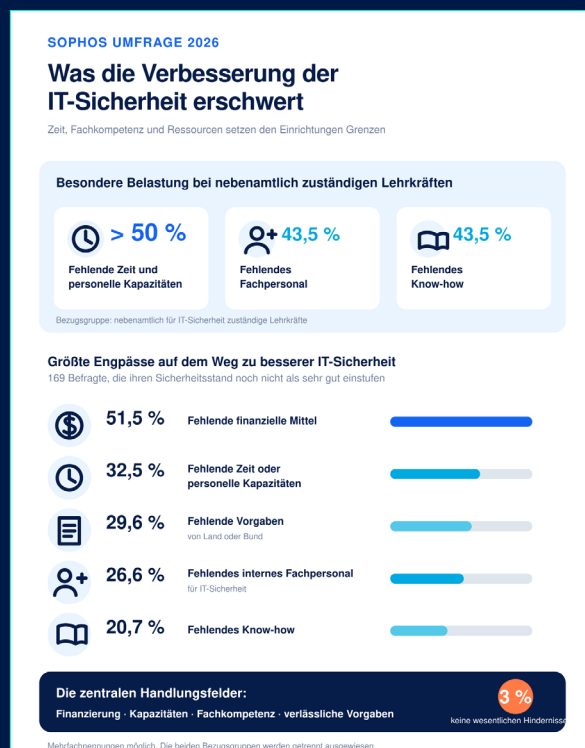


IT-Verantwortung bleibt häufig eine Zusatzaufgabe

Nur knapp jede vierte befragte Einrichtung verfügt über eine interne Fachkraft, die ausschließlich für IT-Sicherheit zuständig ist. In den übrigen Einrichtungen liegt die Verantwortung häufig bei der allgemeinen IT, der Schulleitung oder einem externen Dienstleister. Vielerorts übernehmen auch IT-affine Lehrkräfte diese Aufgabe zusätzlich.

Die Folgen zeigen sich bei der Weiterentwicklung der IT-Sicherheit. Neben finanziellen Mitteln fehlen vor allem Zeit und qualifizierte Fachkräfte. Einige Verantwortliche vermissen außerdem klare Vorgaben von Land oder Bund. IT-Sicherheit konkurriert damit häufig mit anderen Aufgaben um die vorhandenen Ressourcen.

Die Antworten zeigen: Die Verantwortlichen erkennen die Bedrohung und benennen klar, was einen besseren Schutz erschwert – fehlende Ressourcen, Fachkompetenz und verlässliche Strukturen.



IT-Sicherheit in der Investitionsplanung

Der Digitalpakt 2.0 bietet Schulen und Schulträgern die Möglichkeit, IT-Sicherheit verbindlich in ihre Investitionsplanung aufzunehmen. Dazu gehören klare Zuständigkeiten und die Frage, wie die Systeme nach der Anschaffung dauerhaft sicher betrieben werden können.

28 Prozent der Befragten haben entsprechende Maßnahmen bereits fest eingeplant, die Hälfte denkt darüber nach. Zugleich wissen 12,5 Prozent nicht, ob IT-Sicherheit überhaupt förderfähig ist. Bei den konkreten Planungen stehen Netzwerksicherheit und Schulungen an erster Stelle. Es folgen Multi-Faktor-Authentifizierung, Cloud-Sicherheit und Richtlinien für den sicheren Einsatz von KI. Für viele Schulträger besteht der nächste Schritt nun darin, aus diesen Überlegungen konkrete, förderfähige Vorhaben zu entwickeln.

Zentrale IT-Sicherheit in der Praxis

Wie sich solche Vorhaben in der Praxis umsetzen lassen, zeigen die Beispiele aus Bad Dürkheim und Alzey-Worms. Beide Kreisverwaltungen betreuen die IT-Sicherheit mehrerer Schulen zentral. Integrierte Sicherheitslösungen und eine kontinuierliche Überwachung erleichtern die Administration, entlasten die Verantwortlichen und tragen zu einem verlässlichen digitalen Schulbetrieb bei.

Kreisverwaltung Bad Dürkheim: Cybersecurity für 14 Schulen aus einer Hand

PRAXISBEISPIEL · LANDKREIS BAD DÜRKHEIM

14 Schulen zentral und rund um die Uhr absichern

14
SCHULEN

plus weitere Verwaltungsstandorte

Begrenzte personelle Ressourcen treffen auf wachsende Anforderungen an die IT-Sicherheit.

SICHERHEITSARCHITEKTUR

Schulen — Zentrale Plattform — 24/7

Endgeräte und Netzwerke werden zentral verwaltet. Sicherheitsereignisse analysiert das MDR-Team rund um die Uhr und reagiert bei Bedarf unmittelbar.

Im Einsatz: Sophos Fusion · Sophos XDR · Sophos MDR

WIRKUNG IM ALLTAG

- Zentrale Verwaltung**
aller eingebundenen Geräte
- Gezielte Zugänge**
und eine kleinere Angriffsfläche
- Schnelle Reaktion**
auch am Wochenende

” Nach der Umstellung können wir uns nun auf eine Überwachung rund um die Uhr durch externe Profis verlassen, die Sicherheitsvorfälle auch am Wochenende im Blick haben und gegebenenfalls schnell reagieren können.

Jens Preßler · Referatsleiter, Landkreis Bad Dürkheim

Hier geht es zum detaillierten Anwenderbericht der [Kreisverwaltung Bad Dürkheim](#)

Kreisverwaltung Alzey-Worms: Integrierte Cybersicherheit für Schulen

PRAXISBEISPIEL · LANDKREIS ALZEY-WORMS

Rund 450 Endgeräte im Blick – mehr Freiraum für die IT

RUND

450
ENDGERÄTE



an den kreiseigenen Schulen

Eine heterogene IT soll gemeinsam geschützt werden – auch wenn eigenes Sicherheitspersonal nicht dauerhaft verfügbar ist.

SICHERHEITSARCHITEKTUR



Endpunkte, Server, Firewall und Schwachstellenmanagement laufen auf einer Plattform zusammen.

Sicherheitsereignisse werden kontinuierlich überwacht, miteinander in Beziehung gesetzt und durch das MDR-Team analysiert und bewertet.

Im Einsatz: Sophos Fusion · Sophos MDR · Sophos NDR · Sophos Managed Risk · Sophos Firewall

WIRKUNG IM ALLTAG



Zentraler Überblick
über alle relevanten Systeme



Kurze Reaktionszeiten
auch außerhalb der Dienstzeit



Freiraum für die IT
und ihre strategischen Aufgaben

”

Das Sicherheitsempfinden hat sich bei uns exorbitant gesteigert. Wir wären nicht in der Lage gewesen, diese kurzen Reaktionszeiten bei Detection and Response selbst umzusetzen – erst recht nicht außerhalb der Dienstzeit.

Marc Kramer · Kreisverwaltung Alzey-Worms

Hier geht es zum detaillierten Anwenderbericht der [Kreisverwaltung Alzey-Worms](#)

Aktuelle Cyberrisiken: KI, Drittanbieter und Ransomware

Phishing mit KI: Wenn Angriffe täuschend echt wirken

Phishing ist laut der aktuellen Studie von Sophos* mit 47,5 Prozent die am häufigsten genannte Bedrohung der vergangenen zwölf Monate. Mithilfe generativer KI lassen sich entsprechende Nachrichten schneller erstellen, sprachlich anpassen und in großer Zahl personalisieren. Namen, Funktionen oder öffentlich bekannte Termine können ihnen einen glaubwürdigen Rahmen geben. Deshalb lohnt ein genauer Blick auf den Absender, die verlinkte Internetadresse und die in der Nachricht verlangte Handlung.

Die IT-Verantwortlichen haben diese Entwicklung im Blick. Eine deutliche Mehrheit rechnet damit, dass KI-gestützte Angriffe und weitere KI-bezogene Sicherheitsrisiken den Schulalltag in den kommenden zwei Jahren spürbar beeinflussen werden. Konkrete Schutzmaßnahmen sind bislang allerdings deutlich weniger verbreitet. Viele Einrichtungen haben erste Schritte unternommen; umfassend vorbereitet sind erst wenige.

Wenn das Risiko außerhalb der Schule liegt

Die digitale Infrastruktur einer Schule reicht heute weit über das eigene Netzwerk hinaus. Zu ihr gehören die Konten der Nutzerinnen und Nutzer ebenso wie externe Plattformen, Cloud-Dienste und KI-Anwendungen.

87 Prozent der befragten Organisationen bestätigen, dass sie Lernplattformen, Schulverwaltungssysteme, Cloud-Dienste oder andere externe Lösungen nutzen. Nur 38 Prozent haben deren Sicherheitsstandards geprüft. 34 Prozent setzen entsprechende Plattformen ohne formale Prüfung ein. Weitere 15 Prozent verfügen nach eigener Aussage nicht über das Personal oder die Ressourcen, die dafür erforderlich wären.

PHISHING-BEISPIEL

Eine Nachricht, die plausibel klingt

Drei Details zeigen, weshalb sich ein zweiter Blick lohnt.

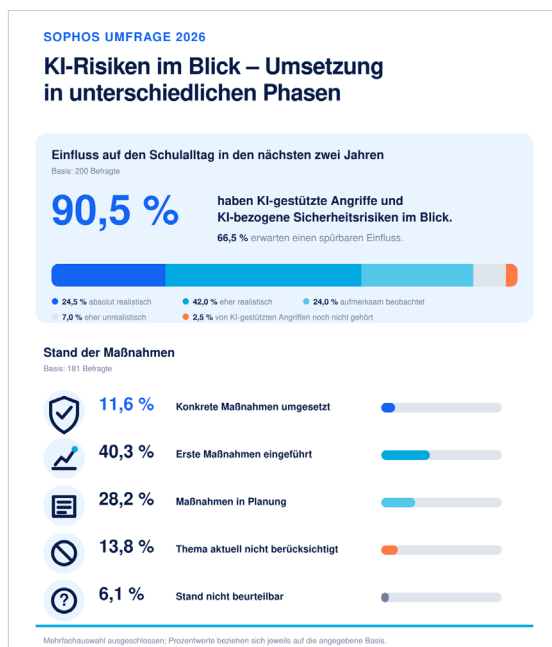
1 Abweichende Internetadresse
Der vertraute Name verdeckt eine fremde Domain.

2 Ungewöhnlicher Zeitdruck
Frist und andgedrohte Sperrung drängen zu einer schnellen Reaktion.

3 Zugangsdaten erneut abfragen
Der Button führt zu einer neuen Anmeldung mit Benutzernamen und Passwort.

Vertrauter Absender, plausibler Anlass, korrekte Sprache:
Entscheidend sind die Details.

Phishing-Bemerkung: Die verwendete e-mail-Adresse ist keine echte Internetadresse.



Sophos State of Ransomware Report: Identitäten als Einfallstor

Die internationale [Sophos-Studienreihe „State of Ransomware“](#) zeigt für deutsche Bildungseinrichtungen eine klare Verschärfung der Lage über die Jahre hinweg. Die Studie wies für den Bildungssektor 2021 eine Angriffsrate von 44 Prozent aus. Nach einem zwischenzeitlichen Hoch von 80 Prozent lag sie 2024 bei 63 Prozent. 2025 rückte zudem die Belastung der betroffenen IT-Teams in den Fokus: Fast 40 Prozent berichteten von Angst und psychischen Folgen.

Auch der aktuelle Sophos State of Ransomware Report 2026 zeigt im Bildungssektor eine weitere weltweite Verschärfung der Lage. Nach den neuesten Auswertungen waren 71 Prozent der Ransomware-Attacken die bedeutendsten Angriffe auf die schulischen Bildungseinrichtungen. Dabei waren bösartige E-Mails mit 31 Prozent die häufigste technische Ursache. Identitätsbasierte Attacken lösten 85 Prozent der Angriffe im gesamten Bildungssektor aus. Die Folge: Die Verschlüsselungsrate von Daten im Bereich der allgemeinen Bildung hat sich mehr als verdoppelt und stieg von 29 Prozent im Jahr 2025 auf 61 Prozent im Jahr 2026.

Die häufigsten betrieblichen Ursachen im Bereich der allgemeinen Bildung waren menschliches Versagen (52 Prozent), mangelnder Schutz (47 Prozent), unbekannte Sicherheitslücken (42 Prozent) und Personal- oder Kapazitätsmangel (41 Prozent).

Die Ransomware-Attacken haben schwere Auswirkungen auf den Lehrbetrieb: 31 Prozent der Bildungseinrichtungen brauchten einen Monat oder länger, um die Systeme und Daten wiederherzustellen und sich zu erholen - mehr als jeder andere befragte Sektor.

Auch die Belastung der Sicherheitsteams ist weiterhin angespannt. Etwa 39 Prozent der Teams im Bildungssektor meldeten Abwesenheiten von Mitarbeitern aufgrund von Stress oder psychischen Problemen, im Vergleich zu 29 Prozent in allen Sektoren.



Rechtliche Einordnung: Wenn ein IT-Vorfall auch zum Datenschutzvorfall wird

**Gastbeitrag von Dr. Andreas Daum, Rechtsanwalt
(Fokus: Cybersecurity & Data Economy) bei Noerr
Partnerschaftsgesellschaft mbB**

Phishing-Mails, kompromittierte Zugangsdaten oder ein Ransomware-Angriff können den Schutz personenbezogener Daten verletzen und damit einen Datenschutzvorfall auslösen. In Schulen sind davon häufig sensible Informationen betroffen, darunter Schülerdaten, Noten, Gesundheitsinformationen oder Kontaktdaten von Erziehungsberechtigten.

In der aktuellen Sophos-Umfrage* berichteten 12,5 Prozent der befragten Organisationen von einem Datenschutzvorfall mit Offenlegung personenbezogener Daten. 22,5 Prozent hatten bereits einen unbefugten Zugriff auf das Schulnetz oder dort gespeicherte Daten erlebt.

DSGVO: Prüfen, dokumentieren und gegebenenfalls melden

Wird ein Datenschutzvorfall bekannt, muss die verantwortliche Stelle prüfen, welche Daten und Personen betroffen sind und welche Risiken daraus entstehen. Wer im Schulbereich datenschutzrechtlich verantwortlich ist, richtet sich nach dem jeweiligen Landesrecht. Die Verantwortung kann bei der Schule, dem Schulträger oder einer anderen öffentlichen Stelle liegen.

Nach Art. 33 DSGVO ist ein Datenschutzvorfall unverzüglich und möglichst innerhalb von 72 Stunden an die zuständige Aufsichtsbehörde zu melden. Das gilt, sofern ein Risiko für die Rechte und Freiheiten natürlicher Personen nicht ausgeschlossen werden kann. Eine verspätete Meldung ist zu begründen. Unabhängig von der Meldepflicht muss jeder Datenschutzvorfall intern dokumentiert werden.

Besteht voraussichtlich ein hohes Risiko für die betroffenen Personen, sind auch diese nach Art. 34 DSGVO unverzüglich zu benachrichtigen. Informationen für minderjährige Schülerinnen und Schüler sind klar, verständlich und altersgerecht zu formulieren. Ob zusätzlich die Erziehungsberechtigten einzubeziehen sind, hängt von Alter und Einsichtsfähigkeit der Betroffenen sowie den einschlägigen schul- und landesrechtlichen Regelungen ab.



Potenzielle Konsequenzen bei Verstößen

Verstöße gegen diese Pflichten können aufsichtliche Maßnahmen, Bußgelder oder Schadensersatzansprüche nach sich ziehen. Welche Bußgeldregelungen gelten, hängt auch von der Trägerform ab. Für Länder, Kommunen und kommunale Schulträger sind insbesondere die jeweiligen Landesdatenschutzgesetze maßgeblich. Schulen in freier Trägerschaft können einem anderen Bußgeldregime unterliegen.

Schadensersatzansprüche nach Art. 82 DSGVO setzen einen DSGVO-Verstoß, einen daraus entstandenen materiellen oder immateriellen Schaden und einen ursächlichen Zusammenhang zwischen beiden voraus.

Anforderungen risikogerecht umsetzen

Kinder genießen bei der Verarbeitung ihrer personenbezogenen Daten besonderen Schutz. Umfang und Sensibilität schulischer Daten stellen daher hohe Anforderungen an die Risikobewertung, die technischen und organisatorischen Maßnahmen sowie die Kommunikation mit den Betroffenen.

Welche Maßnahmen angemessen sind, hängt von den verarbeiteten Daten, den Zugriffsberechtigungen und den beteiligten Akteuren ab. Entscheidend ist eine nachvollziehbare und dokumentierte Bewertung: Welche Daten werden verarbeitet? Wer kann darauf zugreifen? Welche Risiken ergeben sich daraus? Welche Schutzmaßnahmen wurden abgeleitet? Und wie wird ihre Wirksamkeit regelmäßig überprüft?

Wer Datenverarbeitungen, Zuständigkeiten und technische Abhängigkeiten kennt, Risiken bewertet und Entscheidungen dokumentiert, schafft eine belastbare Grundlage für den Umgang mit Sicherheitsvorfällen.

Wenn ein IT-Vorfall zum Datenschutzvorfall wird

Der rechtliche Reaktionspfad nach der DSGVO



Rechtliche Einordnung nach Art. 33 und 34 DSGVO

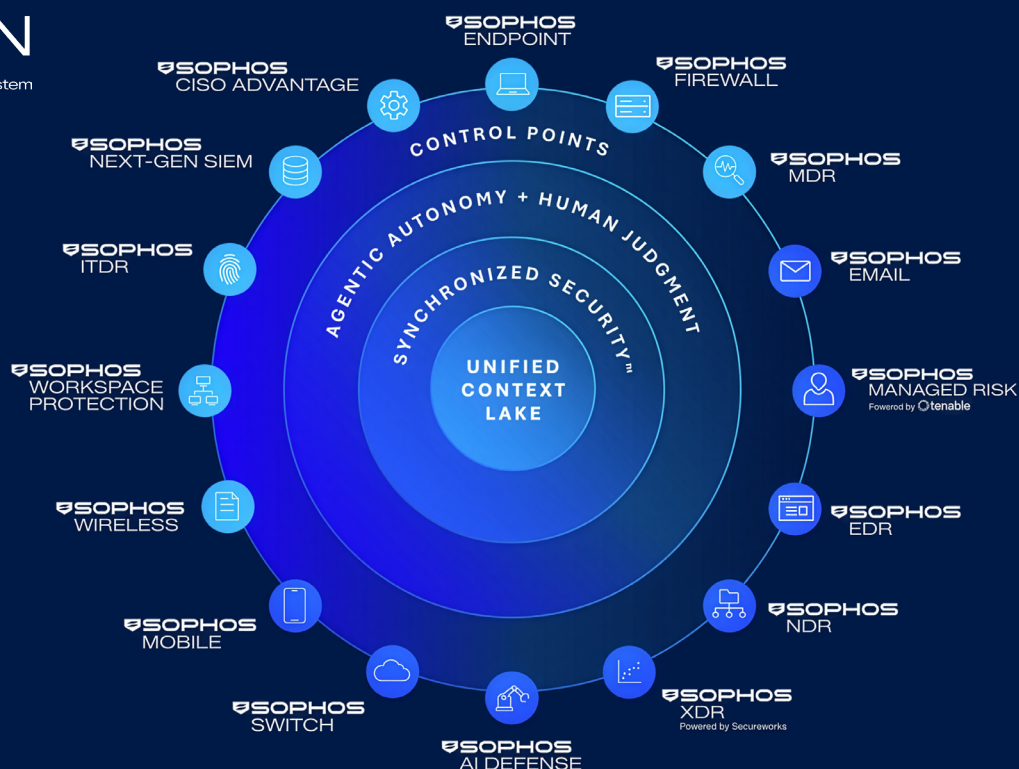
Dokumentieren gilt immer. Melden und benachrichtigen hängen von der Risikobewertung ab.

Von Sicherheits-Lösungen zum integrierten Cyber Defense System

Sophos Cyber Defense System

Schulen und Schulträger stehen vor der Aufgabe, eine komplexe IT-Infrastruktur aus Endgeräten, Netzwerken, Cloud-Diensten und digitalen Identitäten abzusichern. Die Ergebnisse der Befragung zeigen, wie schwer es vielen Einrichtungen fällt, diese Sicherheit mit begrenzten Ressourcen dauerhaft zu organisieren. Das Cyber Defense System Sophos Fusion vereint unterschiedliche Kontrollpunkte in einer einzigen, offenen Architektur. Dadurch können Schulträger die IT-Sicherheit ihrer Schulen zentral verwalten und den administrativen Aufwand begrenzen. Sophos AI Defense hilft Schulträgern, den Einsatz von KI in ihrer Umgebung zu überblicken und zu kontrollieren, indem es Transparenz, Risikoinformationen und klare Regeln für die sichere Nutzung der KI an einem Ort vereint.

Im Zentrum steht ein KI-natives Cybersecurity-Verteidigungssystem, das Endpoint-, Netzwerk-, E-Mail-, Cloud- und Identitätssicherheit sowie professionelle Sicherheitsservices in einer offenen Architektur zusammenführt. Neben Sophos-Lösungen liefern über 500 integrierte Drittanbieter-Technologien Echtzeit-Telemetriedaten an Sophos Fusion. Dadurch agieren alle Kontrollpunkte, Dienste, Datenquellen und IT-Sicherheitsanalysten – unabhängig vom Anbieter – als Einheit, womit Bedrohungen schneller erkannt und Reaktionsmaßnahmen effizienter koordiniert werden. Mithilfe agentischer KI erkennt und untersucht das System Angriffe in Echtzeit und leitet automatisierte Abwehrmaßnahmen ein.



Zusätzlich unterstützen passende Lösungen die Umsetzung von Datenschutz-, Compliance- und Jugendschutzanforderungen. Rollenbasierte Richtlinien steuern Internetzugriffe, trennen WLAN-Netze und ermöglichen die sichere Einbindung privater Endgeräte (BYOD). Moderne Schutzmechanismen erkennen Bedrohungen frühzeitig und reagieren automatisiert, bevor sich Angriffe ausbreiten.

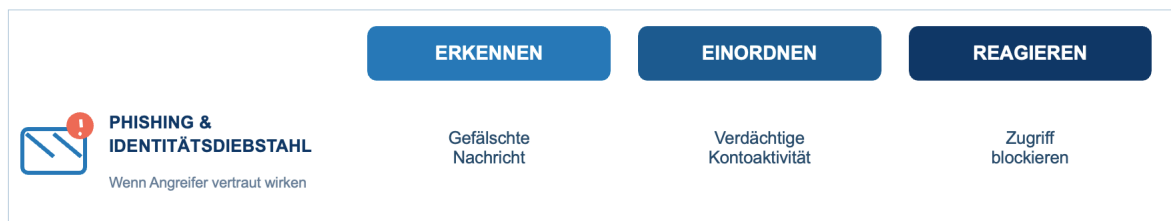
Der entscheidende Vorteil für Schulen und Schulträger: Das Sophos Cyber Defense System deckt nicht nur alle Bereiche der IT-Sicherheit für individuelle Infrastrukturen ab, sondern bindet auch bestehende Sicherheitslösungen nahtlos ein, ohne die Komplexität zu erhöhen.

Für Schulen bedeutet das: Das Cyber Defense System Sophos Fusion verbindet Sicherheitskontrollen, Datenquellen und Integrationen in einer gemeinsamen Architektur. So erhalten Schulträger einen zentralen Überblick über ihre Sicherheitslage und können Bedrohungen schneller und koordiniert abwehren.

Drei Szenarien, drei Sophos-Sicherheitsansätze

Schulen und Schulträger sind unterschiedlichen Formen der Cyberkriminalität ausgesetzt. Die Bandbreite reicht von gezielten Störungen des Schulbetriebs über Erpressung und den Diebstahl sensibler Daten bis zur Übernahme von Konten und Systemen. Entscheidend ist, verdächtige Signale früh zu erkennen, richtig einzuordnen und schnell darauf zu reagieren. Wie diese Sicherheitslogik in unterschiedlichen Angriffsszenarien greift, zeigen die folgenden Beispiele.

Szenario 1 – Phishing & Identitätsdiebstahl: Wenn Angreifer wie Kollegen aussehen



Das Angriffsmuster

Eine täuschend echte Microsoft-365-Mail fordert zur erneuten Anmeldung auf. Die verlinkte Seite imitiert einen echten Login und greift die Zugangsdaten ab. Mit dem übernommenen Konto erhalten Angreifer Zugriff auf E-Mails, Cloud-Daten und verbundene Systeme.

Der konkrete Fall: 280 Millionen gestohlene Datensätze

Am 7. Mai 2026 drang die Hackergruppe über das Lernmanagementsystem Canvas in 330 Bildungseinrichtungen weltweit ein, darunter deutsche Schulen ([Quelle](#)). Gestohlen wurden 280 Millionen Datensätze mit Namen, E-Mail-Adressen und internen Nachrichten. Der Vorfall führte zu Lösegeldforderungen, möglichen Haftungsfragen sowie datenschutzrechtlichen Prüf- und gegebenenfalls Meldepflichten. Auch das Vertrauen in die Sicherheit der betroffenen Einrichtungen nahm Schaden.

Was Schutz bietet

BSI und CISA nennen kompromittierte Zugangsdaten als einen der wichtigsten Einfallstore für Cyberangriffe. Sie empfehlen Sensibilisierung, Multi-Faktor-Authentifizierung und eine kontinuierliche Überwachung von Identitäten und Zugriffsrechten. Die CISA hebt zudem phishing-resistente MFA und Identity & Access Management hervor.

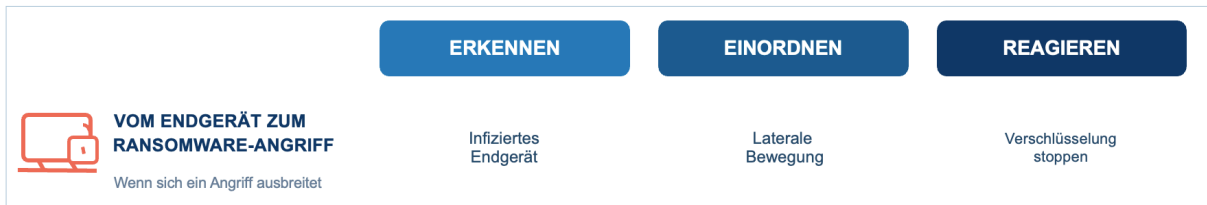
Die Sophos-Lösungen

- ▶ [Sophos Managed Detection and Response \(MDR\)](#) analysiert Identitäts- und Endpoint-Signale rund um die Uhr und reagiert auf verdächtige Aktivitäten.
- ▶ [Sophos Email](#) blockiert Phishing-Mails und schädliche Links.
- ▶ [Sophos Identity Threat Detection and Response \(ITDR\)](#) erkennt Identitätsrisiken und verdächtige Anmeldeaktivitäten.
- ▶ [Sophos NDR](#) überwacht in Zusammenarbeit mit verwalteten Endpoints und Firewalls Netzwerkaktivitäten und erkennt ungewöhnliche Datenverkehrsflüsse von nicht verwalteten Systemen und IoT-Geräten, nicht autorisierte Assets, interne Bedrohungen, bisher unbekannte Zero-Day-Angriffe und ungewöhnliche Muster tief im Netzwerk.
- ▶ [Sophos Phish Threat](#) trainiert Mitarbeitende und Lehrkräfte mit realistischen Phishing-Simulationen.

Jetzt handeln

Schützen Sie Ihre Einrichtung vor Phishing-Angriffen. Entdecken Sie, [wie Sophos Ihnen hilft](#).

Szenario 2 – Vom infizierten Endgerät zum Ransomware-Angriff



Das Angriffsmuster

Ein schädlicher Anhang oder eine Schwachstelle kann Angreifern Zugang zum Netzwerk verschaffen. Dort stehlen sie Zugangsdaten, erweitern ihre Berechtigungen und bewegen sich zwischen den Systemen. Haben sie Server und sensible Daten erreicht, folgen Datendiebstahl, Verschlüsselung und Lösegeldforderung.

Der konkrete Fall: 2,5 Terabyte gestohlene Daten

Im Januar 2025 griff LockBit ein Schulnetzwerk in der Vorderpfalz an. Betroffen waren 45 Schulen; 2,5 Terabyte Daten wurden im Darknet veröffentlicht ([Quelle](#)). Allein aus einem Gymnasium stammten 350 Gigabyte mit Stammdaten, Zeugnissen, Gesundheitsinformationen und internen Dokumenten. Der Schulträger isolierte Systeme und schloss Schwachstellen. Hinzu kamen die datenschutzrechtliche Aufarbeitung und ein erheblicher Vertrauensverlust.

Was Schutz bietet

BSI und CISA empfehlen, die Angriffskette bereits vor der Verschlüsselung zu unterbrechen. Dazu gehören die Überwachung verdächtiger Anmeldungen, Multi-Faktor-Authentifizierung, eine zügige Schwachstellenbehebung sowie getestete Backups und ein eingeübter Incident-Response-Plan.

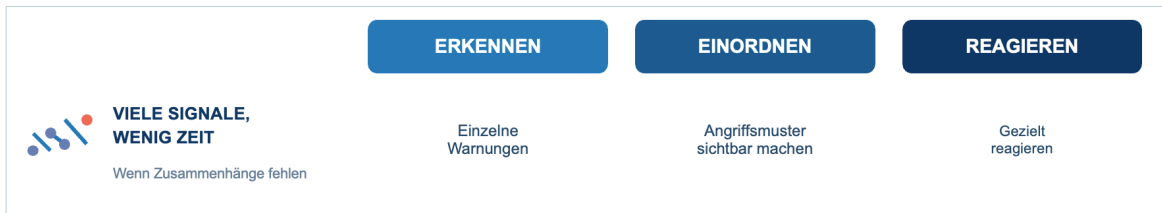
Die Sophos-Lösungen

- ▶ [Sophos Endpoint](#) erkennt Malware und unterbindet verdächtige Verschlüsselungsaktivitäten.
- ▶ [Sophos Firewall](#) kontrolliert und segmentiert den Netzwerkverkehr, um die Bewegungsfreiheit von Angreifern zu begrenzen.
- ▶ [Sophos Identity Threat Detection and Response \(ITDR\)](#) erkennt identitätsbezogene Risiken und verdächtige Anmeldeversuche.
- ▶ [Sophos Extended Detection and Response \(XDR\)](#) führt Signale aus Endpoints, Netzwerk und Identitäten zusammen.
- ▶ [Sophos Managed Detection and Response \(MDR\)](#) überwacht die Umgebung rund um die Uhr und neutralisiert Bedrohungen.

Jetzt handeln

Schützen Sie Ihre Einrichtung vor Ransomware. Entdecken Sie, [wie Sophos Ihnen hilft](#).

Szenario 3 – Kleine IT-Teams, große Angriffsfläche: Wenn Security-Signale unentdeckt bleiben



Das Angriffsmuster

Ein kommunaler Schulträger betreut 15 Schulen mit 6.000 Schülerinnen und Schülern, 700 Mitarbeitenden und 4.000 Endgeräten. Das kleine IT-Team erhält täglich Meldungen über ungewöhnliche Anmeldungen, Malware, verdächtige PowerShell-Aktivitäten oder auffällige Netzwerkverbindungen. Einzeln wirken solche Ereignisse oft harmlos; in Kombination können sie auf einen laufenden Angriff hinweisen.

Der konkrete Fall: Angriff auf einen Schulfoto-Onlinedienst

Im Frühjahr 2026 drangen Angreifer in die Systeme eines Schulfoto-Onlinedienstes ein, über den zahlreiche Schulen ihre Klassenfotos abwickeln. Sie stahlen und löschten Fotos, Namen, Adressen und Bestelldaten ([Quelle](#)). Wie in vielen kleinen IT-Teams fehlten auch hier die Kapazitäten, um die Vielzahl täglicher Warnsignale bei Drittanbietern kontinuierlich im Blick zu behalten. Der Dienst wurde unterbrochen, Zugriffsrechte mussten überprüft und der Vorfall datenschutzrechtlich bewertet werden. Besonders für Eltern und Kinder bedeutete die Offenlegung persönlicher Bilder einen erheblichen Kontroll- und Vertrauensverlust.

Was Schutz bietet

BSI und CISA empfehlen, verdächtige Authentifizierungen und Angreifertechniken über die gesamte Angriffskette hinweg zu überwachen und gemeinsam auszuwerten. Regelmäßig erprobte Incident-Response-Pläne schaffen zusätzliche Handlungssicherheit.

Die Sophos-Lösungen

- ▶ **Sophos Extended Detection and Response (XDR)** Powered by Secureworks führt Sicherheitsdaten aus Endpoints, Netzwerken, Identitäten und Cloud-Umgebungen zusammen und macht Angriffsmuster sichtbar. Die aktuelle Version bietet noch leistungsfähigere Erkennung, integrierte Bedrohungsinformationen, erweiterte bidirektionale Integrationen, Automatisierungs-Playbooks (SOAR), das Sophos Email Monitoring System (EMS), eine deutlich verbesserte Benutzererfahrung für Analysten und vieles mehr.
- ▶ **Sophos Identity Threat Detection and Response (ITDR)** erkennt verdächtige Anmeldungen und den Missbrauch von Zugangsdaten.

- ▶ **Sophos Managed Detection and Response (MDR)** übernimmt die Überwachung, Untersuchung und Reaktion rund um die Uhr und entlastet das interne IT-Team. Die aktuelle Version ist erweitert um umfassendere Integrationen, integrierte Bedrohungsinformationen, Sophos EMS, einen neu gestalteten Arbeitsbereich für Analysten, kontinuierliche agentenbasierte Bedrohungssuche durch das weltweit größte agentenbasierte SOC und vieles mehr.
- ▶ **Sophos Next-Gen SIEM** ist ein auf Compliance ausgerichtetes Add-on für Sophos XDR und Sophos MDR, das eine langfristige Datenaufbewahrung, Compliance-Berichte und Unterstützung für benutzerdefinierte Integrationen bietet.

Jetzt handeln

Entlasten Sie Ihr IT-Team und sorgen Sie für dauerhaft wirksamen Schutz. Entdecken Sie, [wie Sophos Ihnen hilft](#).

Der nächste Schritt: Sicherheit planbar machen

Der Digitalpakt 2.0 bietet die Gelegenheit, IT-Sicherheit dauerhaft im digitalen Schulbetrieb zu verankern. Ausgangspunkt sind eine Bestandsaufnahme der vorhandenen Infrastruktur, klare Zuständigkeiten und ein Sicherheitskonzept, das auch Betrieb, Überwachung und Reaktion berücksichtigt. So lassen sich förderfähige Maßnahmen gezielt entwickeln und technische Investitionen langfristig absichern.

Sophos-Lösungsmatrix für mehr IT-Sicherheit in Schulen

Mit seinem integrierten Lösungsangebot setzt das Sophos AI-Native Cybersecurity Defense System dort an, wo Schulen und Schulträger häufig vor besonderen Herausforderungen stehen: bei begrenzten Ressourcen, komplexen Infrastrukturen und fehlenden durchgängigen Sicherheitsstrukturen. Aufeinander abgestimmte Lösungen und ein hoher KI-gestützter Automatisierungsgrad ermöglichen mehr Sicherheit bei geringerem administrativem Aufwand. Je nach Ausgestaltung des jeweiligen Länderprogramms können entsprechende Maßnahmen im Rahmen des Digitalpakts 2.0 förderfähig sein.

Herausforderung	Sophos-Lösung	So profitieren Schulen und Schulträger
Einheitliche, zentrale Verwaltung der gesamten Sicherheitsinfrastruktur	Sophos Fusion	Sophos Fusion ist das branchenweit umfassendste Cyber-Abwehrsystem und schützt Organisationen vor KI-gestützten Bedrohungen, die sich schneller bewegen, als die Cyberabwehr reagieren kann. Aufbauend auf der Architektur des Sophos AI-Native Cyber Defense System erfasst Sophos Fusion alle Informationen, vernetzt sämtliche Elemente und ermöglicht es Abwehrmaßnahmen, als Einheit zu reagieren.
Sichere Anbindung verteilter Standorte mit geringem Aufwand	Sophos Firewall mit Sophos RED Devices	Mit der Sophos Firewall werden Netzwerke von Schulen und Schulträgern inklusive verteilter Standorte zentral geschützt. Die Anbindung der Standorte erfolgt sicher und ohne zusätzliche Administration über Sophos RED Devices.
Jugendschutzfilter	Sophos Firewall	Mit individuellen Benutzerrichtlinien wird der Zugriff auf Webinhalte gesteuert, um Jugendschutzvorgaben gezielt umzusetzen.
Absicherung des Netzwerks, Kontrolle der Netzwerkkommunikation und Segmentierung	Sophos Firewall, Sophos Endpoint	Leistungsfähige Erkennungstechnologien identifizieren auch Malware, die herkömmliche Schutzmechanismen übersehen können. Sophos Endpoint und die Zero-Day Protection der Sophos Firewall ergänzen den Netzwerkschutz. Segmentierung begrenzt zugleich die Bewegungsfreiheit eines Angreifers.

Herausforderung	Sophos-Lösung	So profitieren Schulen und Schulträger
WLAN – Bereitstellung und Absicherung	Sophos Wireless	Flächendeckende und sichere Bereitstellung von WLAN-Netzen durch zentral gesteuerte Sicherheitsvorgaben der Firewall und Sophos Central
Schutz für Endgeräte	Sophos Endpoint	Eine integrierte Endpoint-Schutz- und EDR-Lösung, die auch KI-gestützte Angriffe bekämpft. Sie stoppt Bedrohungen, die entweder von Menschen oder von agentischen KI-Tools ausgehen. Die leistungsstarke Anti-Ransomware, verhaltensbasierte Bedrohungserkennung, Exploit-Prävention, adaptive Abwehrmaßnahmen und Funktionen zur Reduzierung der Bedrohungsfläche stoppen Angriffe, bevor sie Schaden anrichten können.
Schutz für Mobilgeräte, z.B. Tablets	Sophos Mobile	Verwaltung, Sicherung, Konfiguration und Einrichtung traditioneller und mobiler Endpoints inklusive einheitlicher Sicherheitsrichtlinien unabhängig vom Gerätetyp, Besitzer oder Standort des Geräts.
Phishing-Mails an Lehrkräfte oder Verwaltung	Sophos Email, Sophos ITDR, Sophos MDR, Sophos Phish Threat	Sophos Email erkennt Phishing-Versuche, schädliche URLs und Impersonation, bevor diese die Benutzenden erreichen. Sophos ITDR erkennt identitätsbezogene Risiken und verdächtige identitätsbezogene Aktivitäten. Sophos MDR untersucht Identitäts-, Endpoint- und andere Security-Signale und reagiert auf aktive Bedrohungen. Sophos Phish Threat sensibilisiert Mitarbeitende und Lehrkräfte durch realistische Phishing-Simulationen.
Malware, Exploits und Ransomware-Aktivitäten	Sophos Endpoint	Erkennt und blockiert Malware, Exploit-Techniken und Ransomware-Aktivitäten. CryptoGuard schützt vor Ransomware, indem verdächtige Verschlüsselungsaktivitäten erkannt und unterbunden werden.

Herausforderung	Sophos-Lösung	So profitieren Schulen und Schulträger
Identitätsbezogene Risiken und Aktivitäten, 24/7-Überwachung und Reaktion auf Bedrohungen	Sophos ITDR, Sophos XDR, Sophos MDR	Sophos ITDR erkennt identitätsbezogene Risiken und Aktivitäten, wenn ein Angreifer versucht, kompromittierte Benutzerkonten und Berechtigungen für die weitere Angriffskette zu nutzen. Sophos XDR führt Informationen aus Endpoint, Netzwerk, Identität und weiteren Security-Quellen zusammen und analysiert sie. Sophos MDR untersucht verdächtige Aktivitäten rund um die Uhr und reagiert auf aktive Angriffe.
Sichere Nutzung von KI-Tools im schulischen Alltag	Sophos AI Defense	Sophos AI Defense basiert auf Sophos Fusion und hilft den Einsatz von KI zu überwachen, das Verhalten von KI zu steuern und die Organisation vor KI-bedingten Risiken zu schützen. Die Lösung erkennt jegliche Nutzung von KI, steuert die KI-Nutzung anhand von individuellen Vorgaben und unterbindet proaktiv gefährliche KI-Aktivitäten auf Endpunkten und im Netzwerk.

Ausgezeichnete Sicherheit. Anerkannt von Experten und Anwendern.

Auszeichnungen führender IT-Fachmedien und Branchenplattformen bestätigen unsere Kompetenz im Bereich Cybersicherheit.



Erfahren Sie mehr zu den
Angeboten von Sophos
speziell für Schulen und
Schulträger hier.

Sie haben Fragen rund um IT-Sicherheit
an Schulen? Unser erfahrenes Schulteam
unterstützt Sie gerne.

Deutschland

E-Mail: publicsalesDE@sophos.de
www.sophos.de/digitale-schule