

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.
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.

Herausforderung	Sophos-Lösung	So profitieren Schulen und Schulträger
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.
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.



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

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