



Microsoft Education Sicherheits-Toolkit

Sichere IT – vereinfacht für
alle Lernumgebungen



Bei Microsoft verstehen wir, dass Schulen und Institutionen in einigen der am stärksten bedrohten und komplexesten digitalen Umgebungen arbeiten. Da Cyberangriffe immer häufiger und ausgefeilter werden, ist Cybersicherheit unerlässlich – nicht nur zum Schutz vertraulicher Daten von Studierenden, von Forschung und geistigem Eigentum, sondern auch zur Sicherstellung der Kontinuität von Lehre, Lernen und institutionellen Abläufen.

Wir verpflichten uns, Bildungseinrichtungen so zu befähigen, dass sie sichere, resiliente und vertrauenswürdige digitale Infrastrukturen schaffen können, die akademischen Erfolg ohne Kompromisse ermöglichen.

Unsere Vision für die Sicherheit auf dem Campus basiert auf Einfachheit, Skalierbarkeit und Intelligenz:

- Wir bieten eine vereinfachte Verwaltung mit einem integrierten Technologie-Stack, der darauf ausgelegt ist, Vorfälle zu reduzieren und Lern- und Forschungsumgebungen zu schützen.
- Wir liefern KI-gestützte Sicherheitslösungen, um Datenschutz, Compliance und Management mit maschineller Geschwindigkeit und im großen Maßstab zu unterstützen.
- Wir helfen Schulen und Institutionen, ihre Security Operations (SecOps) mit Automatisierung und integrierten Tools zu skalieren und investieren durch praxisorientierte Student Security Operations Centers (SOCs) und Qualifizierungsprogramme in die nächste Generation von Cyber-Sicherheitsfachkräften.

Diese Säulen sind eine belastbare, adaptive Sicherheitsgrundlage, die Institutionen jeder Größe schützt und sichere, innovative Lernumgebungen ermöglicht.

Führungskräfte im Bildungsbereich erkennen die Notwendigkeit rechtzeitiger, strategischer Maßnahmen, um Lernumgebungen zu schützen, die digitale Widerstandsfähigkeit zu stärken und sich auf die Zukunft der KI-gestützten Bildung vorzubereiten. Dieser Moment bietet eine große Chance: Institutionen schützen ihren Campus und sie gestalten die Zukunft der Cybersicherheit. Indem Studierende in Sicherheitsoperationen eingebunden werden und praktische Erfahrungen mit KI-gestützten Tools sammeln, entwickelt sich die Bildung von einer reaktiven zu einer proaktiven Führung und digitalen Widerstandsfähigkeit.

Schulen und Institutionen auf der ganzen Welt sind bereits Vorreiter:

- [Singapore Management University](#) hat die Zero Trust Framework und Security Copilot von Microsoft eingeführt, wodurch die Reaktionszeiten verkürzt, die Arbeitsbelastung des Sicherheitsteams verringert und eine schnellere, sicherere IT-Entscheidungsfindung ermöglicht wurden.
- [Oregon State University](#) hat mit Microsoft Sentinel und Defender ein von Studierenden betriebenes SOC ins Leben gerufen, das praktische Erfahrungen im Bereich Cybersicherheit vermittelt und gleichzeitig die Fähigkeiten zur Erkennung und Reaktion auf Bedrohungen stärkt.
- [New York City Public Schools](#) verwaltet 750.000 LTE-fähige Geräte für Lernende mit Microsoft Intune und stellt so eine sichere, skalierbare und effiziente Geräteverwaltung im größten Schulbezirk der USA sicher.

Die einheitliche Sicherheitsplattform von Microsoft – basierend auf Microsoft 365 – integriert Security Copilot, Sentinel, Defender XDR, Intune, Entra ID und Purview in ein einziges, KI-gestütztes System. Mit diesem Ansatz können Institutionen Geräte absichern, Daten schützen, Compliance verwalten und schneller auf Bedrohungen reagieren – alles über ein einheitliches Dashboard.

Eine der spannendsten Entwicklungen ist das Aufkommen von Studierenden geleiteten SOC's. Es ist ein wirkungsvoller Ansatz, Lernende zu Cyber-Verteidigenden zu machen und bedeutende Karrierewege zu eröffnen.

Sicherheit ist nicht mehr nur eine Verteidigungslinie, sondern ein Katalysator für Innovation. Mit den vertrauenswürdigen Lösungen von Microsoft können Institutionen KI sicher einführen, sicheren Fernunterricht ermöglichen, die globale Forschung unterstützen und das schützen, was am wichtigsten ist: Daten von Lernenden und Integrität im Bildungswesen.

Wir bei Microsoft sind überzeugt, dass Sicherheit mehr ist als nur Schutz – sie eröffnet neue Möglichkeiten. Gemeinsam können wir sichere, inklusive Umgebungen schaffen, in denen Lernen gedeiht, Forschung vorankommt und alle Lernenden Technologie mit Selbstvertrauen erkunden können.



Matt Jubelirer
General Manager,
Microsoft Bildung

Inhalt

Übersicht

- 5 [Microsoft Secure Future Initiative](#)
- 9 [Navigieren in diesem Sicherheitstoolkit](#)
- 11 [Sichereres Lernen ermöglichen mit den Microsoft-Sicherheitstools](#)

Tools

- 13 [Microsoft-Sicherheitstools](#)

Campus-Erfolgsgeschichten

- 16 [Sicherung von Lernumgebungen: K-12-Campus-Erfolgsgeschichten](#)
- 20 [Innovationen im Bereich der Sicherheit in der Hochschulbildung in der Praxis](#)
- 24 [Weitere Kundensicherheitsreferenzen](#)

Planung

- 29 [Strategische Planung für sicherere Lernumgebungen](#)
- 31 [Die aktuelle Sicherheitslage Ihres Campus bewerten](#)
- 34 [Sicherheitsgovernance und Richtlinien](#)
- 36 [Technologiesicherheitsstrategie](#)
- 38 [Readiness der Organisation](#)
- 40 [Finanzielle und strategische Begründung](#)

Implementierung

- 43 [K-12-Implementierungsszenarien](#)
- 47 [Implementierungsszenarien im Hochschulbereich](#)

Forschung

- 52 [Microsoft Security in der Bildung: Von der Bereitstellung bis zum Einfluss auf den Campus](#)
- 54 [Daten und Analytics](#)
- 56 [Ergebnisse aus Wissenschaft und Industrie](#)
- 58 [Glossar der Begriffe](#)
- 59 [Checkliste für die nächsten Schritte](#)

Übersicht

In diesem Abschnitt

[Microsoft Secure Future Initiative](#)

[Navigieren in diesem Sicherheitstoolkit](#)

[Sichereres Lernen ermöglichen mit
den Microsoft-Sicherheitstools](#)



Microsoft Secure Future Initiative

Microsoft ermöglicht Bildungseinrichtungen, mit einer maßgeschneiderten Cybersicherheitsplattform, die vertrauliche Daten von Lernenden, Lehrkräften und Mitarbeitenden schützt, den sich ständig weiterentwickelnden Cyberbedrohungen immer einen Schritt voraus zu sein. Unsere zuverlässige Cloud-First-Lösung wurde entwickelt, um die IT-Komplexität zu reduzieren und gleichzeitig Schulen dabei zu helfen, Tools zu konsolidieren, Sicherheitsoperationen zu optimieren und die Beschaffung zu vereinfachen.

Mit integrierter, KI-gestützter Bedrohungserkennung und -reaktion können Schulen und Institutionen die Transparenz verbessern, die Behebung beschleunigen und die manuellen Workloads reduzieren – sodass IT-Teams sich darauf konzentrieren können, das Lernen zu ermöglichen. Die Microsoft 365-Plattform basiert auf globalen Sicherheitsstandards und Zero-Trust-Prinzipien, geht von einem möglichen Sicherheitsvorfall aus und überprüft Zugriffe explizit, um eine widerstandsfähige Verteidigung sicherzustellen, die sich flexibel an die Anforderungen jeder Campusumgebung anpasst.

Jede Ebene unseres Ansatzes wird von der Secure Future Initiative (SFI) geleitet

- **Von Grund auf sicher:** Sicherheit steht bei der Entwicklung jedes Produkts oder Diensts an erster Stelle. Das UX Toolkit von SFI hilft, auf Benutzende abzielende Angriffe zu reduzieren, indem es die Standardsicherheitsfunktionen verbessert und die Reibung verringert. Es wurde von Produktteams der Bereiche Windows, Azure und Defender übernommen.
- **Standardmäßig sicher:** Sicherheitsmaßnahmen sind standardmäßig aktiviert, werden standardmäßig erzwungen, erfordern keinen zusätzlichen Aufwand und sind nicht optional. Microsoft 365 Copilot Control System (CCS), Windows Smart App Control und durchgesetzte MFA für Azure und Microsoft Entra ID zeigen, wie Sicherheitseinstellungen aktiviert und gepflegt werden.
- **Sicherer Geschäftsbetrieb:** Sicherheitskontrollen und -überwachung werden verbessert, um aktuelle und zukünftige Bedrohungen abzuwehren. Mit automatisierter Erkennung, Betrugsprävention und integrierter Richtlinienumsetzung stärkt SFI den sicheren Geschäftsbetrieb durch effektiven Schutz in der Praxis.

Sichere Lernumgebungen ermöglichen

Microsoft setzt sich dafür ein, Institutionen bei der Schaffung sicherer, geschützter und inklusiver Lernumgebungen zu unterstützen, um die Daten der Lernenden zu schützen, Cyberbedrohungen zu minimieren und die IT-Verwaltung zu vereinfachen.

- **Gerätehärtung und Identitätsschutz:** Stärken Sie Umgebungen mit den integrierten Funktionen von Windows 11, stellen Sie den Identitätsschutz durch Entra ID sicher und modernisieren Sie Systeme mit Lösungen wie Intune und Defender XDR.
- **Endpunkt- und Appschutz:** Schützen Sie Geräte von Lernenden, unterstützen Sie die Einhaltung von Compliance und sichern Sie den Zugriff auf Apps in der Cloud und auf Endpunkten mit Intune und Defender for Cloud Apps.
- **Betriebssystemschutz:** Nutzen Sie die integrierten Sicherheitsfunktionen von Windows 11, wie Smart App Control, virtualisierungsbasierte Sicherheit und Kernelmodus-Schutz, um eine sichere Grundlage für Lernumgebungen zu schaffen.
- **Hardwarebasierte Schutzmaßnahmen:** Fördern Sie die Geräteintegrität mit Hardwarefunktionen wie TPM 2.0 und dem Microsoft Pluton-Sicherheitschip, die Daten schützen und sicheres Booten sowie Verschlüsselung unterstützen.

„Microsoft basiert auf Vertrauen, und Vertrauen muss verdient und aufrechterhalten werden. Unser Versprechen an unsere Kunden und unsere Community besteht darin, Ihre Cybersicherheit über alles andere zu stellen.“

— Charlie Bell,
EVP, Security bei Microsoft

Entdecken Sie im [Windows Security Book](#), wie Microsoft Bildungseinrichtungen bei der Schaffung sicherer, vertrauenswürdiger Lernumgebungen unterstützt. Entdecken Sie bewährte Methoden, Tools und Strategien, um die Sicherheit zu stärken und die Sicherheit der Lernenden auf breiter Basis zu unterstützen.

Gemeinsame Herausforderungen in K-12 und Hochschulen

Identitätssicherheit

K-12	HOCHSCHULEN	MICROSOFT-LÖSUNG
Geräteflexibilität: Sichere Multi-Faktor-Authentifizierung für 1:1- oder gemeinsam genutzte Geräte Gemischte Umgebungen: Persönliche Geräte von Lernenden und gemeinsam genutzte Klassenzimmercomputer Überlegungen zum Alter: Altersentsprechende Authentifizierung für alle Klassenstufen	Hohe Fluktuation von Benutzenden: Fortlaufende Einschreibungen und Abschlüsse Externe Partner: Gäste, Anbietende, Forschende Mehrere Abteilungen: Getrennte Schulen und Colleges Alumni-Zugang: Fortlaufende Kontakte zu Absolvierenden Komplexe Anmeldeinformationen: Verwaltung aller Anmeldungen und Berechtigungen	Entra ID • Zertifikatbasierte Autorisierung • Richtlinie für bedingten Zugriff • Externe Identitäten • FIDO 2 Schlüssel • Multi-Tenant-Organisationen • Temporärer Zugangspass • Lebenszyklusrichtlinien für Benutzende/Gruppen • Bestätigte Anmeldeinformationen • Windows Hello School Data Sync (SDS)

Datensicherheit und Compliance

K-12	HOCHSCHULEN	MICROSOFT-LÖSUNG
Schutz von Studierendendaten: Studierendendaten schützen als gesetzliche Pflicht Länderübergreifende Compliance: Hilft, die Einhaltung von Vorschriften in mehreren Ländern zu erfüllen	Schutz vertraulicher Daten: Schützen Sie vertrauliche Forschungs-, Gesundheits-, Zulassungs- und Finanzdaten Länderübergreifende Compliance: Hilft, die Einhaltung von Vorschriften in mehreren Ländern zu erfüllen Verhindern von Insider-Bedrohungen: Insider-Bedrohungen verhindern	Purview • DLP • Informationsbarrieren • Informationsschutz • Insider-Bedrohungsschutz Security Copilot

Compliance-Anforderungen

K-12	HOCHSCHULEN	MICROSOFT-LÖSUNG
Regulatorische Compliance: Hilft bei der Erfüllung der Anforderungen von FERPA, HIPAA, DSGVO und EU KI Act und der Aufbewahrungspflichten für Daten	Regulatorische Compliance: Hilft bei der Erfüllung der Anforderungen von FERPA, HIPAA, Title IX, GBLA, DSGVO und EU KI Act	Entra ID • Prüfung und Berichterstattung Security Copilot Purview • Communication Compliance • DLP • eDiscovery • Informationsbarrieren • Informationsschutz • Datensatzverwaltung

Sicherheitsmanagement

K-12	HOCHSCHULEN	MICROSOFT-LÖSUNG
Ressourcenbeschränkungen: Begrenzte technische Ressourcen und Personal verwalten Angriffsreaktion: Auf eine hohe Anzahl von Cyberangriffen reagieren Versicherungsanforderungen: Erfüllen Sie die Anforderungen an den Cyber-Versicherungsschutz	Dezentralisierte IT: Dezentrale IT-Umgebungen verwalten Budgetbeschränkungen: Begrenztes Budget und fehlende Sicherheitsexpertise angehen Programme für Studierende: SOC-Programme für Studierende einführen	Defender XDR Security Copilot Sentinel

Gerätesicherheit

K-12	HOCHSCHULEN	MICROSOFT-LÖSUNG
Gerätezugriff: Sicheren Zugriff für 1:1-Geräte und gemeinsam genutzte Geräte bereitstellen Einhaltung der Vorschriften des Schulbezirks: Unterstützen Sie die Geräte-Compliance in großen Schulbezirken Bedrohungsschutz: Vor Schadsoftware und unbefugtem Zugriff schützen	Zugriff auf persönliche Geräte: Sicheren Zugriff für persönliche Geräte bereitstellen Vermeiden von Datenschutzverletzungen: Verhindern Sie Datenschutzverletzungen und Schadsoftware Compliance-Anforderungen: Unterstützt die Einhaltung von Geräte-Compliance-Anforderungen	Defender für Endpunkt • EDR-Richtlinien • Netzwerkschutz • Webinhaltsfilterung Entra ID • Bedingter Zugriff mit Geräte-Kompatibilität • Internetzugriff und privater Zugriff • Webinhaltsfilterung Intune • Richtlinien für den Schutz von Apps • Richtlinie zur Gerätekonformität Purview • DLP für den Datenaustausch

App-Sicherheit

K-12	HOCHSCHULEN	MICROSOFT-LÖSUNG
M365-Bereitstellung: Sichere M365-Apps für Studierende bereitstellen Richtlinienverwaltung: Plattform- und App-Sicherheitsrichtlinien verwalten Bedrohungsschutz: Gegen Phishing- und Malware-Angriffe in Apps schützen	Multi-Cloud-Umgebungen: Sichere Multi-Cloud- und Multiplattform-Umgebungen betreiben Hybride Sicherheit: Daten On-Premises verwalten und Cloud-App-Sicherheit Identitätsföderation: Föderierte und mehrinstanzenfähige Identitäten unterstützen	Defender • Defender for Cloud – Apps • Defender for Identity • Defender for Office 365 Purview • SharePoint-Richtlinien Entra ID • Identitätsverbund • Multi-Tenant-Organisationen • Gruppen- und Teams-Richtlinien Sentinel

K-12	HOCHSCHULEN	MICROSOFT-LÖSUNG
Sicherer KI-Zugriff: Lernenden einen sicheren KI-Zugang ermöglichen Missbrauchsprävention: Auf Bedenken hinsichtlich KI-Missbrauch und Informationszugriff eingehen Schutz der Kommunikation: Schützen Sie Kommunikation und vertrauliche Daten mit KI-Tools	Fortschrittliche Bedrohungsabwehr: Abwehr komplexer und skalierbarer KI-gesteuerter Angriffe Verhindern von Insider-Bedrohungen: Verhindern, dass Insider KI für den Datenzugriff ausnutzen Erweiterte Zugriffssicherheit: Datensicherheit stärken, während KI den Zugriff erweitert	Copilot • Unternehmensdatenschutz • Einstellungen für Schutz und Sicherheit Defender XDR • Bedrohungsüberwachung Sentinel Purview • Communication Compliance • DLP-Richtlinie • Informationsbarrieren • Informationsschutz • Insider-Bedrohungsschutz • Security Copilot

Navigieren in diesem Sicherheitstoolkit

Das Microsoft Education Sicherheits-Toolkit hilft Führungskräften im Bildungsbereich in Schulen, Institutionen, lokalen und regionalen Abteilungen sowie Bildungsministerien, ihre IT-Umgebungen zu vereinfachen und abzusichern und sichere sowie innovative Lernerfahrungen zu ermöglichen. Indem sie eine einzige, integrierte Microsoft-Sicherheitsplattform, KI-gestützte Bedrohungserkennung und Zero-Trust-Prinzipien nutzen, können Schulen und Institutionen die IT-Komplexität reduzieren, die Reaktion auf Vorfälle beschleunigen und Lernende, Lehrkräfte sowie Forschung schützen.

Unterteilt in fünf Abschnitte – [Übersicht](#), [Kundschaftserlebnisse](#), [Planung](#), [Implementierung](#) und [Auswirkungen](#) können Sie mithilfe der Navigationsregisterkarten auf der rechten Seite des Toolkits ganz einfach Rahmenwerke, Richtlinien, Praxisbeispiele und bewährte Strategien erkunden, die Sie vom Verständnis der Sicherheitslandschaft bis zur erfolgreichen Implementierung begleiten.



Microsoft 365 Copilot verwenden

Microsoft 365 Copilot fungiert als Ihr KI-Assistent und hilft Ihnen, sich in Sicherheitsdokumentationen zurechtzufinden und Möglichkeiten mithilfe von Eingaben in natürlicher Sprache zu erkunden. Fordern Sie Copilot auf, unbekannte Sicherheitskonzepte zu erläutern, komplexe Implementierungsschritte in überschaubare Phasen zu unterteilen oder Tools und Ressourcen zu identifizieren, die auf Ihre Umgebung zugeschnitten sind. Egal, ob Sie Sicherheitsfachkraft sind oder gerade erst anfangen – Microsoft 365 Copilot hilft Ihnen, die Dokumentation mit Klarheit und Selbstvertrauen zu navigieren.

Wählen Sie den richtigen Ausgangspunkt aus

Navigieren Sie direkt zu den Abschnitten, die für Ihre aktuellen Anforderungen am relevantesten sind:

- **Neu bei der Sicherheit im Bildungsbereich?** Beginnen Sie mit dem **Abschnitt Übersicht**, um die Sicherheitsvision von Microsoft zu verstehen und zu erfahren, warum Sicherheit heute wichtiger denn je ist.
- **Entwickeln Sie Ihre Strategie?** Verwenden Sie die im **Abschnitt „Plan“** bereitgestellten Frameworks, um Lücken zu identifizieren und die Sicherheit an Ihren institutionellen Zielen auszurichten.
- **Entwickeln Sie den Fall Ihrer Institution?** Entdecken Sie den **Abschnitt „Kundenreferenzen“**, um zu sehen, wie andere Bildungseinrichtungen mit Microsoft-Lösungen messbare Ergebnisse erzielen.
- **Stellen Sie Lösungen bereit?** Der **Abschnitt „Implementieren“** bietet ausführliche Anleitungen zu Microsoft-Sicherheitslösungen und bewährten Praktiken.
- **Blicken Sie in die Zukunft?** Besuchen Sie den **Forschungsbereich** für die neuesten Microsoft Insights, Branchenerkenntnisse und akademische Forschung zur Bildungssicherheit.

Dieses Toolkit dient sowohl als umfassender Leitfaden als auch als praktisches Arbeitsbuch. Verwenden Sie die Bewertungsvorlagen, Checklisten und Frameworks, um ein Programm zu entwickeln, das Ihre Institution schützt und gleichzeitig Innovation ermöglicht. Sicherheit ist mehr als nur Schutz – sie befähigt Ihre Institution dazu, die digitale Transformation, den Einsatz von KI und innovative Lehrmethoden, die die moderne Bildung prägen, selbstbewusst zu nutzen.

Kundenerlebnisse erkunden

Erfahren Sie, wie Schulen und Institutionen ihren Sicherheitsstatus mit Microsoft erfolgreich gestärkt haben. Von den Onslow County Schools, die Sicherheit mit Lernzugang in Einklang bringen, bis zur Oregon State University, die ein von Lernenden geleitetes Security Operations Center aufbaut – diese Erfahrungen bieten verwertbare Erkenntnisse, die Ihre eigene Sicherheitsstrategie informieren können. Nutzen Sie diese Erkenntnisse, wenn Sie Implementierungsstrategien erkunden, gemeinsame Herausforderungen angehen und den Wert für Stakeholder aufzeigen.

Erste Schritte mit Sicherheitsbewertungen

Im gesamten Sicherheitstoolkit finden Sie praktische Übungen und Bewertungsaufgaben, um den Sicherheitsstatus Ihrer Schule oder Bildungseinrichtung zu bewerten. Diese Tools unterstützen Sie dabei, Lücken zu identifizieren, Verbesserungen zu priorisieren und eine Roadmap für umfassenden Schutz zu erstellen. Beginnen Sie mit der Überprüfung Ihrer aktuellen Abdeckung bei der Geräte- und App-Verwaltung, der Datenschutzfunktionen in Cloud- und On-Premises-Umgebungen sowie der Einhaltung lokaler, bundesstaatlicher und globaler Datenschutzbestimmungen.



[Copilot-Prompt](#)

Agieren Sie als Sicherheitsadministrator für eine **[K–12/Higher Ed]**-Institution. Identifizieren Sie die häufigsten, klassifizieren Sie jede nach Schweregrad und NIST CSF-Kategorie und empfehlen Sie die spezifischen Microsoft-Tools, die sich mit jeder Lücke befassen. Fassen Sie Ihre Empfehlungen in einer Tabelle zusammen und listen Sie auf, welche zusätzlichen Informationen Sie von mir benötigen, um die Bewertung zu optimieren.

TIPP

Teilen Sie Elemente wie Sicherheitsbewertungsergebnisse, aktuelle Vorfälle oder Systeme mit hohem Risiko. Mit konkreten Signalen kann Copilot Lückenanalysen erstellen, die sich auf Ihre reale Umgebung stützen, anstatt auf allgemeine Annahmen.

Sichereres Lernen ermöglichen mit den Microsoft-Sicherheitstools

Cybersicherheit in der Bildung bedeutet mehr als nur Schutz – sie ermöglicht sicheres und robustes Lernen. Schulen und Institutionen operieren in besonders wertvollen und anfälligen Umgebungen, in denen personenbezogene Daten, Forschung und digitale Tools täglich zusammentreffen. Mit der Ausweitung des digitalen Lernens wachsen auch die Herausforderungen – und die Chancen, Vertrauen, Zugang und institutionelle Widerstandsfähigkeit zu stärken.

Microsoft Security bietet Schulen und Institutionen eine integrierte Sicherheitslösung, die speziell für die Bildung entwickelt wurde und auf Zero Trust- sowie Secure-by-Design-Prinzipien basiert, um den Vorsprung zu behalten. Unsere KI-basierten Lösungen vereinfachen die Verwaltung, unterstützen skalierbare Abläufe und bereiten Teams auf die Zukunft vor. Sicherheit ist eine strategische Priorität, die das Lernen schützt, die Mitarbeitenden befähigt und Vertrauen in der Bildungsgemeinschaft aufbaut.

Konkrete Wirkung im Bildungsbereich

Wie Schulen und Institutionen Sicherheit in eine Chance verwandeln.

- **Strategische Wegbereiter:** Nutzen Sie Sicherheit, um digitales Lernen zu beschleunigen, Chancengleichheit zu fördern und die Entwicklung von Fachkräften zu unterstützen.
- **Vertrauensaufbauende:** Stärken Sie das Vertrauen in den Zugang für Studierende, das Engagement von Alumni und den Ruf Ihrer Institution.
- **Vereinfacher des Betriebs:** Minimieren Sie Störungen und automatisieren Sie Reaktionsprozesse mit integrierten Tools und intuitiven Dashboards.
- **Karriere-Starter:** Bereiten Sie Lernende durch praxisnahe Erfahrungen und studentische Security Operations Centers (SOCs) auf Karrieren im Bereich Cybersicherheit vor.
- **Wachstumsförderer:** Skalieren Sie mit flexiblen Cloud-First-Lösungen den Schutz in Lehr- und Forschungsumgebungen sowie Lernumgebungen.
- **Resilienztreiber:** Entwickeln Sie die institutionelle Readiness mit Secure-by-Default- und Secure-by-Design-Lösungen, die auf Zero Trust basieren.
- **Innovationskatalysator:** Befähigen Sie Lehrkräfte und IT-Teams, neue Technologien mit Vertrauen zu übernehmen, unterstützt durch integrierte Compliance und Sicherheit.

Tools

In diesem Abschnitt

Microsoft-Sicherheitstools



Microsoft-Sicherheitstools

Sicherheitslösungen im Bereich Bildung navigieren

Microsoft bietet umfassende Sicherheitstools, die auf die Bedürfnisse von Bildungseinrichtungen zugeschnitten sind. Damit Sie den Zweck jedes Tools und dessen Einbindung in Ihren Workflow rasch erfassen können, haben wir prägnante Zusammenfassungen und sorgfältig ausgewählte Tools in jeder Kategorie bereitgestellt.

Ganz gleich, ob Sie Geräte von Lernenden absichern, Compliance-Vorgaben erfüllen oder Ihr Team auf zukünftige Cybersicherheitsherausforderungen vorbereiten: Der integrierte Ansatz von Microsoft bietet flexible, kosteneffiziente Sicherheit, die speziell auf die Anforderungen der Bildung zugeschnitten ist.



Windows 11-Sicherheit

Bieten Sie Studierenden, Lehrkräften und Mitarbeitenden umfassenden Sicherheitsschutz vom Chip bis zur Cloud mit hardwarebasierten Schutzmaßnahmen, die vor Bedrohungen schützen.

FUNKTIONEN

- Sicherer Kern-PC-Schutz
- Windows Hello – kennwortlose Authentifizierung
- BitLocker-Verschlüsselung
- Microsoft Defender Antivirus (integriert)
- Intelligente App-Steuerung
- Copilot+ PC-KI-Sicherheit auf dem Gerät



Microsoft Security Copilot

Schützen Sie Ihre Einrichtung mit der Geschwindigkeit und der Skalierbarkeit von KI – mit einem generativen KI-gestützten Assistenten für den täglichen Betrieb in den Bereichen Sicherheit und IT.

FUNKTIONEN

Zusätzliche Security Copilot-Agents arbeiten mit Defender, Entra, Purview, Intune, Sentinel und Drittanbieter-Tools zusammen.



Microsoft Defender

Erkennen und reagieren Sie auf Angriffe auf Ihre Geräte, Identitäten, Apps, E-Mails und Clouds mit führenden XDR-Produkten (Extended Detection and Response).

FUNKTIONEN

- Defender XDR
- Defender for Office 365
- Defender für Endpunkt
- Defender for Identity
- Defender for Cloud Apps

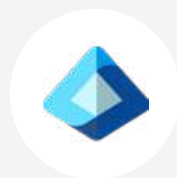


Microsoft Purview

Schützen Sie Daten überall dort, wo sie sich befinden, mit einer Sammlung einheitlicher Produkte für Informationsschutz, Governance und Compliance.

FUNKTIONEN

- Informationsschutz
- Verhinderung von Datenverlust
- Insider-Risikomanagement
- Communication Compliance
- Informationsbarrieren
- Data Governance: Data Map und Einheitlicher Katalog
- eDiscovery
- Data Lifecycle Management
- Compliance Manager
- Datensicherheitsmanagement (Data Security Posture Management, DSPM) für KI



Microsoft Entra

Verifizieren Sie jede Identitäts- und Zugriffsanforderung in Ihren Clouds, Plattformen und Geräten mit einer Sammlung von Identitäts- und Zugriffsprodukten. Verfügbar als Teil der Entra Suite für Bildung.

FUNKTIONEN

- Entra ID
- Bedingter Zugriff
- ID-Schutz
- Externe ID
- ID-Governance
- Privileged Identity Management
- Entra-Domänendienste
- Geprüfte ID



Microsoft Intune

Verbessern Sie die Gerätesicherheit und sorgen Sie für reibungslose Workflows mit Lösungen zur Endpunktverwaltung.

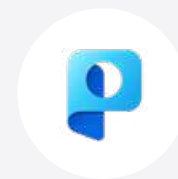
FUNKTIONEN

- Intune for Education
- Windows Autopilot
- Verwaltung mobiler Anwendungen (MAM)
- Gerätekonformität
- Verwaltung von Endpunktberechtigungen



Microsoft Sentinel

Erhalten Sie unübertroffene Transparenz über Bedrohungen mit einer SIEM-Lösung (Security Information and Event Management), die einen einheitlichen Data Lake für kosteneffiziente Langzeitaufbewahrung und fortschrittliche Analysen umfasst.



Microsoft Priva

Respektieren Sie die Privatsphäre von Lernenden und Mitarbeitenden mit proaktivem Risikominderungs- und Compliance-Management, das Schulen dabei unterstützt, FERPA-, DSGVO- und andere Datenschutzerfordernungen zu erfüllen.

FUNKTIONEN

- Privacy Risk Management
- Subject Rights Requests

Campus- Erfolgsgeschichten

In diesem Abschnitt

[Sicherung von Lernumgebungen: K-12-
Campus-Erfolgsgeschichten](#)

[Innovationen im Bereich der Sicherheit in
der Hochschulbildung in der Praxis](#)

[Weitere Kundensicherheitsreferenzen](#)



Sicherung von Lernumgebungen: K-12-Campus-Erfolgsgeschichten

Ganz gleich, ob sie Hunderttausende von Geräten verwalten, Sicherheit und Bildungszugang in Einklang bringen oder vertrauliche Daten mit begrenzten IT-Ressourcen schützen müssen – K-12-Schulbezirke stehen vor komplexen Sicherheitsherausforderungen. Erfahren Sie, wie drei führende Schulen ihren Sicherheitsansatz mit Microsoft-Lösungen transformiert haben.





Die New York City Public Schools setzten Microsoft Intune ein, um mehr als 750.000 Geräte in 1.800 Schulen innerhalb weniger Tage zu verwalten.

Herausforderung

Als COVID-19 auf Online-Unterricht umstellte, sahen sich die New York City Public Schools einer außergewöhnlichen Herausforderung gegenüber: Bereitstellung und Verwaltung von Geräten für über 750.000 Lernende in wenigen Tagen statt in mehreren Monaten.

Die New York City Public Schools entschieden sich aufgrund der plattformübergreifenden Möglichkeiten und der Kosteneffizienz für Microsoft Intune, da es bereits in ihren Microsoft 365 Education-Lizenzen enthalten war. Der Schulbezirk stellte 550.000 LTE-fähige iPads und 200.000 Chromebooks bereit und gab dabei Lernenden in temporären Unterkünften sowie solchen ohne Internetzugang Vorrang. In enger Zusammenarbeit mit dem Intune-Team von Microsoft verkürzten sie eine sechsmonatige Implementierung auf nur wenige Tage, mit täglichem – manchmal stündlichem – Support während kritischer Bereitstellungsphasen.

Wirkung

Die Auswirkung war unmittelbar und dauerhaft. Intune ermöglichte eine zentralisierte Verwaltung für alle Gerätetypen, beseitigte die Notwendigkeit der physischen Softwareverteilung und ermöglichte stille, transparente Updates, die Störungen im Lernprozess minimierten.

Heute nutzen die New York City Public Schools weiterhin Intune, um Bereitstellungen zu automatisieren, digitale Prüfungen stadtweit zu unterstützen und den Gerätezustand sowie die Gerätesicherheit zu überwachen – und so den IT-Betrieb zu modernisieren und das Lernen der Lernenden zu sichern.

„Wir haben die größte Bereitstellung von LTE-fähigen Geräten in Rekordzeit initiiert. Jede Minute, in der man darauf wartet, dass ein Gerät funktioniert, ist verlorene Unterrichtszeit. Intune ermöglicht es uns, alles im Hintergrund und transparent zu verwalten und bietet eine zentrale Oberfläche, um Hunderttausende von Ressourcen zu überblicken.“

—Alexander Horwatt

Executive Director of Technology
Innovation NYC Public Schools

Wichtige Fragen

- Wie können Funktionen zur schnellen Bereitstellung von Geräten, wie die Pandemie-Reaktion von NYC PS, Ihren Bezirk auf unerwartete Störungen vorbereiten?
- Welche Auswirkungen hätte die zentralisierte Verwaltung verschiedener Geräteplattformen auf die Effizienz und den Sicherheitsstatus Ihres IT-Teams?
- Wie könnte die Gewährleistung, dass jeder Lernende Zugang zu vernetzten Geräten hat – unabhängig von den Umständen – die Chancengleichheit in Ihrem Schulbezirk fördern?

Microsoft-Tools

- [Microsoft 365 Education](#)
- [Microsoft Intune](#)
- [Windows Autopilot](#)

➔ [Die vollständige Kundenreferenz lesen](#)



Onslow County Schools

Onslow brachte Sicherheit und Zugang mithilfe von Microsoft Intune Endpoint Privilege Management in Einklang.

Herausforderung

Die Onslow County Schools, der 11. größte Schulbezirk in North Carolina, mussten Lernenden und Lehrkräften den Zugang zu wichtiger Bildungssoftware – einschließlich sicherer Prüfungsbrowser und Designsoftware – ermöglichen, ohne die Sicherheit zu gefährden. Wie Chief Technology Officer Jeff Pittman erklärt: „Microsoft-Technologie ist das Herzstück unserer gesamten Organisation“, aber der Schulbezirk musste strenge Sicherheitsvorgaben einhalten und gleichzeitig Innovationen fördern.

Wirkung

Durch die Einführung von Microsoft Intune Endpoint Privilege Management (EPM) auf 14.000 Geräten für die Klassen 6 bis 12 hat Onslow den Sicherheitsstatus erhöht und die Lernergebnisse verbessert. Die Lösung ermöglicht es Lernenden und Lehrkräften, genehmigte Anwendungen ohne Administratorrechte auszuführen und dabei das Prinzip der minimalen Rechte zu wahren. Seit der Einführung hat der Schulbezirk seine Microsoft-Sicherheitsbewertung nahezu verdreifacht.

Die Auswirkungen gehen über die Sicherheit hinaus. Lehrkräfte können jetzt innerhalb von 30 Minuten Zugriff auf neue Software erhalten, statt wie bisher 48 Stunden warten zu müssen. Dank der nahtlosen Cloudverwaltung über Azure kann das IT-Team von Onslow Support für Geräte leisten, unabhängig davon, ob sie sich im oder außerhalb des Netzwerks befinden, und so kontinuierliches Lernen ohne Einbußen bei der Sicherheit sicherstellen.

„Durch den Einsatz von EPM zur Ausführung des Anti-Betrugs-Browsers konnten wir die Lernergebnisse verbessern, sodass die Lernenden eine konzentriertere, sichere und gerechte Testumgebung haben.“

—Tiffany Rhodes,
Educator
Onslow County Schools

Wichtige Fragen

- Wie könnte das Ausbalancieren von Sicherheit und Bildungszugang – wie beim EPM-Ansatz von Onslow – dazu beitragen, die konkurrierenden Prioritäten Ihres Schulbezirks besser zu vereinbaren?
- Welche Auswirkungen hätte die Reduzierung der Softwarebereitstellungszeit von 48 Stunden auf 30 Minuten auf die Effektivität Ihres Lehrpersonals?
- Wie könnte die Verdreifachung Ihrer Sicherheitsbewertung bei gleichzeitiger Verbesserung der Bildungsergebnisse die Technologiestrategie Ihres Schulbezirks verändern?

Microsoft-Tools

- [Azure](#)
- [Microsoft Defender for Identity](#)
- [Windows Autopilot](#)
- [Microsoft Intune](#)
- Microsoft Intune Suite
- Microsoft Intune-Endpunkt Privilegverwaltung



[Die vollständige Kundenreferenz lesen](#)



Westminster School



Die Westminster School nutzt Microsoft Defender Experts, um die Daten von Lernenden und Mitarbeitenden auf dem Campus zu schützen.

Herausforderung

Die Westminster School stand vor wachsenden Cybersicherheit-Herausforderungen, während ein kleines IT-Team vertrauliche Daten von 1.350 Lernenden und 550 Mitarbeitenden schützte. Das Team bewältigte drei bis vier Sicherheitsvorfälle pro Woche, kämpfte mit übermäßigen falsch-positiven Warnungen und trug die kritische Verantwortung für den Schutz von Visainformationen, medizinischen Details und personenbezogenen Daten.

Westminster setzte als erste Schule in Australien auf Microsoft Defender Experts for XDR. IT-Lead Chris Rowtcliff beschreibt den Service als „eine Erweiterung unseres eigenen Teams“. Der verwaltete Dienst bietet ganzheitlichen Sicherheitsschutz mit menschlichen Fachkräften, reduziert Fehlalarme nahezu auf Null und stellt sicher, dass jede echte Bedrohung eingehend überprüft wird.

Wirkung

Diese Partnerschaft hat sich schnell bewährt. Als eine lernende Person versehentlich auf einen Malware-Link klickte, blockierte Defender Experts nicht nur die Bedrohung, sondern verfolgten sie auch bis zu einer anderen lernenden Person zurück. Durch diese Erkenntnis konnte die Schule mit pädagogischer Unterstützung reagieren, statt sich ausschließlich auf technische Lösungen zu beschränken.

Die Auswirkungen gehen über die Reaktion auf Bedrohungen hinaus. Das Team bearbeitet nun nahezu 100 % der Aufgaben, profitiert von wöchentlichen Experten-Check-ins und trägt durch kollaboratives Feedback zur Produktentwicklung bei Microsoft bei. Mit fortschrittlichen Tools und bewährtem Fachwissen hat die Schule ein sichereres Umfeld geschaffen und gleichzeitig Widerstandsfähigkeit gegen zukünftige Bedrohungen aufgebaut.

„Ich kann gar nicht genug betonen, wie viel Sicherheit und Gelassenheit uns Defender Experts for XDR verschafft hat. Wir fühlen uns so viel weniger überwältigt, weil wir wissen, dass die Schule und die Lernenden sicher sind.“

—Chris Rowtcliff,
Head of IT
Westminster School

Wichtige Fragen

- Wie könnten verwaltete Sicherheitsdienste wie Defender Experts for XDR Ihrem kleinen IT-Team dabei helfen, sich auf strategische Initiativen zu konzentrieren, anstatt von einer Alarmflut überfordert zu werden?
- Welchen Mehrwert würden „Fachkräfte auf Abruf“ Ihrer Schule bieten, um aus Vorfällen zu lernen und zukünftige Bedrohungen zu verhindern?
- Wie könnte die Reduzierung von Sicherheitswarnungen auf nahezu null die Effektivität und das Wohlbefinden Ihres IT-Teams verändern?

Microsoft-Tool

- [Microsoft Defender](#)

➔ [Die vollständige Kundenreferenz lesen](#)

Innovationen im Bereich der Sicherheit in der Hochschulbildung in der Praxis

Vom Schutz vertraulicher Forschungsdaten bis zur Sicherung globaler Studierendenschaften stehen Hochschulen vor einzigartigen Sicherheitsherausforderungen, die innovative Lösungen erfordern. Erfahren Sie, wie drei führende Universitäten ihren Sicherheitsstatus transformiert und gleichzeitig ihren Bildungsauftrag vorangebracht haben.





Oregon State University



Die Oregon State University implementierte Microsoft Sentinel und Microsoft Defender, um Forschungsdaten zu schützen und die Erkennungsgeschwindigkeit von Wochen auf Minuten zu verkürzen.

Herausforderung

Im Jahr 2021 bedrohte ein schwerwiegender Cybersicherheitsvorfall die kritischen Forschungsdaten der OSU und unterstrich die dringende Notwendigkeit, ihren Ruf als R1-Forschungseinrichtung zu schützen. Chief Information Security Officer David McMorries merkt an: „Wir möchten ein Umfeld schaffen, in dem Wissenschaft, Lernen und Forschung sicher in einer Cyber-Umgebung durchgeführt werden können.“

Wirkung

Die OSU implementierte Sentinel und Defender mit Microsoft 365 Education-Lizenzen, um SOC zu ihrer Sicherheitsgrundlage zu machen. Mit Microsoft-Entwicklungssupport erreichte OSU innerhalb von zwei Jahren ein Sicherheitsniveau, für das normalerweise fünf Jahre erforderlich gewesen wären. Tausende von Vorfällen wurden auf etwa 30 pro Tag reduziert, und die Erkennungszeiten verkürzten sich von Wochen auf Minuten. Sentinel wurde zu ihrem „revolutionären“ zentralen Dashboard für die Bedrohungsabwehr.

OSU hat außerdem Microsoft Security Copilot integriert, um ihr von Studierenden betriebenes SOC zu befähigen. Studentische Analysten nutzen KI, um anspruchsvolle Abfragen zu formulieren und Prozesse zu automatisieren. Dabei erwerben sie Fähigkeiten für die Berufspraxis und schützen gleichzeitig die Forschungsarbeit. Diese doppelte Mission – die Sicherung von Forschung bei gleichzeitiger Ausbildung zukünftiger Cybersicherheitsfachkräfte – verdeutlicht das Engagement der OSU für Schutz und Bildung.

„Microsoft Copilot for Security wird ein hervorragendes Lehrtool für die Studierenden sein, die im SOC der OSU arbeiten.“

—Emily Longman
Security Operations Center Manager
– Oregon State University

Wichtige Fragen

- Wie könnten von Studierenden unterstützte Security Operations, die durch KI-Tools wie Copilot for Security verbessert werden, sowohl Ihre Sicherheitsanforderungen als auch Ihre Ziele in der Personalentwicklung adressieren?
- Welche Auswirkungen hätte es auf den Schutz Ihrer vertraulichen Forschungs- und Studierendendaten, wenn sich die Erkennungszeit für Sicherheitsvorfälle von Wochen auf Minuten verkürzen ließe?
- Inwiefern könnte das Erreichen von „fünf Jahren Reife in zwei Jahren“ die Fähigkeit Ihrer Institution, offene Zusammenarbeit mit robuster Sicherheit in Einklang zu bringen, grundlegend verändern?

Microsoft-Tools

- [Microsoft Sentinel](#)
- [Microsoft Defender](#)
- [Microsoft Security Copilot](#)
- [Microsoft Entra ID](#)
- [Microsoft 365 Education](#)

→ [Die vollständige Kundenreferenz lesen](#)



Die RMIT University hat Microsoft Entra Verified ID eingeführt, um 95.000 Studierenden weltweit sofortige digitale Berechtigungsnachweise bereitzustellen.

Herausforderung

Die RMIT University, die 95.000 Studierende in 230 Ländern betreut, erkannte die Notwendigkeit, die Vergabe von digitalen Berechtigungsnachweisen für Studierende in einer zunehmend digitalen Welt zu verbessern. Wie Enterprise Architect Ajay Radhakrishnan erläutert, konzentrierten sie sich auf die „verpassten Chancen“ in der Identitätstechnologie und betonten gleichzeitig die Bedeutung von Verbindungen für lebenslanges Lernen. Die Herausforderung: Erstellung sicherer, überprüfbarer digitaler Nachweise, die internationalen Datenschutzbestimmungen entsprechen und gleichzeitig die 14-tägige Wartezeit auf physische Ausweise verkürzen.

Das Blockchain Innovation Hub der RMIT ist eine Partnerschaft mit Microsoft eingegangen, um Entra Verified ID zu implementieren und drei Anwendungsfälle zu entwickeln: Zugang der Studierenden zur Bibliothek und zu Campus-Rabatten, Alumni-Transkripte für Bewerbungen und verifizierbare Schulungszertifikate.

Wirkung

Der Pilotversuch zeigte, dass digitale Nachweise innerhalb von Sekunden statt in 14 Tagen ausgestellt werden konnten. Studierende verwalten jetzt ihre eigenen digitalen Nachweise über mobile Geräte und greifen mit einem einzigen QR-Code auf sämtliche Dienste zu – von Bibliotheksservices bis hin zur zukünftigen Beschäftigungsüberprüfung. Die Lösung baut auf der bestehenden Azure AD-Infrastruktur von RMIT auf und unterstützt offene Standards zur zukünftigen Interoperabilität mit anderen Partnern.

„Die COVID-19-Pandemie hat diesen Bedarf wirklich beschleunigt, weil wir nicht wollten, dass die Studierenden auf den Campus kommen, um ihre Ausweise abzuholen.“ Wir haben verifizierte Microsoft Entra-ID verwendet, um den Prozess zu digitalisieren und viele Effizienzgewinne zu erzielen.“

—**Michael Fairbairn**,
Associate Director des
Blockchain Innovation Hub der
RMIT University

Wichtige Fragen

- Wie könnten sofortige, Blockchain-verifizierte digitale Nachweise die Studierendenerfahrung Ihrer Institution von der Einschreibung bis zum Alumni-Engagement verändern?
- Welche betrieblichen Effizienzgewinne könnten sich aus der Abschaffung physischer Ausweise ergeben, während gleichzeitig die Sicherheit und Compliance über globale Jurisdiktionen hinweg verbessert werden?
- Wie könnten von Studierenden kontrollierte, übertragbare Nachweise, die mit breiteren Infrastrukturen verbunden sind, einen Wert schaffen, der über die traditionellen Campusgrenzen hinausgeht?

Microsoft-Tools

- [Microsoft Entra ID](#)
- Microsoft Entra Verified ID

[→ Die vollständige Kundenreferenz lesen](#)

University of Venda



Die südafrikanische University of Venda migrierte zu Azure und erreichte eine Verfügbarkeit von 99 % für 15.000 Studierende.

Herausforderung

Die University of Venda (Univen) in Südafrika mit 15.000 Studierenden stand vor erheblichen infrastrukturellen Herausforderungen. Verstreute On-Premises-Server verursachten häufige Ausfallzeiten, während sechsmonatige Beschaffungszyklen das Wachstum behinderten. Wie CIO Sam Khoza erklärt, bestand ihre Mission darin, „die Strategie der Universität durch moderne Technologien zu unterstützen“, um weltweit wettbewerbsfähige Personen mit Abschluss hervorzubringen.

Wirkung

Univen hat 18 Kernsysteme mit Microsoft Unified Support zu Microsoft Azure migriert. Die Migration umfasste das Dokumentverwaltungssystem, die HR- und Finanzplattformen sowie das Moodle LMS. Die Ergebnisse ließen nicht lange auf sich warten. Die Serviceverfügbarkeit stieg auf 99 %, und es gab keinerlei Berichte über Systemunzugänglichkeit, selbst während der Stoßzeiten der Prüfungen.

Univen gehörte außerdem zu den ersten Universitäten in Afrika, die Security Copilot zusammen mit Sentinel, Defender und Purview implementierten. Khoza merkt an: „Als eine der ersten Universitäten in Afrika, die Microsoft Security Copilot implementiert haben, nehmen wir eine Vorreiterrolle im Bereich KI-gestützte Sicherheit ein.“ Wir profitieren nun von einer schnelleren Bedrohungserkennung, intelligenteren Reaktionen und größerem Vertrauen. Die Partnerschaft mit Microsoft Unified Support stellte Technologie bereit und entwickelte interne Kompetenzen, wodurch das IKT-Team in die Lage versetzt wurde, komplexe Aufgaben zu bewältigen und Innovationen voranzutreiben.

„Was früher ein halbes Jahr für die Bereitstellung brauchte, kann jetzt auf Azure ganz einfach innerhalb weniger Stunden abgeschlossen werden.“

—Vusani Nengovhela

Server Engineer

University of Venda

Wichtige Fragen

- Wie könnte die Verkürzung der Bereitstellungszeit von sechs Monaten auf wenige Stunden die Reaktionsfähigkeit Ihrer Institution auf Bildungsbedürfnisse verändern?
- Welche Auswirkungen hätte eine Dienstverfügbarkeit von 99 % auf das Lernerlebnis Ihrer Lernenden und die Produktivität Ihrer Mitarbeitenden?
- Wie könnte die Rolle als regionaler Pionier im Bereich KI-gestützte Sicherheit Ihre Institution als Technologieführer positionieren und gleichzeitig kritische Daten schützen?

Microsoft-Tools

- [Microsoft 365 for Education](#)
- [Azure](#)
- [Microsoft Sentinel](#)
- [Microsoft Security Copilot](#)
- [Microsoft Defender](#)
- [Microsoft Purview](#)
- [Exchange Online](#)



[Die vollständige Kundenreferenz lesen](#)

Weitere Kundensicherheitsreferenzen





Memphis-Shelby County Schools

K-12 | 214 Campus | 110.000 Lernende

Lösung

Mit Power Apps und Power Automate wurden maßgeschneiderte Daten-Tools zur Datenerfassung und zum Reporting entwickelt, die die vielfältigen betrieblichen Anforderungen erfüllen und Kosten für die Einführung neuer Software eingespart haben.

Tools

Azure SQL · Power Apps · Power Automate · Dataverse · Power BI · Power Pages

[→ Vollständigen Artikel lesen](#)



Newington College

K-12 | 3 Campus | 3.200 Lernende

Lösung

Das Newington College hat sich mit Microsoft Education und Quorum zusammengetan, um umfassende Cybersicherheitslösungen zu implementieren, dazu gehören Quorums Cyber One MDR, Microsoft 365 und Intune. Dies geschah nach einem Sicherheitsvorfall, durch den deutlich wurde, dass der Schutz und die Verwaltung der Bildungstechnologie verbessert werden mussten.

Tools

Azure · Microsoft 365 Education · Microsoft Defender for Endpoint · Microsoft Defender for Identity · Microsoft Intune · Microsoft Sentinel · Microsoft Defender for Cloud

[→ Vollständigen Artikel lesen](#)



New York City Department of Education

K-12 | 1,600 Campus | 920.000 Lernende

Lösung

Als die 1,2 Millionen Lernende von New York City mit pandemiebedingten Schulschließungen und Wiedereröffnungen konfrontiert waren, stellte das Bildungsministerium schnell eine cloudbasierte Remote-Lernplattform auf Azure Synapse Analytics bereit, um eine hohe Leistung, ein optimiertes Management und Sicherheit auf Unternehmensniveau zu erreichen.

Tools

Azure · Azure Virtual Desktop · Azure Blob Storage · Azure Data Lake Storage · Azure Synapse Analytics · Microsoft 365 Education · Microsoft Teams · Microsoft Purview · Power BI · Windows 11

[→ Vollständigen Artikel lesen](#)



Orange Unified School District

K-12 | 42 Campus | 26.000 Lernende

Lösung

Der Orange Unified School District hat erfolgreich 30.000 Geräte an Lernende und Mitarbeitende bereitgestellt und dabei Microsoft 365 Education sowie Windows-PCs eingesetzt. Dadurch konnte das kleine IT-Team die Verwaltung vereinfachen, die Sicherheit stärken und die Learning-Umgebung für den zukünftigen Erfolg der Lernenden bereichern.

Tools

Microsoft 365 Education · Microsoft Entra ID · Microsoft Defender for Endpoint · Microsoft Intune · Windows Autopilot · Windows 11

[→ Vollständigen Artikel lesen](#)



Wichita Public Schools

K-12 | 90 Campus | 47.000 Lernende

Lösung

Die Wichita Public Schools, die fast 50.000 Lernende und 5.600 Lehrkräfte betreuen, prüfen derzeit den Einsatz von Microsoft Copilot mit Datenschutzfunktionen, um personalisiertere und vielfältigere Lernerfahrungen zu bieten, die auf die individuellen Bedürfnisse der Lernenden zugeschnitten sind.

Tools

Azure · Microsoft 365 Education · Microsoft Teams · Office 365 · Windows 11

[→ Vollständigen Artikel lesen](#)



Babson College

Hochschulen | 2 Campus | 3.700 Lernende

Lösung

Babson College modernisierte seine veraltete Infrastruktur durch die Implementierung von Microsoft Copilot, Azure AI und Microsoft 365 Education, um prädiktive Modelle zur Identifizierung gefährdeter Studierender zu entwickeln, KI-gestützte Lerntools wie einen Mathbot für MINT-Kurse zu erstellen und Studierende mit KI-Fähigkeiten auf ihre berufliche Zukunft vorzubereiten.

Tools

Power BI · Microsoft 365 Education · Microsoft Copilot · Azure OpenAI

[→ Vollständigen Artikel lesen](#)



Howard University

Hochschulen | 1 Campus | 11.000 Studierende

Lösung

Die Howard University, eine historisch afroamerikanische Hochschule, hat einen Ransomware-Angriff im Jahr 2021 überwunden und ihre Sicherheitsbewertung innerhalb eines Jahres verdoppelt, indem sie zu Microsoft Azure migrierte und mit Cloudforce zusammenarbeitete. Dies zeigt, wie ressourcenbeschränkte Hochschulen durch strategische Cloud-Einführung ihre Sicherheit stärken, die Effizienz steigern und Kosten einsparen können.

Tools

Azure · Azure Virtual Desktop · Microsoft Entra ID

[→ Vollständigen Artikel lesen](#)



Rowan University

Hochschulen | 6 Campus | 23.000 Lernende

Lösung

Rowan University hat ihre IT-Infrastruktur mit der Cloud-Smart-Strategie von Microsoft Azure modernisiert, was zu verbesserter Zugänglichkeit, Zuverlässigkeit und Sicherheit führte und den Professoren bis zu 50 % mehr Unterrichtszeit verschaffte. Es bestehen zudem Pläne, in KI-Technologien zu expandieren.

Tools

Azure · Microsoft 365 Education · Microsoft Intune · Microsoft Sentinel

[→ Vollständigen Artikel lesen](#)



University of Illinois Urbana-Champaign

Hochschulen | 1 Campus | 56.000 Studierende

Lösung

Die University of Illinois Urbana-Champaign hat an einem einzigen Wochenende erfolgreich 350.000 Benutzungsidentitäten mit einem personenzentrierten Ansatz zu Microsoft Azure Active Directory migriert und dabei wichtige Erkenntnisse gewonnen, die auch anderen Organisationen bei ähnlichen Herausforderungen in der Identitätsverwaltung wertvolle Hilfe bieten können.

Tools

Microsoft Entra ID

[→ Vollständigen Artikel lesen](#)



University of Washington

Hochschulen | 3 Campus | 52.000 Lernende

Lösung

Die Information School der University of Washington hat ihre Cybersicherheit-Kurslabore zu Azure Lab Services migriert und damit kostspielige lokale Geräte in flexible virtuelle Maschinen verwandelt, die den Zugriff vereinfachten, den Verwaltungsaufwand reduzierten und die Lernziele der Studierenden besser unterstützten.

Tools

Azure · Azure Lab Services · Azure Compute

[→ Vollständigen Artikel lesen](#)

Planung

In diesem Abschnitt

[Strategische Planung für
sicherere Lernumgebungen](#)

[Die aktuelle Sicherheitslage Ihres
Campus bewerten](#)

[Sicherheitsgovernance und Richtlinien](#)

[Technologiesicherheitsstrategie](#)

[Readiness der Organisation](#)

[Finanzielle und strategische Begründung](#)



Strategische Planung für sicherere Lernumgebungen

Die Sicherung Ihres Campus beginnt mit einem Plan

IT- und Sicherheitsteams Ihrer Schule sind mehr als nur Verantwortliche für Technologie – sie sind unverzichtbare Partner bei der Schaffung sicherer, widerstandsfähiger Lernumgebungen und beim Vorantreiben der Mission Ihrer Schule. Sicherheitsverantwortliche schützen nicht nur Geräte und Daten, sondern auch die Zukunft aller Lernenden und Lehrkräfte, die sie unterstützen.

Dieser Planungsleitfaden bietet einen strukturierten Ansatz für den Aufbau einer umfassenden Sicherheitsstrategie, die auf die Bildung zugeschnitten ist. Bevor Sie Microsoft Security Tools und Programme implementieren, hilft es Ihnen, Ihre Ziele abzustimmen, Ihre Umgebung zu bewerten und die wichtigsten Aspekte zu priorisieren. Egal, ob Sie die IT für eine einzelne K-12-Schule betreuen oder die Sicherheitsleitung für eine Hochschule mit mehreren Standorten und komplexen Forschungsanforderungen übernehmen – dieser Leitfaden unterstützt Sie dabei, eine solide Grundlage für effektive, skalierbare Cybersicherheit zu legen.



[Copilot-Prompt](#)

Hier ist der Link zu unserer neuesten Sicherheitsstrategie [Link einfügen].

Erstellen Sie einen Kommunikationsplan und Nachrichtenvorlagen, in denen Sie Lehrkräften und Mitarbeitenden unsere neue Sicherheitsstrategie erläutern. Fügen Sie Versionen für Lehrkräfte, Schulleitung und IT sowie FAQs zu häufigen Anliegen hinzu.

TIPP

Beschreiben Sie die Stimmung der Mitarbeitenden – ob sie sich überfordert, vorsichtig oder neugierig fühlen. Copilot kann Tonfall und Botschaften anpassen, um auf echte Bedenken einzugehen und die Akzeptanz zu fördern.

Bestimmen Sie Ihren Kurs zum sicheren Lernen

K-12-Schulbezirke legen Wert auf einfache, hochwirksame Sicherheit. Microsoft 365 A3 bietet eine zuverlässige Grundlage mit essenziellen Sicherheitsfunktionen wie Multi-Faktor-Authentifizierung (MFA), [Defender for Endpoint Plan 1](#) und [Intune](#) für die Geräteverwaltung. Diese Tools tragen dazu bei, das Lernen der Lernenden zu sichern und gleichzeitig den IT-Betrieb überschaubar zu halten.

Defender for Endpoint Plan 1 ist in Microsoft 365 A3-Lizenzen für Lehrkräfte enthalten, jedoch nicht in Student Use Benefit-Lizenzen. Für Geräte von Lernenden ziehen Sie zusätzliche Lizenzen oder alternative Schutzmaßnahmen in Betracht, je nach Ihren Sicherheitsanforderungen und Ihrem Budget.

Microsoft 365 A5 bietet erweiterte Funktionen für Bedrohungserkennung, Compliance-Management und KI-Governance, damit Schulen den sich entwickelnden Risiken einen Schritt voraus sind. Entdecken Sie den vollständigen [Funktionsvergleich](#), um die richtige Lösung für Ihre Lernumgebung zu finden.

Hochschulen stehen vor einzigartigen Herausforderungen – vom Schutz sensibler Forschung über die Verwaltung weitläufiger Multi-Campus-Netzwerke bis hin zur Einhaltung strenger regulatorischer Standards. Sie benötigen ein umfassendes Sicherheitsframework, das über verschiedene Umgebungen hinweg skalierbar ist und sich an komplexe Governance-Anforderungen anpassen kann. Die fortschrittlichen Sicherheitsangebote von Microsoft unterstützen dies mit integrierten Tools für den Identitätsschutz, die Verhinderung von Datenverlust und die sichere Zusammenarbeit – entwickelt, um den Anforderungen der Bildung gerecht zu werden.



Copilot-Prompt

Vergleichen Sie die Sicherheitsfunktionen der Microsoft 365 A3- oder A5-Lizenzen für unsere **[K-12/Higher Ed]** Umgebung, mit Fokus auf Sicherheit, Compliance, KI-Governance und Geräteverwaltung. Empfehlen Sie auf Grundlage unserer Prioritäten, welcher Plan am besten geeignet ist, und begründen Sie Ihre Empfehlung. Präsentieren Sie die Ergebnisse in einer Entscheidungsmatrix und listen Sie die wichtigsten Kriterien auf, die Führungskräfte berücksichtigen sollten.

TIPP

Beschreiben Sie die Stimmung der Mitarbeitenden. Copilot kann Tonfall und Botschaften anpassen, um auf echte Bedenken einzugehen und die Akzeptanz zu fördern.



Copilot-Prompt

Erstellen Sie einen gestaffelten Rollout-Plan über 30, 60 und 90 Tage für phishing-resistente MFA, beginnend mit administrativen Konten. Listen Sie Voraussetzungen, Change-Management-Schritte, Schulungsbedarf und Risiken auf. Identifizieren Sie, welche Benutzungsgruppen Ausnahmen oder Pilottests benötigen.

TIPP

Informieren Sie Copilot darüber, welche Benutzungsgruppen häufig Probleme mit Anmeldungen oder dem Zugriff auf Geräte haben. Dies hilft dabei, eine MFA-Einführung so zu gestalten, dass Unterrichtsstörungen minimiert und Gruppen unterstützt werden, die zusätzliche Hilfe benötigen.

Wirkungsvolle erste Schritte in der Planungsphase

PHISHING-RESISTENTE MFA AKTIVIEREN:

Aktivieren Sie die Multi-Faktor-Authentifizierung für alle Benutzenden mit [Microsoft Entra ID](#). Phishing-resistente Methoden wie Passkeys (FIDO2), Windows Hello for Business und zertifikatbasierte Authentifizierung bieten den stärksten Schutz vor Diebstahl von Anmeldeinformationen. Sie können mehr als [99,9 % der Angriffe](#) auf Konten abwehren, indem Sie die Multi-Faktor-Authentifizierung in Ihren Konten aktivieren.

PLAN FÜR DIE MFA-BEREITSTELLUNG

Erwägen Sie einen stufenweisen Ansatz, der mit Admin-Konten und Benutzenden mit hohem Risiko beginnt und dann auf die gesamte Institution ausgeweitet wird. Während MFA erhebliche Sicherheitsvorteile bietet, erfordert die Implementierung von phishing-resistenter Authentifizierung in einer Bildungseinrichtung eine sorgfältige Planung. Microsoft stellt [umfassende Bereitstellungsleitfäden](#) bereit, um Ihren Rollout zu unterstützen.

MICROSOFT DEFENDER AKTIVIEREN

Verwenden Sie [Microsoft Defender](#) und die [Microsoft Secure Score](#) Posture-Analyse als Grundlage für fortlaufende Verbesserungen.

Die aktuelle Sicherheitslage Ihres Campus bewerten

Sie können nichts schützen, von dem Sie nicht wissen, dass Sie es haben.

Der erste Schritt bei der Planung eines umfassenden Sicherheitsprogramms besteht darin, zu verstehen, wo Ihre Bildungseinrichtung derzeit steht. Dadurch können Sie neue Möglichkeiten entdecken, Ihren Bildungsauftrag durch besseren Schutz, vereinfachte Compliance und betriebliche Effizienz zu stärken.

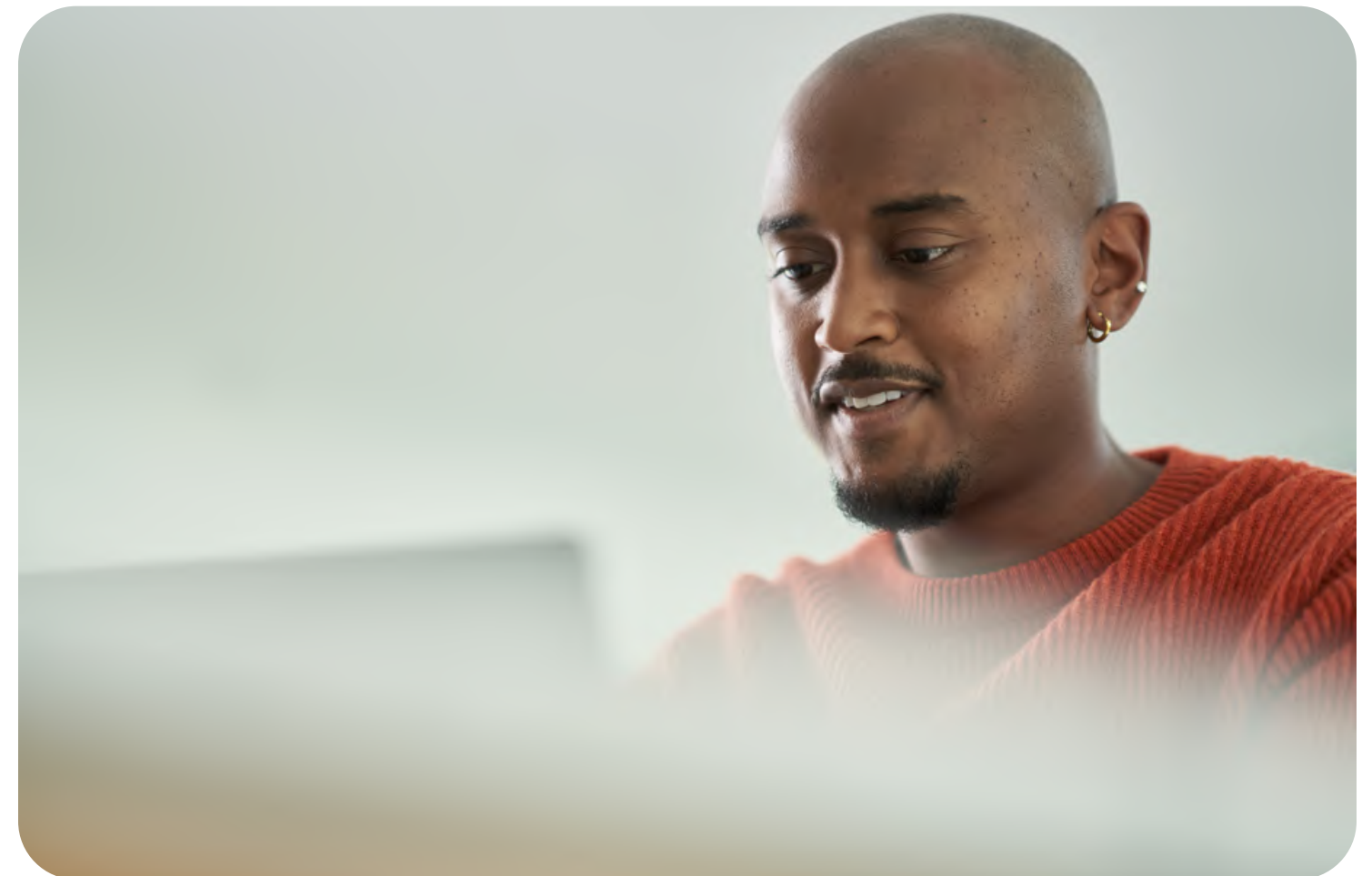
Nutzen Sie die integrierten Sicherheitslösungen von Microsoft, um Ihre Bereitschaft zu bewerten, Ihre Investitionen zu priorisieren und sofortigen Nutzen zu erzielen.

Entwickeln Sie auf den Sicherheitsgrundlagen von Windows 11 weiter

Ihre Sicherheitsstrategie beginnt auf Geräteebene. [Windows 11](#) bietet Chip-to-Cloud-Sicherheit mit integriertem Schutz:

- **Schutz durch hardwaregestützte Sicherheit:** [Verwenden Sie Trusted Platform Module \(TPM\) 2.0](#) und [Secured-Core-PC-Schutz](#), um sich vor Firmware-Angriffen und Diebstahl von Anmeldeinformationen zu schützen.
- **Kennwortlose Authentifizierung ermöglichen:** Führen Sie [Windows Hello for Business](#) mit biometrischer Authentifizierung oder PIN ein – besonders wertvoll für K-12-Lernende.
- **Anwendungen und Daten schützen:** Implementieren Sie [Smart App Control](#), um schädliche Anwendungen zu blockieren, während [BitLocker](#) Laufwerke verschlüsselt.

Organisationen, die Windows 11 verwenden, berichten von einem [Rückgang der Sicherheitsvorfälle um 62 %](#). Diese sichere Grundlage integriert sich nahtlos mit [Microsoft Intune](#) und [Defender for Endpoint](#).



Schützen Sie KI-Innovationen mit integrierten Schutzmaßnahmen

Microsoft bietet mehrschichtige KI-Sicherheitsmaßnahmen.

[Copilot+ PCs](#): Enthält gesicherten Core-Schutz und [Microsoft Pluton](#)-Sicherheitsprozessor. Neuronale Verarbeitungseinheiten (NPUs) ermöglichen die lokale KI-Verarbeitung und sorgen dafür, dass vertrauliche Daten auf dem Gerät bleiben, statt in die Cloud zu gelangen – für mehr Datenschutz.

[Microsoft 365 Copilot](#): Sicherheit auf Unternehmensniveau arbeitet automatisch:

- **Respektieren Sie vorhandene Berechtigungen:** Pflegen Sie die Zugriffssteuerungen und Vertraulichkeitsbezeichnungen Ihrer Institution.
- **Schädliche Inhalte blockieren:** Jugendgefährdender Inhalt, Gewalt, Hassreden filtern und Prompt-Injection-Angriffe verhindern.
- **Die Verschlüsselungsrichtlinien respektieren:** Wenden Sie die Verschlüsselungs- und DLP-Richtlinien von [Microsoft Purview](#) automatisch an.
- **Bewahren Sie Daten in Ihrem Mandanten auf:** Speichern Sie Eingabeaufforderungen und Antworten in Ihrer Umgebung. Ihre Daten werden [nicht zum Trainieren von KI-Modellen verwendet](#).
- **Stellen Sie Audit-Trails bereit:** Verfolgen Sie alle Copilot-Interaktionen über Microsoft Purview, um die FERPA- und COPPA-Compliance zu überwachen.

Diese Schutzmaßnahmen ermöglichen eine vertrauensvolle KI-Adoption, während gleichzeitig strenge Sicherheits- und Kinderschutzstandards eingehalten werden.

Gängige Bedrohungen erkennen

Bildungseinrichtungen sind mit einer Vielzahl von Cybersicherheitsbedrohungen konfrontiert, die den Unterricht stören und vertrauliche Daten kompromittieren können. Dazu gehören Ransomware-Angriffe, die Systeme lahmlegen, Phishing-Versuche, die auf Mitarbeitende und Studierende abzielen, Insider-Bedrohungen durch kompromittierte Konten oder missbräuchliche Zugriffe sowie staatliche Angriffe, die auf Forschung und Infrastruktur abzielen.

Das Verständnis dieser Risiken unterstützt Ihr Team dabei, Strategien mit den Gegebenheiten Ihrer Umgebung in Einklang zu bringen, damit Sie das schützen können, was am wichtigsten ist.

Machen Sie sich Gedanken zu Sicherheitsprioritäten

Verwenden Sie die Tabelle, um über Ihre Umgebung zu reflektieren und Stärken zu finden, auf denen Sie aufbauen können. Beginnen Sie Ihre Bewertung mit den folgenden Schlüsselfragen.

FRAGEN SIE

INSIGHTS

Was ist in Ihrer Umgebung am wichtigsten?

Beginnen Sie mit Ihrer wertvollsten Ressource. Dabei kann es sich um Studierendeninformationssysteme, Forschungsdaten, Finanzunterlagen und Lernmanagementplattformen handeln. Diese Systeme sind zentral für Ihre Mission und sollten besonders geschützt werden.

Wer benötigt Zugriff?

Identifizieren Sie Ihre Gruppen von Benutzenden wie Studierende, Lehrende, Mitarbeitende, Admins und externe Benutzende. Jede Gruppe hat unterschiedliche Bedürfnisse und Risikoprofile.

Was funktioniert gut?

Dokumentieren Sie bestehende Sicherheitsmaßnahmen, erfolgreiche Richtlinien und Benutzungsverhalten, die bereits positive Sicherheitspraktiken unterstützen. Bauen Sie beim Einstieg auf Ihre Stärken auf.

Betonen Sie Compliance und regulatorische Bereitschaft

Schulen mit hoher Regelkonformität stärken das Vertrauen und die Zuversicht der Gemeinschaft. Hochschuleinrichtungen sind auf Compliance angewiesen, um Prioritäten wie Medizin- und Forschungsprogramme voranzubringen. Angesichts der raschen Einführung von KI-Tools im Bildungsbereich benötigen Institutionen auch eine proaktive Governance für aufkommende Technologien.

[Microsoft Purview Compliance Manager](#) verwandelt regulatorische Komplexität in automatisierte Workflows. Ihr Team kann vorgefertigte Vorlagen verwenden, anstatt bei Null anzufangen. Dies hilft Ihnen dabei, Folgendes zu adressieren:

- K-12-Vorschriften wie FERPA für Datensätze von Lernenden, COPPA für jüngere Lernende und andere regulatorische Anforderungen.
- Im Hochschulbereich stehen Themen wie die DSGVO für internationale Studierendendaten, HIPAA-Konformität für medizinische Studiengänge und die Einhaltung von Fördermittelaufgaben im Fokus.

Vorantreiben der KI-Governance für Bildungsinnovation

[Microsoft Purview Data Security Posture Management \(DSPM\) für KI](#) bietet Transparenz und Kontrolle darüber, wie vertrauliche Bildungsdaten mit KI-Systemen wie Microsoft 365 Copilot und Drittanbietertools interagieren. DSPM für KI hilft Institutionen dabei, die Datenfreigabe in KI-Eingabeaufforderungen zu überwachen, automatisierte Schutzrichtlinien anzuwenden, Prüfpfade zu führen und riskantes Verhalten zu erkennen, bevor es Compliance-Vorfälle gibt.



Copilot-Prompt

Erstellen Sie eine FERPA- und COPPA-Compliance-Checkliste und ordnen Sie jede Anforderung den relevanten Purview-Tools (DLP, Informationsschutz, Insider-Risiko, eDiscovery) zu.

TIPP

Teilen Sie frühere Prüfungsergebnisse oder bekannte Compliance-Lücken. Copilot kann dann den Schwerpunkt der FERPA/COPPA-Checkliste auf die Bereiche legen, in denen Ihr Schulbezirk das größte Risiko hat.

Weiterentwickeln

Ihre messgestützte Bewertung schafft die Grundlage für eine strategische Sicherheitsplanung, die Ihren Bildungsauftrag unterstützt. Klare Kennzahlen zeigen Fortschritte und fördern fortlaufende Verbesserungen.

- [Microsoft Secure Score](#): Messen Sie den Sicherheitsstatus Ihrer Institution in Prozent und zeigen Sie den Fortschritt bei der Umsetzung der empfohlenen Sicherheitsmaßnahmen in Ihrer Microsoft 365-Umgebung auf.
- [Microsoft Purview Compliance Manager](#): Bewerten und verwalten Sie die Einhaltung von Vorschriften mit einem punktebasierten Bewertungssystem, das Ihren Fortschritt bei Verbesserungsaktionen in Bezug auf Bestimmungen wie FERPA und DSGVO verfolgt.

Indem Sie Ihre aktuelle Situation verstehen, legen Sie den Grundstein für eine Sicherheitsstrategie, die Ihre Institution stärkt.



Copilot-Prompt

Analysieren Sie, wie wir Microsoft Secure Score in Microsoft 365 verwenden können, um unsere Sicherheitslage zu stärken und einen Zero-Trust-Ansatz zu implementieren. Nennen Sie fünf wirksame Maßnahmen, die unsere Sicherheitsbewertung in diesem Semester verbessern. Priorisieren Sie diese Maßnahmen nach Aufwand und Wirkung, und identifizieren Sie alle Abhängigkeiten, die zuerst anzugehen sind.

TIPP

Teilen Sie Ihre wichtigsten Sicherheitsziele – wie den Schutz von Studierendendaten oder die Verkürzung der Antwortzeit für die Reaktion auf Vorfälle – mit, damit Copilot Sicherheitsbewertungs-Maßnahmen priorisieren kann, die diese Ziele direkt unterstützen.

Sicherheitsgovernance und Richtlinien

Effektive Governance macht aus reaktiver Sicherheit eine strategische. Die richtigen Frameworks optimieren Abläufe, bauen Vertrauen in der Gemeinschaft auf und richten sich nach den spezifischen Anforderungen Ihrer Institution.

Das [Cybersecurity Framework des National Institute of Standards and Technology \(NIST\)](#) bietet freiwillige Leitlinien, die viele Bildungseinrichtungen für praktische Umsetzungspfade und Risikomanagement anwenden. Für Institutionen mit [Microsoft Security Copilot](#) kann die KI-gestützte Richtlinienzuordnung dabei helfen, Ihre aktuellen Richtlinien anhand von NIST-Kategorien zu analysieren und Schwerpunktbereiche zu priorisieren.

Hochschulen mit Forschungs- und medizinischen Programmen benötigen möglicherweise ebenfalls eine [ISO 27001](#)-Zertifizierung. Dieser international anerkannte Standard für das Informationssicherheitsmanagement unterstützt umfassende Datenschutz-, Risikomanagement- und Compliance-Praktiken, die für sensible Forschungsumgebungen erforderlich sind.

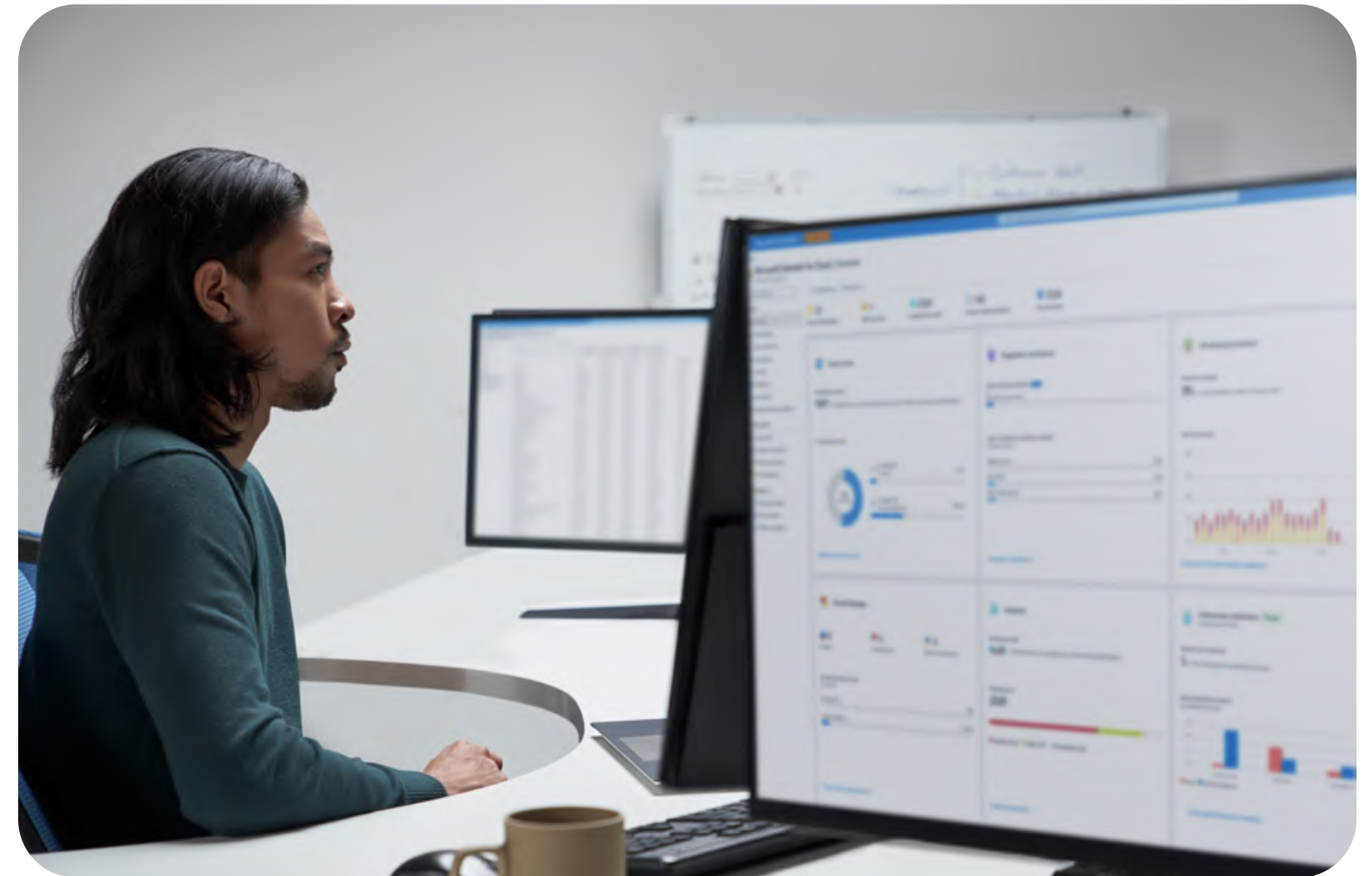


Copilot-Prompt

Ermitteln Sie die Zugriffsanforderungen für alle Benutzergruppen (Studierende, Lehrkräfte, Vertretungen, Forschende, Auftragnehmer) und erstellen Sie empfohlene Richtlinien für bedingten Zugriff mithilfe von Entra ID. Stellen Sie dies in einer Richtlinienmatrix mit Risikostufen dar.

TIPP

Beschreiben Sie saisonale oder vorübergehende Zugriffsanforderungen – Vertretungslehrkräfte, Auftragnehmer, Lehramtsstudierende, wissenschaftliche Fachkräfte mit Gaststatus –, damit Copilot dynamische Zugriffsrichtlinien erstellen kann.



Benutzungszugriffsverwaltung vereinfachen

[Microsoft Entra ID](#) bewältigt die Komplexität von Bildungsumgebungen, in denen sich die Bedürfnisse der Benutzenden schnell ändern. Ihre Richtlinien für den bedingten Zugriff sollten die akademischen Realitäten widerspiegeln, einschließlich temporärer Benutzer, saisonaler Zugriffsanforderungen und Anforderungen an die Zusammenarbeit, die sich mit jedem Semester ändern. Verwenden Sie diese Tabelle, um Benutzungszugriffsrichtlinien zu planen, die Ihrem akademischen Umfeld entsprechen.

K-12-BENUTZENDE	BEIDES	HOCHSCHULEN-BENUTZENDE
Lernende	Fakultät und Lehrende	Forscher
Vertretungskräfte	Personal	Graduiertenstudierende
Freiwillige	Admins	Industriepartner
Zugriff für Eltern und Erziehungsberechtigte	IT-Mitarbeitende	
	Gastbenutzende	
	Auftragnehmende	

Vorfallreaktion in Aktion:
Ransomware in der Prüfungswoche

Während der Prüfungswoche löst eine verdächtige Dateiverschlüsselungsaktivität Warnungen im gesamten Netzwerk Ihrer Institution aus:

1. **Bedrohung erkennen:** [Microsoft Defender XDR](#) identifiziert die Ransomware-Signatur, während [Microsoft Entra ID Protection](#) ungewöhnliche Admin-Anmeldeversuche von einer externen IP-Adresse meldet.

2. **Automatisch antworten:** Innerhalb weniger Minuten isolieren [Microsoft Sentinel](#)-Playbooks betroffene Geräte über [Microsoft Defender für Endpunkt](#), sperren das kompromittierte Administratorkonto über [Microsoft Entra ID](#) und senden [Teams](#)-Benachrichtigungen an Ihre IT-Abteilung und die Schulleitung.

3. **Wiederherstellung mit Anleitung:** Für Institutionen, bei denen [Microsoft Security Copilot](#) bereitgestellt ist, liefert KI-gestützte Analyse Insights in Angriffsmuster und Empfehlungen zur Wiederherstellung, während [Microsoft Purview](#) alles für Versicherungsansprüche und regulatorische

4. Berichterstellung dokumentiert. **Künftige Angriffe verhindern:** [Microsoft Defender for Office 365](#) blockiert proaktiv ransomware-infizierte E-Mails und bösartige Anhänge, bevor sie die Benutzenden erreichen, während [„Sichere Anhänge“](#) und [„Sichere Links“](#) zusätzliche Schutzebenen gegen Phishingkampagnen bieten, die häufig Ransomware-Angriffen vorausgehen.

5. **Ergebnis:** Der Unterricht läuft ohne Unterbrechung weiter, während Ihre automatisierten Systeme die Bedrohung eindämmen und die Wiederherstellungsbemühungen leiten.

Proaktive Planung der Reaktion auf Vorfälle hilft Ihrer Institution, die Kontinuität aufrechtzuerhalten und das Lernen zu schützen – selbst in kritischen Zeiten wie der Abschlusswoche.

Technologiesicherheitsstrategie

Technologieentscheidungen bieten die Chance, die Sicherheit zu verbessern und das Lernen vom ersten Tag an zu unterstützen. Durch die Partnerschaft mit Microsoft und die Nutzung integrierter Sicherheitsfunktionen können Bildungseinrichtungen Umgebungen schaffen, in denen Schutz und Produktivität Hand in Hand gehen.

Optimieren und sichern

Nutzen Sie [Microsoft 365 A3 for Education](#), um essenzielle Sicherheitsfunktionen und Produktivitätstools bereitzustellen, damit Schulbezirke ihre Ressourcen und ihren Schutz von Anfang an optimieren können.

- [Microsoft Defender für Endpunkt](#): Stellen Sie erweiterten Bedrohungsschutz mit Defender für Endpunkt Plan 1 bereit, der in der Lehrkräfte-A3-Lizenzierung enthalten ist und wesentliche Endpunktsicherheit für Geräteumgebungen im Bildungsbereich bietet. Hinweis: Für Student Use Benefit-Abonnements ist eine zusätzliche Lizenzierung für Defender für Endpunkt erforderlich.
- [Microsoft 365 Education](#) – Speicher: Implementieren Sie Cloud-First-Speicher mit integrierter FERPA-Compliance, Schutz der Datenresidenz, automatischer Sicherung und vorhersehbaren Betriebskosten.
- [Microsoft Intune for Education](#): Vereinfachen Sie die Geräteverwaltung für Klassenzimmerumgebungen, ohne Lernabläufe zu unterbrechen.
- [Microsoft Purview Data Security Posture Management](#) (DSPM) für KI: Implementieren Sie grundlegende KI-Überwachung, um Einblick in KI-Nutzungsmuster zu erhalten und Daten von Lernenden vor unangemessener Weitergabe zu schützen.



Entwickeln Sie umfassende, forschungsreife Sicherheit

Für Hochschulen mit anspruchsvolleren Anforderungen trägt ein umfassender Ansatz dazu bei, einen robusten Schutz und die Einhaltung von Compliance sicherzustellen. Nutzen Sie [Microsoft 365 A5 for Education](#), um fortschrittliche Sicherheits-, Analyse- und Compliance-Funktionen mit Support für komplexe Forschungsumgebungen und Multi-Campus-Betrieb bereitzustellen und zu unterstützen.

- Zero-Trust-Grundlage: Etablieren Sie ein essentielles Sicherheitsframework, bevor Sie fortschrittliche KI-Tools wie [Microsoft 365 Copilot](#) und [Security Copilot](#) bereitstellen.
- Hybride Infrastrukturstrategie: Stellen Sie ein Gleichgewicht zwischen Cloud-Kollaboration und lokalen Forschungssystemen her, um regulatorische Compliance, Datenhoheit und den Schutz geistigen Eigentums sicherzustellen.
- [Microsoft Sentinel](#): Konfigurieren Sie KI-gestütztes Security Information & Event Management (SIEM) für unternehmensweite Bedrohungserkennung über mehrere Standorte und Forschungsnetzwerke hinweg.
- [Microsoft Purview](#): Umfassende Data Governance für Fördermittel-Compliance, internationale Forschungszusammenarbeit und automatisierte regulatorische Berichterstattung implementieren.
- [Microsoft Purview DSPM für KI](#): Konfigurieren Sie fortschrittliche KI-Governance mit detaillierten Analysen, Richtliniendurchsetzung und Compliance-Kontrollen, um einen sicheren Forschungsbetrieb zu unterstützen.

Planen Sie Ihre Cloudmigration und Datenresidenzstrategie mit dem bewährten [Framework zur Cloud-Einführung](#) von Microsoft.



Copilot-Prompt

Erstellen Sie einen Schritt-für-Schritt-Plan zur Bereitstellung von Microsoft Intune in einem Schulbezirk mit mehreren Standorten, einschließlich Autopilot-Einrichtung, Compliance-Richtlinien, Einschreibungsoptionen für gemeinsam genutzte vs. 1:1-Geräte und einer empfohlenen Pilotsequenz. Stellen Sie die Empfehlungen als Checkliste bereit.

TIPP

Geben Sie Details zu Ihrem Gerätemix, zu Netzwerkbeschränkungen und dazu an, ob Geräte gemeinsam genutzt werden oder im 1:1-Modell eingesetzt werden. Auf diese Weise kann Copilot die Empfehlungen für die Intune-Registrierung und -Richtlinien an Ihre Umgebung anpassen.

Readiness der Organisation

Cybersicherheitsschulungen sind ein unverzichtbarer Bestandteil eines jeden ausgereiften Programms. Die Entwicklung organisatorischer Readiness befähigt Ihre Institution, durch qualifiziertes Personal, engagierte Benutzende und ausgeprägte Cyberhygiene, die Ihre Mission unterstützen, den größtmöglichen Wert zu schaffen.



[Copilot-Prompt](#)

Skizzieren Sie die Schritte zur Einführung eines SOC-Programms für Studierende, einschließlich der erforderlichen Microsoft-Tools (Sentinel, Defender XDR, Security Copilot), Lehrplanressourcen, Sponsoring durch die Fakultät, Rollen der Studierenden und eines 12-wöchigen Zeitplans für die Implementierung.

TIPP

Geben Sie Ihren verfügbaren Talentpool an (z. B. Cybersicherheits-Club, STEM-Akademie, Werkstudierende) sowie die geschätzten Betreuungsstunden. Copilot kann dann ein Programm entwerfen, das auf Ihre Kapazitäten und das Kompetenzniveau der Studierenden zugeschnitten ist.

Die Readiness-Phasen durchlaufen

Microsoft stellt Ihnen Ressourcen zur Verfügung, mit denen Mitglieder auf Ihrem Campus ihre Kenntnisse und Fähigkeiten im Bereich der Cybersicherheit aufbauen und weiterentwickeln können. Folgen Sie diesen Implementierungsphasen:

- 1. Erstellung einer Grundlage: Führen Sie Microsoft Learn und Microsoft Education Programme zur Förderung des Cybersicherheitsbewusstseins institutionsweit ein.
- 2. Erweiterung des Engagements: Implementieren Sie Cybersicherheitsprogramme für Studierende, und etablieren Sie eine fortlaufende Sicherheitskultur sowie Weiterbildungspläne.
- 3. Erweiterte Funktionen: Starten Sie Security Operations Center (SOC)-Programme für Studierende mit dem Microsoft Student SOC Toolkit, das strukturiertes Lernen mit praktischen Erfahrungen in Microsoft Defender XDR, Sentinel und Security Copilot bietet.

Nutzen Sie die Tabelle, um die relevantesten Ressourcen und Qualifizierungswege für Ihr Team zu identifizieren.

Mit diesen Ressourcen kann jedes Mitglied Ihrer Institution zu einer sicheren, widerstandsfähigen Lernumgebung beitragen.

READINESS-FOKUS	ERSTELLUNG EINER GRUNDLAGE	ERWEITERUNG UND FORTGESCHRITTENE QUALIFIZIERUNG
K-12-IT-Mitarbeitende Sicherheitsgrundlagen für IT-Admins und automatisierte Reaktion auf Bedrohungen	Microsoft Learn Security-Hub Microsoft Certified: Security, Compliance and Identity Fundamentals Beschreiben Sie die Kernfunktionen von Microsoft Security Copilot	Konzipieren Sie Lösungen, die sich an bewährten Sicherheitspraktiken und Prioritäten orientieren Verbessern Sie Ihre Sicherheitsoperationen durch die Verwendung von Microsoft Security Copilot
IT-Personal an Hochschulen Fortgeschrittene SecOps mit KI-gestützter Bedrohungssuche im Unternehmensmaßstab	Microsoft Learn Security-Hub Konfigurieren Ihrer Microsoft Sentinel-Umgebung Verbessern Sie Ihre Sicherheitsoperationen durch die Verwendung von Microsoft Security Copilot	Microsoft Certified: Security, Compliance and Identity Fundamentals Microsoft Security Operations Analyst
Fakultät, Personal und Admins Cybersicherheit im Klassenzimmer, sichere Nutzung von Technologie und Schutz von Forschungsdaten	Cybersicherheit in K-12-Klassenzimmern mit Microsoft-Tools aufbauen Was ist Cybersicherheit? Azure für Forschende – Teil 1: Einführung in Cloud Computing	Cybersicherheitskonzepte mit Minecraft Education vermitteln Stärken Sie die Cybersicherheitsführung an K-12-Schulen mit Microsoft-Tools Azure für Forschende – Teil 2: Cloud Security and Cost Management
K-12-Lernende Digitale Bürgerschaft; sichere Erkundung von KI	K-12-Cybersicherheit – Gesprächsleitfaden und Infografik Minecraft Cyber- und digitale Bürgerschaft	Grundlagen der Sicherheit (SC-900) Unterrichtstoolkit: Generative KI erschließen verantwortungsvoll und sicher
Studierende in Hochschulen Berufsvorbereitung und praktische Erfahrung im Sicherheitsbereich	Microsoft Student Security Operations Center Toolkit Microsoft Learn Student Hub – Zertifizierungen für Studierende	Microsoft Certified: Security, Compliance, and Identity Fundamentals Microsoft-Cybersicherheit – Stipendienprogramm

Finanzielle und strategische Begründung

Investieren in Microsoft-Sicherheitslösungen ermöglicht Bildungseinrichtungen, messbare Ergebnisse zu erzielen, Ressourcen effizienter zu nutzen und die Compliance zu stärken.

Von Microsoft in Auftrag gegebene Forrester Total Economic Impact-Studien untersuchten den Sicherheits-ROI für K-12- und Hochschuleinrichtungen, die Microsoft 365 Education A5 verwenden:

- [Zusammengesetzte K-12-Organisation](#): 118 % ROI mit einem Nutzen von 4,22 Mio. USD über drei Jahre im Vergleich zu Kosten von 1,94 Mio. USD.
- [Zusammengesetzte Hochschuleinrichtung](#): 128 % ROI mit 7,28 Millionen US-Dollar Erträgen gegenüber 3,19 Millionen US-Dollar Kosten.
- [Voraussichtlicher Microsoft Security Copilot ROI](#): 99 bis 348 % mit einem prognostizierten Nettobarwert von 500.000 bis 1,8 Millionen US-Dollar.

Entdecken Sie die Tabelle mit strategischen Werten, um zu erfahren, wie strategische Investitionen in Sicherheit Ihrer Institution messbare Vorteile bringen.

INVESTITIONSSCHWERPUNKT	QUANTIFIZIERTE VORTEILE	FINANZIELLE UND BETRIEBLICHE AUSWIRKUNGEN
KI-gestützte Sicherheitsabläufe	• Security Copilot bietet 23 bis 47 % Produktivitätssteigerungen bei SecOps • Verbesserte Prävention von Sicherheitsverletzungen durch schnellere Reaktion auf Bedrohungen	Erzielt eine Rendite (ROI) von 99 bis 348 % in verschiedenen Branchen.
Sicherheit und Compliance	• 15 % weniger schwerwiegende Sicherheitsverletzungen • 29 % geringere Kosten für die Behebung von Sicherheitsverletzungen	Ersparnis: 972.800 US-Dollar für allgemeinbildende Schulen (K-12) und 1,2 Millionen US-Dollar für Hochschulen.
Anbieterkonsolidierung	• 30 % geringere Kosten für Sicherheitslizenzierungen • Vereinfacht die Verwaltung durch Konsolidierung auf einen einzigen Anbieter	Ersparnis: 1,1 Millionen US-Dollar für allgemeinbildende Schulen (K-12) und 1,7 Millionen US-Dollar für Hochschulen.
Personaleffizienz	• Eine wesentliche Erweiterung des IT-Sicherheitsteams wird vermieden. • Verschafft einen entscheidenden Vorteil in einem wettbewerbsintensiven Talentmarkt • Mildert Einstellungs- und Bindungsherausforderungen	Ersparnis: 545.700 US-Dollar für K-12 und 1,1 Mio. US-Dollar für Hochschulen. Maximiert die Effizienz des bestehenden Personals, um die Vergrößerung der Teams deutlich zu reduzieren.
Produktivitätsgewinne	• Spart 15 Minuten pro angestellter Person • Verbessert die Sicherheits-Benutzungserlebnisse und die Systemverfügbarkeit • Verbesserte Prävention von Sicherheitsverletzungen durch schnellere Reaktion auf Bedrohungen	Ersparnis: 1,7 Mio. US-Dollar für K-12 und 3,3 Mio. US-Dollar für Hochschulen. • 23 bis 47 % Produktivitätssteigerungen in SecOps mit Security Copilot • ROI 99-348 % in allen Branchen

Lizenzen optimieren

Wählen Sie den richtigen Microsoft 365 Education-Plan für Ihr Unternehmen aus. Berücksichtigen Sie Faktoren wie Ihr aktuelles Sicherheitsrisiko, die Teamkapazität und die verfügbaren Ressourcen.

- **A3-Basisansatz:** Beginnen Sie mit grundlegender Sicherheit, die auf Ihren bestehenden Microsoft-Investitionen aufbaut, indem Sie mit MFA starten und schrittweise weitere Sicherheitsebenen hinzufügen.
- **A5 umfassender Ansatz:** Implementieren Sie erweiterte Sicherheits-, Compliance- und Analysefunktionen mit Enterprise-Bedrohungsschutz und Compliance-Tools, die den Multi-Campus-Betrieb unterstützen und die Optimierung der Gesamtbetriebskosten ermöglichen.



Copilot-Prompt

Bewerten Sie unsere aktuellen Sicherheitsanbieter und erstellen Sie eine Konsolidierungsübersicht, die zeigt, welche Tools durch den Microsoft-Sicherheitsstack ersetzt werden können. Fügen Sie prognostizierte Einsparungen, Integrationsvorteile und einen stufenweisen Migrationsplan hinzu.

[Stellen Sie einen Link bereit oder laden Sie ein Dokument hoch, in dem alle vorhandenen Sicherheitsanbieter sowie die aktivierten Apps und Funktionen aufgeführt sind.]

TIPP

Stellen Sie Ihre aktuelle Anbieterliste bereit und kennzeichnen Sie Tools, die teuer oder schwer zu warten sind. Copilot kann Konsolidierungen priorisieren, die die größten Einsparungen und Effizienzsteigerungen bringen.

Budgetplanung und -begründung

Ihr Team sollte außerdem den Bereitstellungszeitplan, die möglichen Einsparungen Ihrer Einrichtung durch ROI und verfügbare zusätzliche Ressourcen zur Kostenkompensation berücksichtigen.

- **Stufenweiser Ansatz:** Beginnen Sie mit der Bereitstellung der Grundlage (A3-Baseline), erweitern Sie strategisch (A5-Upgrades) und optimieren Sie anschließend in der gesamten Institution.
- **Budgetberechnungsrahmen:** Berechnen Sie den Wert der Risikominderung, fügen Sie betriebliche Effizienzsteigerungen hinzu und beziehen Sie die Entwicklung strategischer Fähigkeiten zur umfassenden Rechtfertigung des ROI ein.
- **Kostenvermeidung:** Verhindern Sie Sicherheitsincident, die im Jahr 2025 durchschnittlich [4,44 Millionen US-Dollar pro Sicherheitsverletzung](#) verursachen; automatisieren Sie die Compliance, um Entwicklungskosten zu senken; und konsolidieren Sie die Infrastruktur, um einen ROI von 118 bis 128 % zu erzielen, wie in bildungsspezifischen Studien nachgewiesen.
- **Bildungsspezifische Fördermöglichkeiten:** Entdecken Sie Zuschussanträge und Branchenpartnerschaften, die Investitionen in Sicherheitsprogramme unterstützen und gleichzeitig die Einhaltung der FERPA-, COPPA- und DSGVO-Anforderungen nachweisen.

Implementierung

In diesem Abschnitt

[K-12-Implementierungsszenarien](#)

[Implementierungsszenarien
im Hochschulbereich](#)



K-12-Implementierungsszenarien

Identitätssicherheit

Technologiezugangsmodelle – ob gemeinsam oder 1:1 – stellen IT-Teams vor besondere Herausforderungen.

Zusammenfassung der Herausforderung

Bei 1:1-Geräteprogrammen haben Lernende häufig Schwierigkeiten mit der Multi-Faktor-Authentifizierung (MFA). Ganz gleich, ob es sich um ein vergessenes Kennwort, verspätete Eingabeaufforderungen oder die Notwendigkeit zusätzlicher Geräte handelt – diese Hürden können das Lernen stören und Frustration verursachen.

In geteilten Umgebungen – wie Labors, Gerätewagen oder Bibliotheken – ist herkömmliche MFA nicht praktikabel. Wenn Dutzende Lernende in kurzen Sessions dieselben Computer nutzen, führen wiederholte Anmeldungen zu Engpässen, die den Unterricht verlangsamen und die IT-Ressourcen belasten.

Microsoft-Lösungen in Aktion

Microsoft-Tools bieten flexible Anmeldeoptionen, die dazu beitragen, die Daten der Lernenden zu schützen, ohne den Lernprozess zu unterbrechen:

1:1-GERÄTE

HERAUSFORDERUNG	MICROSOFT-TOOL	ERGEBNIS IN DER PRAXIS
Lernende vergessen Passwörter oder haben Schwierigkeiten mit MFA auf persönlichen Geräten.	Windows Hello for Business: Ermöglichen Sie Benutzenden, sich auf ihren Windows-Geräten mit biometrischen Daten oder einer PIN anstelle eines herkömmlichen Kennworts anzumelden.	Ermöglicht die sichere Anmeldung per Fingerabdruck, Gesichtserkennung oder PIN, wodurch der Anmeldeaufwand reduziert und Phishing-Risiken minimiert werden.
Eine lernende Person vergisst seine Zugangsdaten direkt vor dem Unterricht oder einer Prüfung.	Entra ID – befristeter Zugriffspass (TAP): Stellen Sie einen zeitlich begrenzten Zugangscode bereit, der für einmalige oder mehrfache Anmeldungen konfiguriert werden kann.	Ermöglicht es Lehrkräften oder IT-Mitarbeitenden, sichere, zeitlich begrenzte Anmeldeinformationen auszustellen, damit das Lernen ohne Verzögerungen fortgesetzt werden kann.
Lehrkräfte und Lernende jonglieren täglich mit mehreren Apps und Anmeldungen.	Entra ID Federated Identity: Bieten Sie Zugriff auf durch Microsoft Entra geschützte Ressourcen, ohne Anmeldeinformationen verwalten zu müssen.	Ermöglicht nahtloses Single Sign-On über verschiedene Apps, reduziert Login-Müdigkeit und hält den Unterricht am Laufen.

GEMEINSAM GENUTZTE GERÄTE

HERAUSFORDERUNG	MICROSOFT-TOOL	ERGEBNIS IN DER PRAXIS
Gemeinsam genutzte Geräte (Labore, Wagen, Bibliotheken) erfordern schnellen Zugriff, aber traditionelle Multi-Faktor-Authentifizierung verlangsamt die Anmeldevorgänge.	Entra ID FIDO2-Schlüssel: Authentifizieren Sie sich, ohne einen Benutzernamen oder ein Kennwort einzugeben.	Ermöglicht berührungsgesteuerten Zugriff mit tragbaren Sicherheitsschlüsseln, wodurch persönliche Mobiltelefone überflüssig werden und die Produktivität der Sessions erhalten bleibt.
District IT muss Benutzende und Geräte in einer großen Umgebung validieren.	Entra ID – zertifikatbasierte Authentifizierung: Fordern Sie Benutzende auf, sich direkt mithilfe von X.509-Zertifikaten zu authentifizieren, die in Microsoft Entra ID authentifiziert sind.	Ermöglicht skalierbare, sichere Anmeldungen mit Public-Key-Infrastruktur (PKI), verringert das Aufkommen von Helpdesk-Anfragen und stärkt die Compliance in gemeinsam genutzten Umgebungen.
Distriktleitende müssen vertrauliche Daten schützen, ohne den Bildungsbetrieb zu stören.	Richtlinien für bedingten Zugriff: Schützen Sie institutionelle Vermögenswerte, indem Sie von den Benutzenden verlangen, eine Aktion auszuführen, um Zugriff zu erhalten.	Passen Sie den Zugriff dynamisch basierend auf Rolle, Risikostufe und Gerätecompliance an und bringen Sie Schutz und Benutzerfreundlichkeit in Einklang.

Erste Schritte

Schulbezirke können einen sicheren, schrittweisen Ansatz zur Stärkung der Identitätssicherheit verfolgen. Indem sie mit Pilotprojekten in einzelnen Klassen beginnen, können Schulen und Bildungseinrichtungen Microsoft Entra ID-Lösungen mithilfe von Schritt-für-Schritt-Anleitungen implementieren, um herauszufinden, was am besten funktioniert, und erfolgreiche Strategien im gesamten Schulbezirk ausrollen – und das alles, ohne den Unterricht zu unterbrechen.

LÖSUNGEN VON MICROSOFT ENTRA ID ENTDECKEN

Lesen Sie Schritt-für-Schritt-Anleitungen, testen Sie in einem Klassenzimmer und skalieren Sie dann im gesamten Bezirk.

 [Erfahren Sie mehr](#)

Erkenntnis

Von der lernenden Person, die sich mit einem Fingerabdruck anmeldet, bis zur Bezirksleitung, die Tausende von Konten absichert, bringen die Identitätslösungen von Microsoft Schutz und Einfachheit in Einklang. Durch die Kombination von Windows Hello, Entra ID-Tools und flexiblen Zugriffsrichtlinien können Schulen Daten schützen und sich gleichzeitig auf das Lernen konzentrieren.



Datensicherheit und Compliance

Schulen erfassen und speichern personenbezogene Informationen (PII), die geschützt werden müssen, um die Sicherheit der Lernenden sicherzustellen und gesetzliche Vorgaben einzuhalten.

Zusammenfassung der Herausforderung

Cyberkriminelle haben es auf Schulen abgesehen, um Systeme zu infiltrieren und vertrauliche Daten zu extrahieren. Ohne robuste Cybersicherheitsmaßnahmen können Bedrohungsakteure auf Daten zugreifen und Schulen daran hindern, ihre Systeme zu nutzen, bis ein Lösegeld gezahlt wird.

Systembetreibende erhalten häufig Datenanfragen von Dienstleistern, die Zugriff auf vertrauliche Daten von Lernenden verlangen. Wenn diese Anfragen festgelegte Prozesse wie die Kommunikation mit der Schulleitung umgehen, können Daten geteilt werden, die sonst nicht freigegeben würden.

Lehrkräfte benötigen Zugriff auf personenbezogene Daten wie akademische und verhaltensbezogene Aufzeichnungen, um individualisierte Bildungspläne (IEPs) zu erstellen und Benotungsberichte zu verfassen. Angemessenen Zugang bereitzustellen, ohne einen uneingeschränkten Zugriff zu gewähren, ist eine Herausforderung, wenn in Schulen so viele Informationen gespeichert werden.

Es kann schwierig sein sicherzustellen, dass Lehrkräfte und Mitarbeitende keine privaten Daten wie Fotos oder Videos von Lernenden weitergeben, wenn Familien Medienfreigabeformulare unterschreiben, die einschränken, wie das Abbild ihres Kindes verwendet werden darf.

Microsoft-Lösungen in Aktion

Microsoft bietet Sicherheitstools, die Daten schützen, ohne Unterricht oder Abläufe zu stören:

HERAUSFORDERUNG	MICROSOFT-TOOL	ERGEBNIS IN DER PRAXIS
Eine bei SIS tätige Person erhält eine Anfrage, Daten von Lernenden mit einem Anbieter zu teilen, der für die Bereitstellung seiner Dienste keinen Zugriff auf diese Daten benötigt.	Purview-Informationsbarrieren: Beschränken Sie die Zwei-Wege-Kommunikation und Zusammenarbeit zwischen Gruppen und Benutzenden in Microsoft Teams, SharePoint und OneDrive.	Die Kommunikation und Zusammenarbeit mit dem Anbieter wird eingeschränkt, sodass eine Datenweitergabe verhindert und bestehende Datenschutzmaßnahmen aufrechterhalten werden.
Eine SPED-Lehrkraft benötigt Zugriff auf die akademischen und Verhaltensdaten eines bestimmten Schülers, um einen IEP zu verfassen, sollte aber keinen schulweiten Zugriff auf jedes Profil von Lernenden haben.	Purview-Informationsschutz: Entdecken, klassifizieren und schützen Sie vertrauliche Informationen – unabhängig davon, wo sie gespeichert sind oder übertragen werden.	IT-Fachkräfte klassifizieren und kennzeichnen die Daten, um sicherzustellen, dass die Lehrkraft auf das zugreifen kann, was für die Rolle angemessen ist, ohne universellen Zugriff auf alle Daten von Lernenden zu gewähren.
Eine Schulleitung teilt in den sozialen Medien Fotos von einer kürzlichen Schulveranstaltung, auf denen lächelnde Gesichter von Lernenden, Lehrkräften und Familien zu sehen sind.	Purview – Verhinderung von Datenverlust: Verhindern Sie, dass interne Benutzende vertrauliche Daten unangemessen mit Personen teilen, die keinen Zugriff darauf haben sollten.	Die unbefugte Weitergabe, Nutzung oder Übertragung vertraulicher Informationen wie Fotos wird eingeschränkt, um die Privatsphäre aller Benutzungsgruppen zu wahren.

So setzen Sie eine Lösung um

Um mit Microsoft Purview zu beginnen, identifizieren Sie zunächst die sensibelsten Datentypen Ihres Schulbezirks und die Rollen von Mitarbeitenden mit Zugriffsberechtigung. Überprüfen Sie anschließend die Kernfunktionen von Purview und wenden Sie geeignete Freigabeeinschränkungen sowie Datenbeschriftungen an.

MICROSOFT-LÖSUNGEN ENTDECKEN

Lernen Sie, wie Sie Datenrisiken erkennen, Compliance verwalten und Datenverlust in Ihrer gesamten Infrastruktur verhindern.

 [Entdecken Sie Microsoft Purview](#)

Beispiele aus der Praxis: Prince William County Public Schools

In Virginia hat die Schulverwaltung der Prince William County Public Schools Maßnahmen ergriffen, um sicherere digitale Erfahrungen für Lernende zu schaffen, die vom Bezirk bereitgestellte mobile Geräte und Laptops nutzen. Der Bezirk hat Microsoft Purview-Produkte eingeführt, um Cybermobbing und Belästigung diskret zu identifizieren und Insights in schädliche oder unangemessene Inhalte zu gewinnen, die von Lernenden geteilt werden. Dadurch konnte der Schulbezirk Verstöße gegen FERPA und CIPA erkennen und vor allem schnell reagieren, wenn ein Vorfall auftrat oder Lernende Support benötigten.

Erfahren Sie, wie die Prince William County Public Schools die Purview-Produktfamilie einsetzen, um die Einhaltung von Bundesvorschriften sicherzustellen und Lernenden ein sichereres digitales Erlebnis zu bieten.

 [Lesen Sie die Geschichte](#)

Erkenntnis

Microsoft Purview hilft Schulen, vertrauliche Daten zu schützen, indem klare Grenzen für Zugriff und Weitergabe gesetzt werden und so die Einhaltung von Datenschutzbestimmungen unterstützt wird. Mit Funktionen wie Informationsbarrieren, Informationsschutz und Verhinderung von Datenverlust können IT-Teams unbefugte Offenlegungen verhindern und zugleich dafür sorgen, dass Lehrkräfte und Admins Zugriff auf die erforderlichen Informationen erhalten.

Implementierungsszenarien im Hochschulbereich

Datensicherheit

Institutionen stehen aufgrund von vertraulichen Forschungsdaten, Gesundheitsdaten, Finanzunterlagen, Zulassungsinformationen und PII, die gespeichert, abgerufen und verwendet werden, vor einzigartigen Herausforderungen in Bezug auf die Datensicherheit.

Zusammenfassung der Herausforderung

Die Durchführung geförderter Forschungsprojekte erfordert Zusammenarbeit und Kommunikation mit anderen Institutionen. Mitarbeitende müssen vertrauliche Daten zwischen autorisierten Gruppen austauschen und verhindern, dass Daten nach außen dringen.

Führungsteams verteilen häufig Dateien mit strategischen Vorgaben, die nicht mit anderen Gruppen geteilt werden sollten. Die Kontrolle des Zugriffs auf vertrauliche Informationen ist entscheidend.

IT-Fachkräfte überprüfen die Infrastruktur auf Risiken und Schwachstellen. Bei Vorfällen wie einer internen Datenschutzverletzung benötigen CTOs Sicherheitsteams, um zu analysieren, was passiert ist, und zukünftige Vorfälle zu verhindern – oft während sie andere kritische Vorgänge erledigen.

Microsoft-Lösungen in Aktion

Microsoft bietet Sicherheitslösungen, die Daten schützen, ohne den Ablauf von Forschung, Lehre oder Betrieb zu stören:

HERAUSFORDERUNG	MICROSOFT-TOOL	ERGEBNIS IN DER PRAXIS
Ein Fakultätsmitglied, das sensible Forschung durchführt, muss Informationen mit einer anderen Universität austauschen und dabei die öffentliche Weitergabe verhindern.	Purview-Informationsbarrieren: Beschränken Sie die Zwei-Wege-Kommunikation und Zusammenarbeit zwischen Gruppen und Benutzenden in Microsoft Teams, SharePoint und OneDrive.	Die Kommunikation über sensible Forschung ist auf autorisierte Gruppen beschränkt, um die gemeinsame Nutzung von Daten zu verhindern und den bestehenden Datenschutz zu gewährleisten.
Ein Provost verteilt ein Memo des Board of Visitors an die Dekane, das nicht mit Lehrpersonal oder Mitarbeitenden geteilt werden sollte.	Purview-Informationsschutz: Entdecken, klassifizieren und schützen Sie vertrauliche Informationen – unabhängig davon, wo sie gespeichert sind oder übertragen werden.	Das Memo ist klassifiziert und gekennzeichnet, um sicherzustellen, dass nur Dekane die Datei öffnen und lesen können.
Ein neu eingestellter Lehrbeauftragter veröffentlicht PDF-Anweisungen in einem Teams-Kanal, die den Studierenden zeigen, wie sie sich bei einer ausschließlich für Lehrkräfte bestimmten Datenbank anmelden können.	Purview – Verhinderung von Datenverlust: Verhindern Sie, dass interne Benutzende vertrauliche Daten unangemessen mit Personen teilen, die keinen Zugriff darauf haben sollten.	Die Aktivität der Person, die den Kurs leitet, löst Warnungen aus, die zu Anpassungen von Richtlinien führen, um den Zugriff auf die PDF-Datei und ähnliche Datentypen künftig zu blockieren.
Ein CTO beauftragt IT-Fachkräfte, Schwachstellen im gesamten System zu identifizieren, nachdem eine mitarbeitende Person versehentlich strategische Pläne mit den Medien geteilt hat.	Purview-Insider-Risikomanagement: Minimieren Sie interne Risiken, indem Sie böswillige und unbeabsichtigte Aktivitäten in Ihrer Einrichtung erkennen, untersuchen und darauf reagieren.	IT-Fachkräfte erkennen und beheben nicht autorisierte Offenlegungen von Daten und befolgen Richtlinien, um ähnliche Vorfälle auf dem gesamten Campus zu verhindern.
Eine studierende Person, die für das Security Operations Center (SOC) der Universität arbeitet, muss campusweite Bedrohungen überwachen, während IT-Mitarbeitende an einer ganztägigen Abteilungsklausur teilnehmen.	Security Copilot: Schützen Sie Ihre Einrichtung mit der Geschwindigkeit und der Skalierbarkeit von KI – mit einem generativen KI-gestützten Assistenten für den täglichen Betrieb in den Bereichen Sicherheit und IT.	Die studierende Person nutzt KI-gestützte Assistenz, um Signale von Microsoft Defender systemübergreifend zu analysieren und Anomalien zu erkennen. Mithilfe von Schritt-für-Schritt-Anweisungen werden Bedrohungen eingedämmt, während das IT-Personal abwesend ist.

So setzen Sie eine Lösung um

Um mit Microsoft Purview zu starten, identifizieren Sie zunächst die sensibelsten Datentypen Ihrer Universität und die Rollen der Mitarbeitenden, die Zugriff benötigen. Überprüfen Sie anschließend die Kernfunktionen von Purview und wenden Sie geeignete Freigabeeinschränkungen sowie Datenbeschriftungen an.

MICROSOFT-LÖSUNGEN ENTDECKEN

Lernen Sie, wie Sie Datenrisiken erkennen, Compliance verwalten und Datenverlust in Ihrer gesamten Infrastruktur verhindern.

➔ [Entdecken Sie Microsoft Purview](#)

Entdecken Sie, wie Sie erkennen, was andere übersehen, schneller auf Bedrohungen reagieren und die Teamkompetenz mit KI-Unterstützung stärken können.

➔ [Erfahren Sie mehr über Security Copilot](#)

Beispiele aus der Praxis: Oregon State University

Im Rahmen ihres Engagements für innovative Sicherheit haben die Admins der Oregon State University Security Copilot eingeführt, um ihren Cyber-Sicherheitsstatus nach einem Zwischenfall zu vertiefen. Security Copilot ermöglichte es IT-Fachleuten, Prozesse zur Erkennung von Bedrohungen und zur Reaktion darauf zu automatisieren, sodass Analysten sich auf wertschöpfende Aufgaben und komplexe Untersuchungen konzentrieren konnten. Dies führte zu einer schnelleren Lösung von Vorfällen, niedrigeren Betriebskosten und verbessertem Schutz vertraulicher Forschungs- und Studierendendaten.

Erfahren Sie, wie Security Copilot der Oregon State University dabei geholfen hat, Schwachstellen zu beheben und campusweit eine proaktivere Sicherheitsstrategie zu implementieren.

➔ [Lesen Sie die Geschichte](#)

Erkenntnis

Hochschulen müssen vertrauliche Forschungsergebnisse schützen, die gemeinsame Nutzung von Daten einschränken und privilegierte Daten schützen, während sie gleichzeitig eine sichere Zusammenarbeit zwischen autorisierten Benutzenden ermöglichen. Microsoft Purview und Security Copilot ermöglichen Universitäten, den Zugang zu verwalten, Datenlecks zu verhindern und schnell auf neue Risiken zu reagieren, ohne Lehre oder Forschung zu unterbrechen.



Copilot-Prompt

Entwerfen Sie einen Implementierungsplan für das Insider-Risikomanagement in unserer Institution, einschließlich Richtlinienvorlagen für Datenlecks, Risikobenutzungsverhalten und den Umgang mit Forschungsdaten. Geben Sie Hinweise für Lehrende, Mitarbeitende und wissenschaftliche Hilfskräfte zur verantwortungsvollen Datenverwaltung.

TIPP

Beschreiben Sie vergangene versehentliche Offenlegungen oder wiederkehrende riskante Verhaltensweisen (z. B. das Teilen von PDFs per persönlicher E-Mail). Copilot kann diese Muster nutzen, um relevantere Insider-Risikorichtlinien zu gestalten.

Datenkonformität

Universitäten müssen die Anforderungen an Datenschutz, Datenaufbewahrung und Data Governance erfüllen, wie sie in bundesstaatlichen Vorschriften wie [FERPA](#), [HIPPA](#) und [GDPR](#) festgelegt sind, um Fördermittel und Verträge zu erhalten.

Zusammenfassung der Herausforderung

Ehemalige Mitarbeitende behalten manchmal auch nach dem Ausscheiden aus einer Institution **Zugang zu internen Systemen**. Universitäten müssen sicherstellen, dass der Zugriff auf vertrauliche Daten entzogen wird, um unbefugte Offenlegungen zu verhindern, die zu rechtlichen Risiken und Rufschädigung führen könnten.

Lehrkräfte nutzen gelegentlich institutionelle E-Mail, um **persönliche oder politische Ansichten** mit Studierenden zu teilen. Universitäten brauchen klare Grenzen in der offiziellen Kommunikation, um öffentliche Kontroversen zu vermeiden und gleichzeitig die akademische Freiheit zu respektieren.

Forschungsteams arbeiten oft **mit internationalen Partnern an komplexen Projekten**. Die Weitergabe geheimer technischer Daten ohne ordnungsgemäße Genehmigung könnte gegen Bundesvorschriften verstoßen und zukünftige Finanzierungsmöglichkeiten gefährden.

Microsoft-Lösungen in Aktion

Microsoft bietet Compliance-Lösungen an, die Institutionen dabei unterstützen, regulatorische Anforderungen einzuhalten:

HERAUSFORDERUNG	MICROSOFT-TOOL	ERGEBNIS IN DER PRAXIS
Ein Gesundheitszentrum eines Colleges integriert eine Telemedizin-Plattform eines Drittanbieters, ohne die HIPAA-Compliance zu überprüfen, was zu nicht autorisiertem Zugriff auf die Gesundheitsdatensätze der Studierenden führt.	Purview Compliance Manager: Automatische Bewertung und Verwaltung der Compliance in Ihrer Multi-Cloud-Umgebung.	Zentral definierte Durchsetzungsrichtlinien identifizieren und unterbinden den Zugriff von Plattformen, die nicht den Vorgaben entsprechen, bevor Zugriff auf Gesundheitsdatensätze gewährt wird.
Ein Finanzhilfebeauftragter sendet fälschlicherweise einen Bericht mit Details zu Studentendarlehen und Zuschüssen an eine nicht autorisierte interne Abteilung, was eine Untersuchung auslöst.	Purview-Insider-Risikomanagement: Minimieren Sie interne Risiken, indem Sie böswillige und unbeabsichtigte Aktivitäten in Ihrer Einrichtung erkennen, untersuchen und darauf reagieren.	Automatisierte Richtlinien erkennen, wenn Finanzhilfedaten an nicht autorisierte Empfänger weitergegeben werden, und lösen Warnmeldungen aus oder schränken den Zugriff ein, um weitere nicht konforme Offenlegungen zu verhindern.
Ein Professor sendet politisch aufgeladene Äußerungen per E-Mail an Studierende, die später durchgesickert sind und mediale Aufmerksamkeit erregen.	Purview Communication Compliance: Minimieren von Kommunikationsrisiken, indem potenziell unangemessene Nachrichten im Unternehmen erkannt und erfasst und danach entsprechende Maßnahmen eingeleitet werden.	Politische Aussagen in Nachrichten werden automatisch erkannt und markiert, bevor sie gesendet werden, wodurch ein frühzeitiges Eingreifen ermöglicht und Reputationsschäden minimiert werden.
Eine Universität erhält eine Prüfungsankündigung vom Bildungsministerium mit Bezug auf ihren Umgang mit der Auszahlung von Finanzhilfen an Studierende.	Purview Records Management: Verwalten Sie behördliche, rechtliche und geschäftskritische Aufzeichnungen.	Alle Finanzhilfedaten werden als Aufzeichnungen mit gesetzeskonformen Aufbewahrungszeiträumen gekennzeichnet, um sicherzustellen, dass die Daten für Prüfungen und Untersuchungen verfügbar bleiben.
Vertrauliche biomedizinische Forschungsdaten wurden von einem ehemaligen Mitarbeiter abgerufen und weitergegeben, der nach seinem Ausscheiden aus der Institution weiterhin Zugang zu internen Systemen hatte.	Purview-Informationsschutz: Entdecken, klassifizieren und schützen Sie vertrauliche Informationen – unabhängig davon, wo sie gespeichert sind oder übertragen werden.	Forschungsdaten werden automatisch gemäß Richtlinien gekennzeichnet und verschlüsselt, sodass der Zugriff auf institutionelle Daten für nicht berechnigte Personen verhindert wird.
Eine mitarbeitende Person des Universitätsgesundheitszentrums greift auf die psychischen Gesundheitsdatensätze einer studierenden Person zu und teilt diese mit einer Person mit Professur ohne die Zustimmung der studierenden Person.	Purview – Verhinderung von Datenverlust: Verhindern Sie, dass interne Benutzende vertrauliche Daten unangemessen mit Personen teilen, die keinen Zugriff darauf haben sollten.	IT-Fachkräfte richten automatisierte Richtlinien ein, um die unbefugte Weitergabe von psychischen Gesundheitsdatensätzen per E-Mail oder Chat zu verhindern und so die Einhaltung von HIPAA zu unterstützen.
Ein Forschungsteam, das an einem Verteidigungstechnologieprojekt arbeitet, teilt über SharePoint vertrauliche technische Daten mit internationalen Partnern, was einen potenziellen unbefugten Export auslöst.	Purview-Informationsbarrieren: Beschränken Sie die Zwei-Wege-Kommunikation und Zusammenarbeit zwischen Gruppen und Benutzenden in Microsoft Teams, SharePoint und OneDrive.	Richtlinien werden konfiguriert, um die Dateifreigabe oder Verknüpfungen zu Dateien für internationale Organisationen einzuschränken und so den Export streng vertraulicher Daten zu verhindern.
Ein IT-Admin weist versehentlich teure Softwarelizenzen nicht berechtigten Benutzenden zu und verstößt damit gegen Beschaffungsrichtlinien und Lizenzvereinbarungen.	Purview Audit: Effektiv auf Sicherheitsereignisse, forensische Untersuchungen, interne Ermittlungen und Compliance-Verpflichtungen reagieren.	Überwachungsprotokolle geben an, wer die Lizenzen zugewiesen hat, wann dies geschah und ob dabei Richtlinien verletzt wurden, wodurch Korrekturmaßnahmen und die Dokumentation für Compliance-Anforderungen ermöglicht werden.



So setzen Sie eine Lösung um

Universitäten müssen nicht alle Purview-Lösungen auf einmal implementieren. Identifizieren Sie zunächst die wichtigsten Datenquellen und Compliance-Prioritäten. Verwenden Sie dann die integrierten Vorlagen und Scan-Tools von Purview, um Risiken zu bewerten und die Abdeckung schrittweise abteilungsübergreifend zu erweitern.

MICROSOFT-LÖSUNGEN ENTDECKEN

Lernen Sie, wie Sie Datenrisiken erkennen, Compliance verwalten und Datenverlust in Ihrer gesamten Infrastruktur verhindern.

→ [Entdecken Sie Microsoft Purview](#)

Erkenntnis

Die Einhaltung von Datenschutzbestimmungen erfordert, dass Hochschulen proaktiv steuern, wer auf vertrauliche institutionelle Daten zugreifen und diese weitergeben kann. Die Nutzung von Microsoft Purview hilft Institutionen, die Privatsphäre zu schützen, Datenlecks zu verhindern und die Rechenschaftspflicht in komplexen akademischen Umgebungen sicherzustellen.



Copilot-Prompt

Erstellen Sie ein Reporting-Framework nach der Implementierung für unsere Sicherheits-Tools (Defender, Purview, Sentinel, Entra ID). Fügen Sie monatliche Kennzahlen, Dashboards für die Führungsebene, Verbesserungsmeilensteine und Kennzahlen hinzu, die mit Compliance oder Auditbereitschaft verknüpft sind.

TIPP

Informieren Sie Copilot darüber, welche Kennzahlen Ihre Führungsebene am meisten schätzt – Betriebszeit, Compliance, Reduzierung von Vorfällen oder Auditergebnisse. Es passt das Reporting-Framework an diese Prioritäten an.

Forschung

Erfahren Sie, wie Schulen und Hochschulen mit Microsoft Security Lernende, Mitarbeitende und Daten schützen – durch KI-gestützte Bedrohungserkennung, Zero Trust-Strategien und integrierte Tools, die das IT-Management vereinfachen und die Resilienz stärken.

In diesem Abschnitt

[Microsoft Security in der Bildung: Von der Bereitstellung bis zum Einfluss auf den Campus](#)

[Daten und Analytics](#)

[Ergebnisse aus Wissenschaft und Industrie](#)

[Glossar der Begriffe](#)

[Checkliste für die nächsten Schritte](#)



Microsoft Security in der Bildung: Von der Bereitstellung bis zum Einfluss auf den Campus

Entdecken Sie praxisnahe Anleitungen zur Bereitstellung, Nutzung und bewährten Methoden für Microsoft Security-Lösungen.

Erreichen Sie die Einhaltung gesetzlicher Vorschriften mit Zuversicht: Vereinfachen Sie Ihren Compliance-Prozess und bereiten Sie sich mit Zero Trust auf zukünftige Veränderungen vor.

Microsoft, 2025

Erfahren Sie, wie Bildungseinrichtungen mit integrierten Sicherheits-, Compliance- und Identitätslösungen von Microsoft den sich wandelnden Complianceanforderungen einen Schritt voraus sein können. Verfolgen Sie eine Zero Trust-Strategie, die den Zugriff kontinuierlich überprüft, vertrauliche Daten schützt und Sicherheitstools in Ihrer Bildungseinrichtung vereinheitlicht. Dieser moderne Ansatz vereinfacht die Einhaltung gesetzlicher Vorschriften, indem er fragmentierte Legacysysteme durch integrierte Lösungen ersetzt, die mehr Transparenz, Kontrolle und Widerstandsfähigkeit bieten.

[Zur Ressource](#)

Leitfaden für Entscheidungstragende zu umfassender Sicherheit: Wichtige Strategien zum Schutz Ihres Unternehmens heute

Microsoft, 2025

Vereinheitlichen Sie die Sicherheit durch die Einführung des umfassenden, integrierten Ansatzes von Microsoft, der auf dem Zero Trust-Framework basiert und den Zugriff über Benutzende, Geräte, Daten und Anwendungen kontinuierlich überprüft. Diese Strategie vereinfacht Abläufe, reduziert Risiken und maximiert den Wert Ihrer Sicherheitsinvestitionen, indem sie Tools konsolidiert und den Schutz in Ihrer digitalen Umgebung effizienter gestaltet.

[Zur Ressource](#)

Modernisieren Sie schnell Ihren Sicherheitsstatus: Nutzen Sie ein Zero Trust-Framework, um Vertrauen bei Ihren Mitarbeitenden, Partnern, Ihrer Kundschaft und bei anderen Stakeholdern aufzubauen

Microsoft, 2025

Entdecken Sie, wie Sie Ihren Sicherheitsstatus stärken können, indem Sie die Führung auf eine gemeinsame Strategie ausrichten, Risiken priorisieren und systematisch die Zero Trust-Prinzipien anwenden, um die Verteidigung zu verbessern. Dieses E-Book unterstützt Organisationen dabei, selbstbewusst auf Bedrohungen zu reagieren, den allgemeinen Sicherheitsstatus zu verbessern und sicherzustellen, dass Fortschritte messbar sind und effektiv an Entscheidungstragende kommuniziert werden.

[Zur Ressource](#)

Schützen Sie Ihre sensibelsten Daten: Schützen Sie Ihre kritischen Ressourcen mit dem Zero Trust-Sicherheitsframework

Microsoft, 2025

Erfahren Sie, wie Sie eine Zero Trust-Strategie implementieren, um vertrauliche Daten in allen Umgebungen – Cloud, On-Premises und mobil – mithilfe automatisierter Kennzeichnung, Verschlüsselung und Zugriffssteuerungen zu identifizieren, zu klassifizieren und zu schützen. Dieses E-Book unterstützt Sie dabei, die Sicherheit zu verbessern, interne und externe Bedrohungen zu reduzieren, Compliance sicherzustellen und gleichzeitig eine nahtlose Zusammenarbeit und Produktivität zu ermöglichen.

[Zur Ressource](#)

Arbeiten Sie von überall aus sicher:
Stärken Sie die Sicherheit mit
einem Zero-Trust-Ansatz

Microsoft, 2025

Bieten Sie sichere Mobil- und Hybridarbeitsumgebungen, indem Sie einen Zero Trust Rahmen einführen, der jede Zugriffsanforderung überprüft, Endpunkte schützt und strenge Identitätskontrollen durchsetzt. Dieser Ansatz reduziert das Risiko von Cyberangriffen, unterstützt flexible Arbeitsumgebungen und gewährleistet Daten- und Gerätesicherheit, ohne die Produktivität zu beeinträchtigen.

[Zur Ressource](#)

SOC für
Studierende: Implementierungsleitfaden

Microsoft, 2025

Erfahren Sie, wie SOC's sowohl die Readiness der Mitarbeitenden als auch die institutionelle Sicherheit stärken, indem sie praktische Erfahrungen, Industriezertifizierungen und die Ausrichtung auf Strategien wie Zero Trust bieten.

[Zur Ressource](#)

KI-Sicherheit und Zero Trust: Agile
Sicherheit für agile Unternehmen

Microsoft, 2024

Schützen Sie Daten, Anwendungen und Infrastruktur durch die Implementierung eines Zero Trust-Sicherheitsframeworks, das den Zugriff überprüft und die Berechtigungen in KI-Systemen begrenzt. Ein Zero Trust-Ansatz für KI-Systeme verbessert den Datenschutz und gewährleistet die Einhaltung gesetzlicher Vorschriften, sodass Unternehmen mit KI innovativ sein können.

[Zur Ressource](#)

Häufige Angriffe und wie Microsoft-
Lösungen für Zero Trust Ihre
Organisation schützen können

Microsoft, 2024

Verstehen Sie, wie Cyberkriminelle Identitäts-, Geräte- und Netzwerkangriffe in ungesicherten Systemen initiieren, und erfahren Sie, wie Microsoft Security-Lösungen und ein Zero Trust-Ansatz Daten, Endpunkte und kritische Infrastrukturen schützen.

[Zur Ressource](#)

Cyber Signals Issue 8 | Bildung unter
Beschuss: Wie Cyberkriminelle unsere
Schulen ins Visier nehmen

Microsoft, 2024

Entdecken Sie, wie offene digitale Umgebungen, die weit verbreitete Nutzung persönlicher Geräte und begrenzte Sicherheitsressourcen zu Cyberangriffen auf K-12-Schulen und Hochschulen führen. Durch die Einführung proaktiver Strategien wie Zero Trust und die Verbesserung von Transparenz und Kontrolle über Netzwerke und Geräte können Schulen und Institutionen sensible Daten besser schützen und das Risiko von Störungen durch immer ausgefeiltere Bedrohungen verringern.

[Zur Ressource](#)

Der grundlegende Leitfaden zu
Zero Trust: Ein führender Ansatz
für KI-optimierte Sicherheit

Microsoft, 2024

Erfahren Sie, wie Sie die Unternehmenssicherheit stärken, indem Sie die Zero-Trust-Architektur von Microsoft anwenden, die den Schutz von Identitäten, Daten, Apps, Endpunkten, Netzwerken, Infrastruktur und KI mithilfe von adaptivem Zugriff und kontinuierlicher Bedrohungsbewertung organisiert. Dieser strukturierte Ansatz senkt Risiken, verbessert die Einhaltung von Compliance-Vorgaben und ermöglicht sichere Innovationen, während er gleichzeitig die Bereitstellung und Verwaltung in der gesamten Organisation vereinfacht.

[Zur Ressource](#)

Microsoft Digital Defense Report 2024

Microsoft, 2024

Entdecken Sie die sich entwickelnde Bedrohungslandschaft, Möglichkeiten zum strategischen Umgang mit Cybersicherheit und die neuen Sicherheitsherausforderungen, die mit der Einführung von KI einhergehen. Dieser Bericht enthält Daten und Statistiken von Microsoft Threat Intelligence, das täglich über 78 Billionen Sicherheitssignale analysiert.

[Zur Ressource](#)

Entdecken Sie, wie Microsoft Security-Lösungen Schulen und Bildungseinrichtungen messbare Vorteile bieten.

The Forrester Wave: Zero Trust-Platforms, 3. Quartal 2025

Forrester, 2025

Erfahren Sie, wie Microsofts strategische Roadmap, Produktfunktionen und Kundenfeedback dazu beitragen, dass Microsoft laut Forrester als führender Anbieter von Zero Trust-Plattformen gilt. Dieser Bericht hebt die Bemühungen von Microsoft hervor, die Identitätsverwaltung über Kern-Sicherheitsprodukte hinweg zu stärken und Organisationen mit Microsoft Security Copilot KI-gestützten Schutz zu bieten.

[Zur Ressource](#)

The Total Economic Impact of Microsoft Sentinel

Forrester, 2024

Entdecken Sie die Vorteile der Modernisierung von Security Operations, indem Sie veraltete Systeme durch Microsoft Sentinel ersetzen, eine cloudbasierte Plattform, die KI und Automatisierung nutzt, um Bedrohungen schneller und effizienter zu erkennen und darauf zu reagieren. Diese Forrester-Studie ergab eine Rendite von 234 %, mit erheblichen Kosteneinsparungen, weniger falschen Positiven und einer verbesserten Teamproduktivität – was Sentinel zu einem strategischen Tool für Führungskräfte im Bildungsbereich macht, die nach skalierbaren, sicheren und kostengünstigen Cybersicherheitslösungen suchen.

[Zur Ressource](#)

New technology: The projected Total Economic Impact of Microsoft Security Copilot

Forrester, 2024

Erfahren Sie, wie Microsoft Security Copilot mithilfe von generative KI messbare Verbesserungen in den Security Operations erzielt, indem Bedrohungserkennung, -untersuchung und -reaktion effizienter gestaltet werden. Die Studie ergab einen durchschnittlichen Produktivitätszuwachs von 46 % bei SecOps-Aufgaben, Kosteneffizienz durch die SecOps-Zentralisierung und einen prognostizierten ROI von 348 %. Dies unterstreicht die Bedeutung der Integration von KI-gesteuerten Tools wie Microsoft Security Copilot in Cybersicherheitsstrategien, um den Schutz zu verbessern und gleichzeitig dem Arbeitskräftemangel entgegenzuwirken.

[Zur Ressource](#)

The Total Economic Impact of Microsoft Security

Forrester, 2023

Lesen Sie, wie Microsoft Security die Effizienz der Cybersicherheit und die Risikominderung durch SIEM-, Compliance- und Identitätsverwaltungslösungen verbessert. Die Studie ergab eine 72-%-ige Verringerung des Risikos einer Sicherheitsverletzung, eine 25-%-ige Reduzierung der Lizenz- und Betriebskosten sowie eine 50-%-ige Steigerung der Effizienz von IT- und Sicherheitsteams.

[Zur Ressource](#)

The Total Economic Impact of Microsoft SIEM and XDR

Forrester, 2022

Entdecken Sie, wie Microsoft SIEM- und XDR-Lösungen die Antwortzeit auf Bedrohungen verkürzen, die Transparenz verbessern und Organisationen bei der Konsolidierung von Anbietern unterstützen. Die Studie ergab eine 65-%-ige Verringerung des Untersuchungsaufwands bei Bedrohungen, eine 88-%-ige Reduzierung der Antwortzeit und jährliche Einsparungen von fast 1,6 Millionen US-Dollar durch die Konsolidierung von Anbietern und Verwaltung.

[Zur Ressource](#)

Ergebnisse aus Wissenschaft und Industrie

Erfahren Sie mehr über die Bedeutung robuster Sicherheits-, Compliance- und Datenschutzmaßnahmen in K-12- und Hochschulumgebungen.

Implementierung einer Zero Trust-Architektur: Allgemeines Dokument

National Institute of Standards and Technology (NIST), 2024

Erfahren Sie, wie Sie eine Zero Trust-Architektur (ZTA) implementieren, die sicheren, autorisierten Zugriff auf Enterprise-Ressourcen in On-Premises- und Multi-Cloud-Umgebungen ermöglicht. Diese Architektur ermöglicht es einer hybriden Belegschaft, von überall, zu jeder Zeit und von jedem Gerät aus auf Ressourcen zuzugreifen, um die Mission der Organisation zu unterstützen. Erfahren Sie, wie Sie ZTA gemäß den in der NIST Special Publication (SP) 800-207, Zero Trust Architecture, beschriebenen Konzepten und Prinzipien implementieren.

[Zur Ressource](#)

The NIST Cybersecurity Framework (CSF) 2.0

National Institute of Standards and Technology (NIST), 2024

Erfahren Sie, wie Sie Cyberrisiken mit dem NIST Cybersecurity Framework (CSF) 2.0 managen können. Das CSF bietet eine Taxonomie übergeordneter Cybersicherheitsstandards und -ergebnisse, die von Schulen und Institutionen genutzt werden kann, um Cybersicherheitsbemühungen besser zu verstehen, zu bewerten, zu priorisieren und zu kommunizieren.

[Zur Ressource](#)

2024 Educause Horizon Report: Cybersecurity and privacy edition

Educause, 2024

Entdecken Sie, wie Hochschulen Cybersicherheit und Datenschutz vor dem Hintergrund des raschen technologischen und geopolitischen Wandels stärken können. Der Bericht betont die Bedeutung der Einführung von Rahmenwerken wie Zero Trust, der Durchführung von Schulungen zum Sicherheitsbewusstsein und der Verbesserung des Risikomanagements, um institutionelle Daten und die Privatsphäre der Studierenden zu schützen.

[Zur Ressource](#)

First Annual Generative AI Study: Business rewards vs. security risks

Information Security Media Group (ISMG), 2023

Gewinnen Sie wertvolle Einblicke in die unterschiedlichen Perspektiven von Führungskräften und Informationssicherheitsbeauftragten (CISOs) zu generative KI – ihre Chancen, Risiken und Implikationen. Diese Studie bietet eine umfassende Momentaufnahme der Perspektiven dieser Schlüsselrollen in verschiedenen Branchen und Sektoren.

[Zur Ressource](#)

Protecting our future: Partnering to safeguard K-12 organizations from cybersecurity threats

Cybersecurity and Infrastructure Security Agency (CISA), 2023

Verstehen Sie die Cybersicherheitsrisiken, denen Grund- und weiterführende Schulen ausgesetzt sind, und wie Sie Empfehlungen zum Schutz von Personen und Daten umsetzen können. Die wichtigsten Erkenntnisse des Berichts umfassen die Implementierung hochwirksamer Cybersicherheitsprotokolle, das Erheben der Sicherheit zur obersten Priorität in Schulen und die Zusammenarbeit mit lokalen, regionalen und nationalen Behörden zur Risikominderung.

[Zur Ressource](#)

Implementing phishing-resistant MFA

Cybersecurity and Infrastructure Security Agency (CISA), 2022

Erfahren Sie, warum die Verwendung von Multi-Faktor-Authentifizierung (MFA) wichtig ist, um das Risiko zu verringern, dass Cyberkriminelle mit kompromittierten Anmeldeinformationen Zugriff auf Daten, Netzwerke und Informationssysteme erhalten. Befolgen Sie die Empfehlungen zur Umsetzung einer phishing-resistenten Multi-Faktor-Authentifizierung und eines Zero Trust-Ansatzes für die Sicherheit.

[Zur Ressource](#)

Planung von Maßnahmen bei Cybersicherheitsvorfällen für Hochschulen und Universitäten

U.S. Department of Education, ND

Verbessern Sie den Sicherheitsstatus durch bewährte Methoden des Risikomanagements, die im Einklang mit dem NIST CSF für Einrichtungen der Hochschulbildung stehen. Erfahren Sie, warum es wichtig ist, einen Plan für die Reaktion auf Vorfälle zu haben, um Netzwerkschäden zu begrenzen, die Schadensbehebung zu beschleunigen und die Strafverfolgungsbehörden bei der Identifizierung und Festnahme von Tätern zu unterstützen.

[Zur Ressource](#)

Glossar der Begriffe

Informieren Sie sich über häufig verwendete Begriffe im Kontext der Cybersicherheit in der Bildung. Weitere Begriffe und Definitionen finden Sie unter „National Initiative for Cybersecurity Careers and Studies“.

Zugriff: Die Fähigkeit und die Mittel, mit einem System zu kommunizieren oder zu interagieren, Systemressourcen zur Verarbeitung von Informationen zu verwenden, Kenntnisse über im System gespeicherte Informationen zu erlangen oder Systemkomponenten und -funktionen zu steuern

Authentifizierung: Der Prozess der Überprüfung der Identität oder anderer Attribute von Benutzenden, Prozessen oder Geräten.

Backdoor: Jede Methode, mit der autorisierte Benutzende oder nicht autorisierte Benutzende die üblichen Sicherheitsmaßnahmen umgehen und Zugriff mit höchsten Rechten (auch bekannt als Root-Zugriff) auf einem Computersystem, einem Netzwerk oder einer Softwareanwendung erlangen.

Sicherheitsverletzung: Jeder erhebliche Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit eines Informationssystems oder eine schwerwiegende Beeinträchtigung der Sicherheit oder Resilienz betrieblicher Systeme, die durch unbefugte Nutzung verursacht wird.

Distributed Denial-of-Service (DDoS): Eine Form der Cyberkriminalität, bei der ein Angreifer ein Ziel mit Internetverkehr überflutet, um den Zugriff auf verbundene Onlinedienste und Websites zu verhindern.

Verschlüsselung: Der Prozess, Daten in eine Form umzuwandeln, die für unbefugte Personen nicht leicht zu verstehen ist

Firewall: Ein Gerät oder eine Software, das bzw. die den Netzwerkdatenverkehr anhand von Regeln kontrolliert, die festlegen, welcher Zugriff gestattet oder untersagt ist

Reaktion auf Vorfälle: Alle Aktivitäten, die sich mit den kurzfristigen, direkten Auswirkungen eines Vorfalls befassen, einschließlich der kurzfristigen Wiederherstellung

Plan für die Reaktion auf Vorfälle: Ein Satz vorgegebener und dokumentierter Verfahren zur Erkennung und Reaktion auf einen Cybervorfall

Insiderbedrohung: Bezieht sich auf das Risiko, dass jemand mit autorisiertem Zugriff oder Wissen über die Ressourcen einer Organisation diese nutzen könnte, um Schaden anzurichten.

Schadsoftware: Software, die den Betrieb eines Systems durch Ausführen einer nicht autorisierten Funktion oder eines nicht autorisierten Prozesses beeinträchtigt

Schadensminderung: Einsatz einer oder mehrerer Sicherheitsmaßnahmen zur Verringerung der Wahrscheinlichkeit eines unerwünschten Ereignisses und/oder zur Begrenzung seiner Folgen

Multi-Faktor-Authentifizierung (MFA): Ein Verfahren zur Bestätigung der Identität einer benutzenden Person (Authentifizierung), bei dem mehr als eine Authentifizierungsmethode wie ein Kennwort, eine PIN, ein Fingerabdruck oder eine Gesichtserkennung verwendet wird.

Passkeys: Eine Form der Multi-Faktor-Authentifizierung, die Kryptografie mit öffentlichem Schlüssel in Kombination mit biometrischen Verfahren wie Fingerabdruck- und Gesichtserkennung oder einer Geräte-PIN verwendet, um die Identität der besitzenden Person des Kontos zu verifizieren.

Kennwortlos: Eine Authentifizierungsmethode, bei der sich eine Benutzerin oder ein Benutzer bei einem Computersystem anmelden kann, ohne ein Kennwort oder ein anderes wissensbasiertes Geheimnis eingeben zu müssen.

Phishing: Ein Cyberangriff, bei dem durch Täuschung Personen dazu gebracht werden, persönliche Informationen wie Kennwörter oder personenbezogene Informationen (PII) preiszugeben, um vertrauliche Daten zu stehlen oder zu beschädigen.

Datenschutz: Die Sicherstellung, dass die Vertraulichkeit und der Zugang zu bestimmten Informationen über eine Entität geschützt sind.

Ransomware: Eine Art von Malware- oder Phishing-Cyber-Sicherheitsangriff, der Dateien und Ordner auf einem Computer, Server oder Gerät zerstört oder verschlüsselt, sodass ein Cyberkrimineller Lösegeld verlangen kann, um die verschlüsselten Daten zu entsperren.

Rotes Team: Eine Gruppe, die für die Nachahmung eines Angriffs oder der Missbrauchsfähigkeiten eines potenziellen Gegners in Hinblick auf die Cybersicherheitsstrategie des Unternehmens autorisiert und organisiert ist.

Resilienz: Die Fähigkeit, unter widrigen Bedingungen zu operieren, dabei wesentliche Betriebsfunktionen aufrechtzuerhalten und den Betrieb zeitnah wiederherzustellen

Risiko: Das Potenzial für ein unerwünschtes oder nachteiliges Ergebnis, das sich aus einem Vorfall, einem Ereignis oder einer Begebenheit ergibt, bestimmt durch die Wahrscheinlichkeit, dass eine bestimmte Bedrohung eine bestimmte Schwachstelle ausnutzt.

Risikobewertung: Der Prozess der Identifizierung, Schätzung, Bewertung und Priorisierung von Risiken für den Betrieb, Vermögenswerte oder Einzelpersonen

SecOps (Sicherheitsoperationen): Eine Methodik, die von IT-Führungskräften implementiert wird, um die Verbindung, Zusammenarbeit und Kommunikation zwischen IT-Sicherheits- und IT-Betriebsteams zu verbessern.

Security Information and Event Management (SIEM): Eine Sicherheitslösung, die Unternehmen dabei unterstützt, Bedrohungen zu erkennen, bevor der Betrieb gestört wird.

Social Engineering: Einsatz von Täuschung, psychologischen Tricks, Überredung und Ausnutzung, um Benutzende zu Handlungen zu verleiten, die dazu führen, dass versehentlich vertrauliche Informationen und Daten preisgegeben werden

Spam: Der Missbrauch elektronischer Kommunikationssysteme zum wahllosen Versenden unerwünschter Spam-Nachrichten

Bedrohung: Jedes Ereignis oder jeder Umstand, der sich durch unbefugten Zugriff, Zerstörung, Offenlegung, Änderung oder Dienstverweigerung negativ auf den Betrieb, die Vermögenswerte oder Personen auswirken kann

Bedrohungsakteure (Cyberkriminelle): Personen oder Gruppen, die schädliche digitale Aktivitäten durchführen, um Systeme zu kompromittieren, Daten zu stehlen oder Dienste zu stören

Sicherheitsrisiko: Eine Schwachstelle in einem Sicherheitssystem, einem Sicherheitsverfahren, internen Kontrollen oder der Implementierung, die von einer Bedrohung ausgenutzt oder ausgelöst werden kann.

XDR – Extended Detection and Response (Erweiterte Erkennung und Reaktion): Ein Ansatz für die Cybersicherheit, der Erkennungs-, Untersuchungs- und Reaktionsfunktionen über eine größere Bandbreite von Bereichen integriert, einschließlich der Endpunkte einer Organisation, Hybrid-Identitäten, Cloudanwendungen und Workloads, E-Mail- und Datenspeicher.

Zero Trust: Ein Ansatz für Cybersicherheit, bei dem davon ausgegangen wird, dass alles eine Bedrohung darstellt; Zero Trust folgt drei Prinzipien: Explizite Überprüfung; Geringstprivilegierter Zugriff; Annahme einer Sicherheitsverletzung

Checkliste für die nächsten Schritte

- ☐ Prüfen Sie Forschungsergebnisse zu Zero Trust und identifizieren Sie, wie Ihre Institution die drei Prinzipien auf Identitäten, Endpunkte, Apps, Infrastruktur, Daten und Netzwerke anwenden kann.
- ☐ Teilen Sie die quantifizierbaren Vorteile der Microsoft Security Lösungen mit IT-Fachleuten, Finanzverantwortlichen und Führungskräften.
- ☐ Entdecken Sie Empfehlungen und Richtlinien von Behörden wie CISA, NIST und dem US-Bildungsministerium.



Microsoft und das Microsoft-Logo sind Marken von Microsoft oder seinen Tochtergesellschaften. Andere Namen und Marken können Eigentum Dritter sein.

Copyright © 2026 Microsoft | 1.0