



REPORT

Ransomware- Report 2026: Bildungswesen

Ergebnisse einer unabhängigen Umfrage unter 226 IT- und Cybersicherheits-Verantwortlichen aus 17 Ländern, deren Unternehmen und Organisationen im letzten Jahr von Ransomware betroffen waren.

Einleitung

Willkommen bei der sechsten Ausgabe des jährlichen Sophos Ransomware-Reports im Bildungswesen, in dem die Realität von Ransomware sowohl für Grund- und weiterführende Schulen (in der Regel für Schüler unter 18 Jahren) als auch für Hochschulen (Universitäten, Hochschulen und gleichwertige Einrichtungen – in der Regel für Studierende über 18 Jahren) im Jahr 2026 aufgezeigt wird.

Der diesjährige Report wirft auch einen neuen Blick auf bislang unerforschte Bereiche, u. a. wo Angriffe in der Umgebung beginnen, die Abwehrrolle von Multi-Faktor-Authentifizierung (MFA) und Firewalls sowie den Zusammenhang zwischen Identitätsangriffen und Ransomware.

Dieser Report basiert auf den realen Erfahrungen von 226 IT- und Cybersecurity-Verantwortlichen im Bildungswesen, 131 aus Grund- und weiterführenden Schulen und 95 aus Hochschulen, die im vergangenen Jahr von Ransomware betroffen waren.

- Angriffs- und Abwehrmethoden
- Datenverschlüsselung und -wiederherstellung
- Lösegeldforderungen und -zahlungen
- Wirtschaftliche Folgen und Auswirkungen auf Mitarbeitende

Hinweis: In diesem Report bezieht sich „Gesamtumfrage“ auf Ergebnisse von Befragten aus allen befragten Branchen. Die 226 Befragten aus dem Bildungssektor sind Teil einer breiteren Gruppe von 2.158 Befragten aus 15 Branchen.

Informationen zu den Ergebnissen

Dieser Report basiert auf den Ergebnissen einer unabhängigen Befragung im Auftrag von Sophos. Im Rahmen der Befragung wurden Fragen zu den Erfahrungen von Unternehmen und Organisationen mit Ransomware-Angriffen und identitätsbasierten Angriffen gestellt, wobei die Lösegeldzahlungsraten, die Wiederherstellungskosten, die Wiederherstellungsdauer und viele weitere Kennzahlen im Jahresvergleich erfasst wurden. Die Antworten wurden von Januar bis März 2026 erhoben und basieren auf den Erfahrungen der Befragten aus den letzten 12 Monaten.

Die Befragten stammen aus 17 Ländern, einer Vielzahl von Branchen aus dem öffentlichen und privaten Sektor sowie aus Unternehmen und Organisationen unterschiedlicher Größe (zwischen 100 und 5.000 Mitarbeitenden), deren Verteilung einer Normalverteilung folgte und über die sechsjährige Laufzeit der Befragung hinweg proportional konstant blieb. Alle Finanzdaten sind in US-Dollar angegeben.

Wichtigste Erkenntnisse

- **Identitätsangriffe, insbesondere per E-Mail, waren im Bildungswesen häufig.**
 - 77 % der Hochschulen und 71 % der Grund- und weiterführenden Schulen bestätigten, dass ihr Ransomware-Angriff auch ihr schwerwiegendster Identitätsangriff war. Beides liegt über der Gesamtumfragequote von 67 % (sektorübergreifend).
 - Schädliche E-Mails waren die Hauptursache für Ransomware-Angriffe in Grund- und weiterführenden Schulen (31 %) und Hochschulen (29 %).
 - Identitätsbasierte Ansätze (z. B. schädliche E-Mail, Phishing, kompromittierte Anmeldedaten oder Brute-Force-Angriffe) initiierten 85 % der Angriffe im gesamten Bildungswesen. Dieser Wert liegt über dem branchenweiten Wert von 79 %.
- **Betriebliche Schwachstellen waren im Bildungswesen stärker ausgeprägt als in der Gesamtumfrage (alle Branchen).**
 - Die entscheidende Lücke im Hochschulwesen war die Expertise: 53 % gaben an, dass sie nicht über das nötige Fachwissen verfügten, um den Angriff rechtzeitig zu erkennen und zu stoppen, verglichen mit 35 % bei der Gesamtbefragung.
 - Die größten betrieblichen Ursachen der Grund- und weiterführenden Schulen waren menschliches Versagen (52 %), mangelnder Schutz (47 %), unbekannte Sicherheitslücken (42 %) sowie fehlendes Personal oder fehlende Kapazitäten (41 %).
- **Verschlüsselungen im Rahmen von Ransomware-Angriffen sind in Grund- und weiterführenden Schulen stark gestiegen.**
 - Die Datenverschlüsselungsrate der Grund- und weiterführenden Schulen hat sich mehr als verdoppelt und ist von 29 % im Jahr 2025 auf 61 % im Jahr 2026 gestiegen.
 - 58 % der Angriffe auf den Bildungssektor führten zu verschlüsselten Daten, was fast der Gesamtumfragequote von 56 % entspricht.
- **Bildungseinrichtungen verließen sich bei der Wiederherstellung von Daten stark auf Backups.**
 - 77 % der Grund- und weiterführenden Schulen stellten verschlüsselte Daten aus Backups wieder her, mehr als die Gesamtumfragequote von 66 %.
 - 69 % der Hochschulen nutzten ebenfalls Backups zur Wiederherstellung.
- **Bildungseinrichtungen zahlten weniger als in der Gesamtumfrage, wiesen jedoch mehr Lösegeldzahlungen von 5 Mio. US\$ oder mehr auf.**
 - Die durchschnittlichen Lösegeldforderungen (Medianwert) im Bildungswesen lagen bei 775.200 US\$ (ggü. 698.000 US\$ in der Gesamtumfrage), während die durchschnittliche Lösegeldzahlung (Medianwert) lediglich 515.000 US\$ betrug (ggü. 769.000 US\$ in der Gesamtumfrage).
 - Die mittleren Lösegeldforderungen im Bildungswesen sind zwei Jahre in Folge gesunken, während die Zahlungen vom Bericht 2025 bis 2026 um 15.000 US-Dollar gestiegen sind.
 - Bildungseinrichtungen zahlten mit höherer Wahrscheinlichkeit 5 Mio. US\$ oder mehr (23 % ggü. 16 % in der Gesamtumfrage).
- **Die Bereinigung kostete mehr und dauerte länger im Bildungswesen.**
 - Die durchschnittlichen Bereinigungskosten im Bildungswesen beliefen sich auf 2,26 Mio. US\$ und lagen damit über dem Gesamtumfragewert von 1,7 Mio. US\$.
 - Die Bereinigungskosten im Bildungswesen sind seit dem Bericht 2025 von 1,66 Mio. US\$ auf 2,26 Mio. US\$ gestiegen, wobei die Kosten für Hochschulen um mehr als 1 Mio. US\$ gestiegen sind.
 - 26 % der Bildungseinrichtungen benötigten ein bis drei Monate, um sich vollständig von einem Ransomware-Angriff zu erholen. Dies entspricht etwa der doppelten Branchenrate von 14 %.
 - Grund- und weiterführende Schulen hatten den größten Anteil an langfristigen Wiederherstellungen: 31 % brauchten einen Monat oder länger, um den Normalbetrieb wiederherzustellen – länger als jede andere Branche.
- **Die Belastung der Sicherheitsteams hat zugenommen.**
 - 53 % der Hochschulteams berichteten von erhöhtem Druck durch Führungskräfte, verglichen mit 40 % in allen Branchen.
 - Rund 39 % der Bildungsteams gaben an, dass Mitarbeiter aufgrund von Stress oder psychischen Problemen nicht zur Verfügung stehen, verglichen mit 29 % in allen Branchen.

Angriffs- und Abwehrmethoden

Ursachen von Angriffen

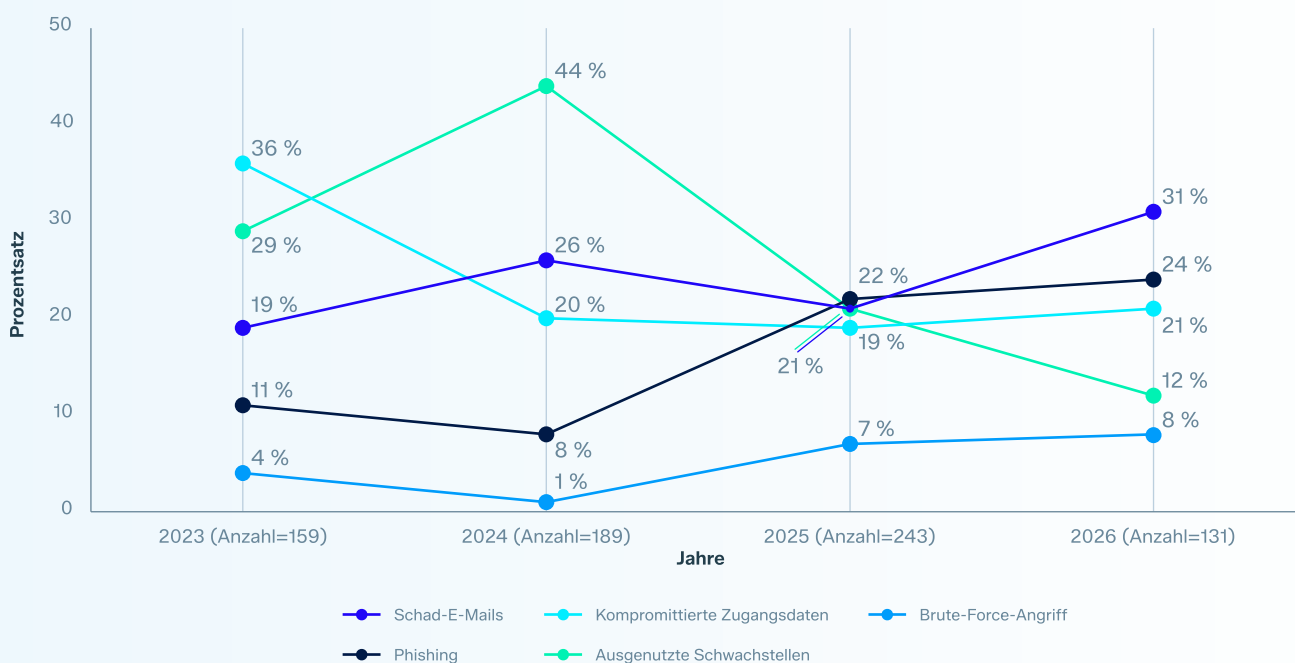
Die diesjährigen Bildungsdaten spiegeln den gleichen Wandel in allen Branchen wider: Identitätsbasierte Angriffe nehmen zu.

Schädliche E-Mails waren die häufigste technische Ursache in Grund- und weiterführenden Schulen (31 %), gefolgt von Phishing (24 %) und kompromittierten Anmeldedaten (21 %). Ausgenutzte Schwachstellen gingen auf 12 % zurück, was den allgemeinen Rückgang in der Gesamtumfrage (alle Branchen) auf 18 % widerspiegelt.

85 %

Der Anteil der Angriffe auf Bildungseinrichtungen, die mit einem identitätsbasierten Ansatz begannen (z. B. schädliche E-Mail, Phishing, kompromittierte Anmeldedaten oder Brute-Force-Angriffe), liegt über der Gesamtumfragequote von 79 %.

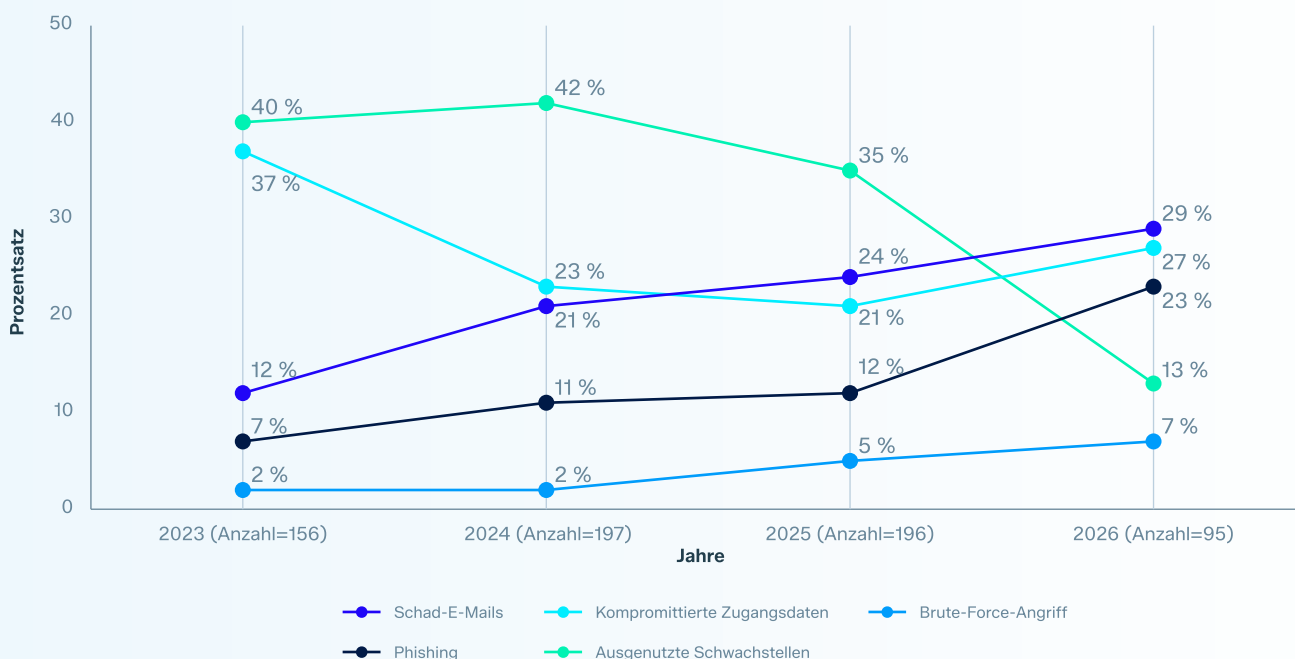
Technische Ursachen von Ransomware-Angriffen 2023–2026: Grund- und weiterführende Schulen



Kennen Sie die Ursache des Ransomware-Angriffs auf Ihr Unternehmen im vergangenen Jahr? Downloads und „Ich weiß nicht“ wurden aus visuellen Gründen aus dem Diagramm ausgeschlossen. Prozentsätze dürfen nicht 100 % betragen. Anzahl der erhaltenen Antworten jeweils in Klammer.

Auch Hochschulen meldeten einen Rückgang ausgenutzter Schwachstellen. Dieser Vektor fiel im Bericht 2026 auf 13 %, gegenüber 35 % im Jahr 2025. **Schädliche E-Mails (29 %) und kompromittierte Zugangsdaten (27 %) sind nahezu gleichauf die Hauptursachen**, dicht gefolgt von Phishing mit 23 %. Sowohl im Bereich der Grund- und weiterführenden Schulen als auch in Hochschulen werden E-Mail-basierte Angriffe als Hauptursachen genannt, was mit der Gesamtumfrage übereinstimmt, in der schädliche E-Mails (26 %) und Phishing (24 %) zusammen die Hälfte aller Vorfälle ausmachen.

Technische Ursachen von Ransomware-Angriffen 2023–2026: Hochschulen

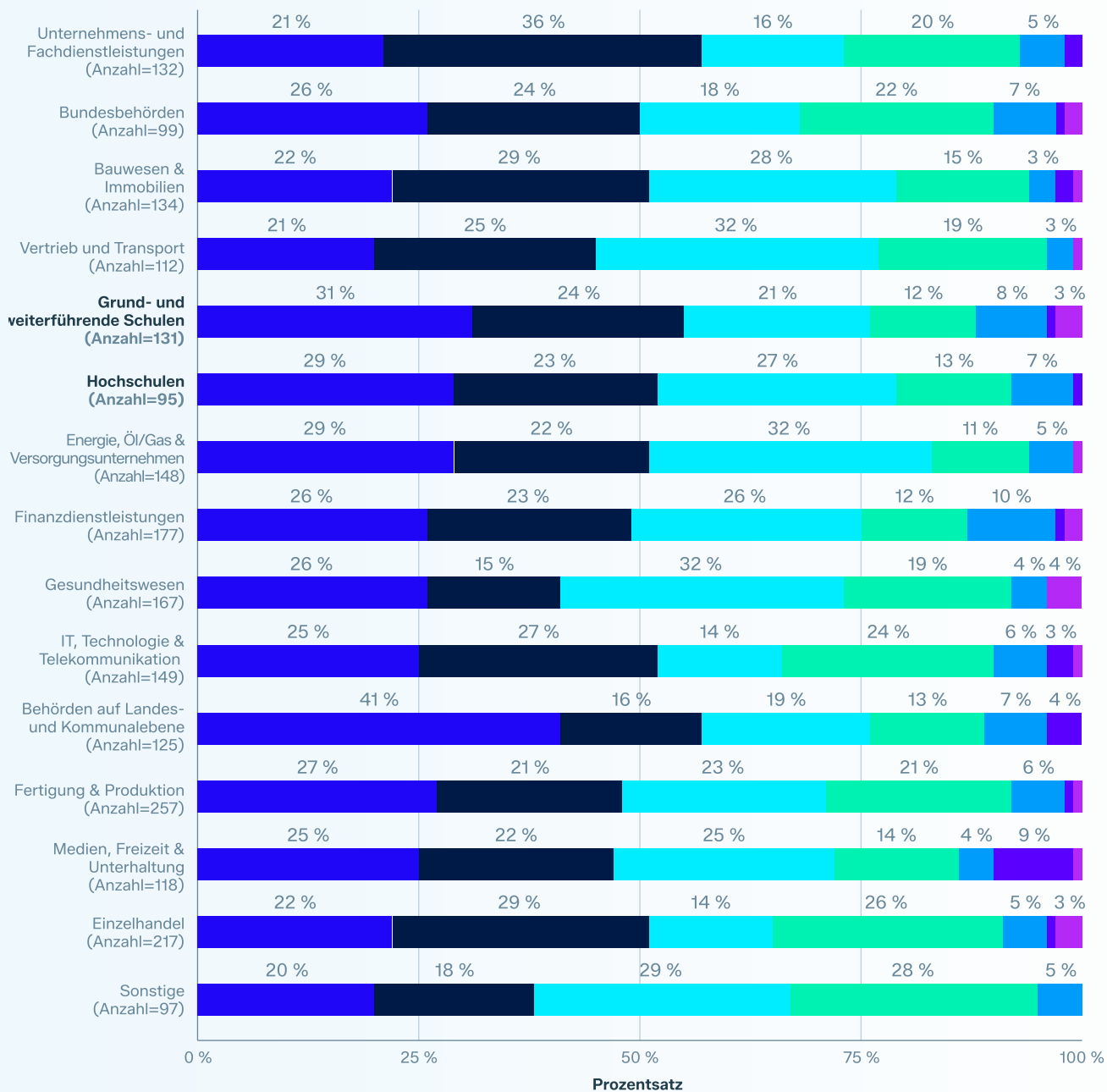


Kennen Sie die Ursache des Ransomware-Angriffs auf Ihr Unternehmen im vergangenen Jahr? Downloads und „Ich weiß nicht“ wurden aus visuellen Gründen aus dem Diagramm ausgeschlossen. Prozentsätze dürfen nicht 100 % betragen. Anzahl der erhaltenen Antworten jeweils in Klammer.

Zusammengenommen machten **identitätsbasierte Vektoren (z. B. schädliche E-Mail, Phishing, kompromittierte Anmeldedaten und Brute-Force-Angriffe) 85 % der Angriffe auf Bildungseinrichtungen aus, was über der Gesamtumfragequote von 79 % liegt**. Die Hochschulen lagen mit 86 % am höchsten, gefolgt von den Grund- und weiterführenden Schulen mit 84 %. Mit anderen Worten: Rund sechs von sieben Angriffen auf Bildungseinrichtungen begannen mit einem identitätsbasierten Ansatz, was unterstreicht, warum Identitätssicherheit für die Verteidigung des Sektors von zentraler Bedeutung ist.

Der Bildungssektor spiegelt den sektorübergreifenden Wandel hin zu mehr E-Mail-basierten Angriffen und weniger Berichten über ausgenutzte Schwachstellen wider. **Sophos-Experten rechnen jedoch mit einem erneuten Anstieg von Exploits**, da Unternehmen und Organisationen Schwierigkeiten haben, mit Patches für von Frontier AI gefundenen Schwachstellen Schritt zu halten.

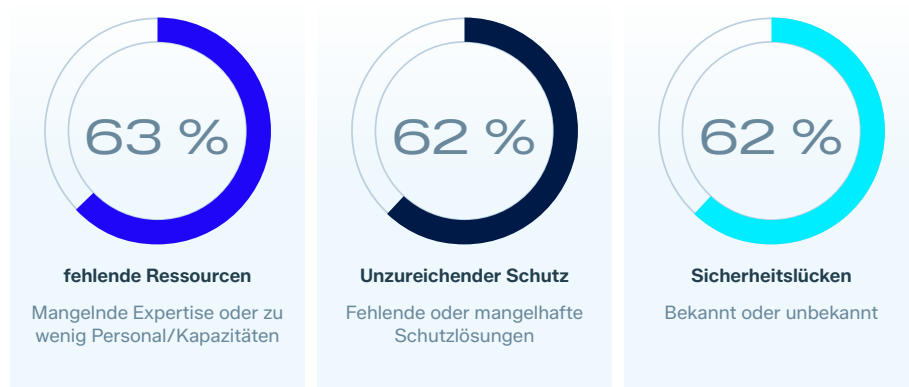
Technische Ursache nach Branche (2026)



Kennen Sie die Ursache des Ransomware-Angriffs auf Ihr Unternehmen im vergangenen Jahr? Anzahl der erhaltenen Antworten jeweils in Klammer.

Was Unternehmen/Organisationen anfällig machte

Bildungseinrichtungen nannten eine Vielzahl von Herausforderungen mit Schutz-, Ressourcen- und Sicherheitslücken. In den drei konsolidierten Kategorien nannten 63 % der Bildungseinrichtungen Ressourcenprobleme (fehlendes Personal oder fehlende Qualifikationen), gefolgt von Schutzproblemen (62 %) und Sicherheitslücken (62 %).



Warum wurde Ihr Unternehmen Ihrer Meinung nach Opfer eines Ransomware-Angriffs? n=226.
Zusammengefasste Antworten.

Im kombinierten Bildungswesen wurde für nahezu jede betriebliche Ursache eine höhere Quote als in der Gesamtbefragung gemeldet, wobei bekannte Sicherheitslücken die einzige Ausnahme waren. Betrachtet man Grund- und weiterführende Schulen getrennt von Hochschulen, offenbaren sich zwei unterschiedliche Schwächen.

Die wichtigste Schwachstellen von Hochschulen war Expertise. 53 % gaben an, dass sie nicht über die Fähigkeiten oder das Wissen verfügten, um den Angriff rechtzeitig zu erkennen und zu stoppen, verglichen mit 35 % bei der Gesamtbefragung – ein Unterschied von 18 Prozentpunkten und ihre größte Schwachstelle.

Die Schwachstellen bei Grund- und weiterführenden Schulen konzentrierten sich auf Kapazitäten und Tools. 52 % der Grund- und weiterführenden Schulen nannten menschliches Versagen (ggü. 35 % in allen Branchen), 47 % mangelnden Schutz und 41 % mangelndes Personal oder fehlende Kapazitäten.

Betriebliche Ursachen: Grund- und weiterführende Schulen sowie Hochschulen im Vergleich zu allen Branchen

Betriebliche Ursache	Grund- und weiterführende Schulen (Anzahl=131)	Hochschulen (Anzahl=95)	Alle Branchen (Anzahl=2.158)
Fehlender Schutz	47 %	36 %	36 %
Unbekannte Sicherheitslücke	42 %	38 %	36 %
Bekannte Sicherheitslücke	33 %	35 %	36 %
Zu wenig Personal/Kapazitäten	41 %	37 %	35 %
Menschliches Versagen	52 %	36 %	35 %
Mangelnde Expertise	33 %	53 %	35 %
Schlechter Schutz	38 %	39 %	33 %

Warum wurde Ihr Unternehmen/Ihre Organisation Ihrer Meinung nach Opfer eines Ransomware-Angriffs? Mehrere Antworten zulässig. Anzahl der erhaltenen Antworten jeweils in Klammer.

53 %

Der Anteil der Hochschulopfer, die angaben, nicht über die Fähigkeiten oder das Wissen zu verfügen, um den Angriff rechtzeitig zu erkennen und zu stoppen, liegt 18 Punkte über der Gesamtumfrage und ihrer größten Schwachstelle.

Im Vergleich zu anderen Branchen hatte das Bildungswesen mit mangelndem Schutz und mangelndem Fachwissen zu kämpfen. Die folgende Tabelle zeigt Branchen in der Spalte der von ihnen am häufigsten genannten betrieblichen Ursache.

Wichtigste betriebliche Ursachen für Ransomware-Angriffe nach Branche

FEHLENDER SCHUTZ	UNBEKANNTE SICHERHEITSLÜCKE	BEKANNTE SICHERHEITSLÜCKE	ZU WENIG PERSONAL/KAPAZITÄTEN	MANGELNDE EXPERTISE	SCHLECHTER SCHUTZ	MENSCHLICHES VERSAGEN
Wir hatten nicht die richtigen Cybersicherheits-Produkte und -Services	Wir hatten eine Schwachstelle in unserer Abwehr, die uns nicht bewusst war.	Wir hatten mindestens eine Schwachstelle in unserer Abwehr, die wir kannten, aber nicht behoben hatten.	Wir hatten nicht ausreichend Cybersicherheitsexperten, die unsere Systeme überwacht haben	Wir hatten nicht ausreichend Fähigkeiten oder Wissen, um den Angriff rechtzeitig zu erkennen und zu stoppen.	Unsere Cybersicherheits-Produkte und -Services konnten den Angriff nicht aufhalten.	Unsere Teams haben einen Fehler gemacht/ Prozesse nicht ordnungsgemäß befolgt
Unternehmens- und Fachdienstleistungen (44 %) Sonstige (42 %) Energie, Öl/Gas & Versorgungsunternehmen* (37 %)	IT, Technologie & Telekommunikation (42 %) Bauwesen & Immobilien (41 %)	Finanzdienstleistungen (44 %) Einzelhandel (38 %) Energie, Öl/Gas & Versorgungsunternehmen* (37 %)	Medien, Freizeit & Unterhaltung (43 %) Behörden auf Landes- und Kommunalebene (42 %)	Hochschulen (53 %) Gesundheitswesen (47 %) Bundesbehörden (43 %)	Vertrieb und Transport (38 %)	Grund- und weiterführende Schulen (52 %) Fertigung & Produktion (39 %)

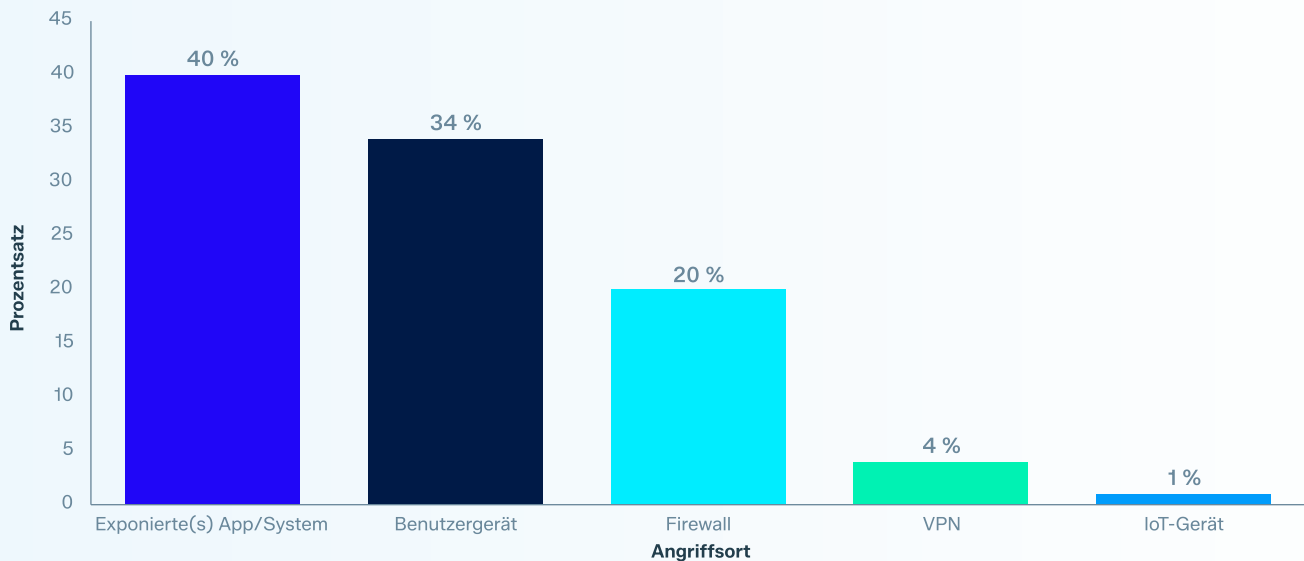
Warum wurde Ihr Unternehmen/Ihre Organisation Ihrer Meinung nach Opfer eines Ransomware-Angriffs? Mehrere Antworten zulässig. Branchen mit mehrere Ursachen sind mit einem Sternchen (*) gekennzeichnet. Anzahl=2.158.

Wo Angriffe beginnen

Neue Forschungsergebnisse in diesem Jahr stellen die Frage, wo Angriffe in der Umgebung begonnen haben, insbesondere bei Vorfällen, die mit einer ausgenutzten Schwachstelle, kompromittierten Anmeldedaten oder einem Brute-Force-Angriff begannen.

Im Bildungswesen waren exponierte Anwendungen und Systeme der häufigste Eintrittspunkt (40 %), gefolgt von Benutzergeräten (34 %) und Firewalls (20 %). Diese Zahlen bilden die Gesamtumfrage genau ab (38 %, 30 % bzw. 21 %), sodass die Bildung hier keine sinnvollen Unterschiede zeigt.

Wo Ransomware-Angriffe beginnen: kombiniertes Bildungswesen



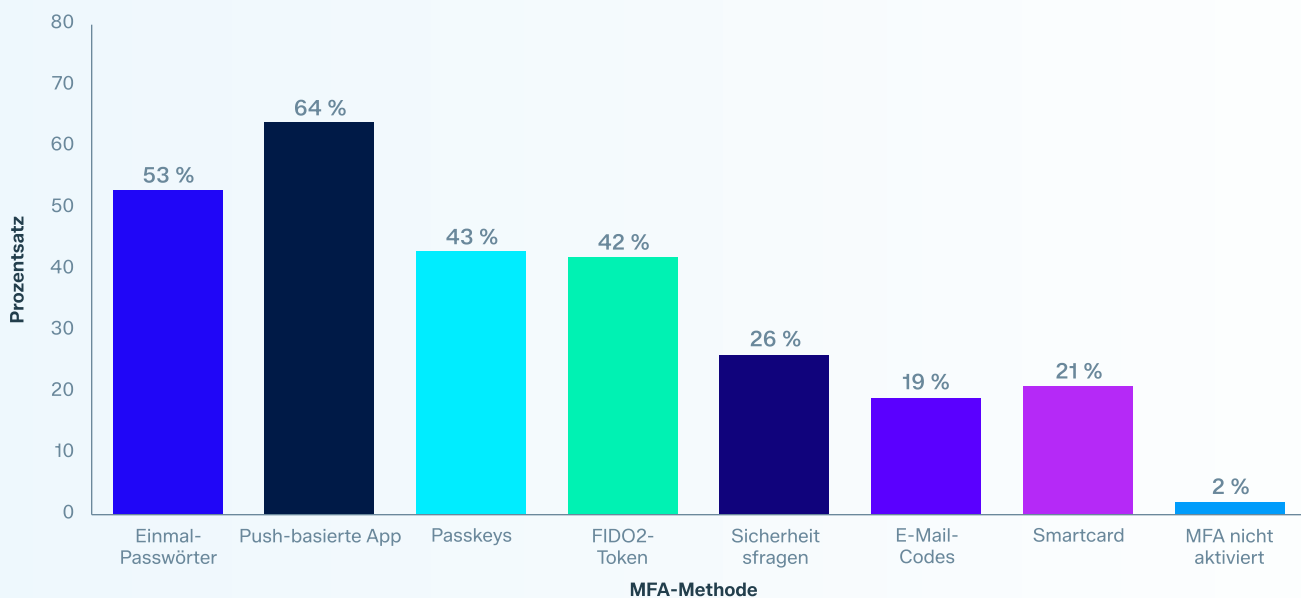
Sie sagten, die Ursache sei eine ausgenutzte Schwachstelle, kompromittierte Anmeldedaten oder ein Brute-Force-Angriff. Wo ist das in Ihrer Umgebung passiert? Kombination aus Hochschulen sowie Grund- und weiterführenden Schulen. Anzahl=99.

Die Rolle von Multi-Faktor-Authentifizierung (MFA)

Wir haben auch die MFA-Methoden untersucht, die zum Zeitpunkt des Angriffs bei Bildungseinrichtungen vorhanden waren, deren Angriff mit Kompromittierten Anmeldedaten begann. Fast alle Opfer im Bildungswesen hatten irgendeine Art von MFA aktiviert (98 %), was dem allgemeinen Umfrageergebnis (97 %) entspricht, wonach MFA bei den meisten auf Zugangsdaten basierenden Angriffen vorhanden war.

Von den Bildungseinrichtungen, die zu MFA befragt wurden, hatten dennoch 81 % ihre Daten verschlüsselt. Dies deutet darauf hin, dass entweder MFA nicht umfassend auf allen kritischen Systemen implementiert wurde, Angreifer Wege fanden, den MFA-Schutz zu umgehen, oder die Angriffsvektoren nicht ausschließlich auf die Kompromittierung von Anmeldedaten setzten.

Zum Zeitpunkt des Angriffs aktivierte MFA-Methoden: kombiniertes Bildungswesen

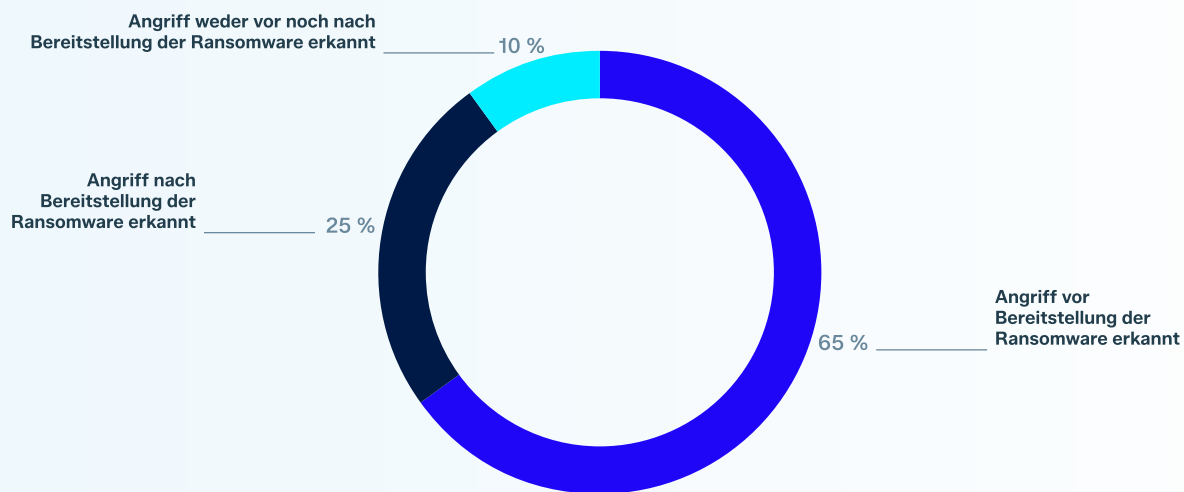


Welche Art von Multi-Faktor-Authentifizierung war zum Zeitpunkt des Angriffs aktiviert? Mehrere Antworten zulässig. Basis: Der Angriff erfolgte aufgrund kompromittierter Anmeldedaten. n=503 Kombination aus Hochschulen sowie Grund- und weiterführenden Schulen. Anzahl=53.

Die Rolle von Firewalls

Im Bildungsbereich identifizierten Firewalls die meisten Angriffe, aber sie halfen nicht immer, sie zu stoppen. 65 % der Anbieter gaben an, dass ihre Firewall den Angriff vor der Bereitstellung der Ransomware erkannt hat, 25 % gaben an, dass sie den Angriff danach erkannt hat und 10 % gaben an, dass sie den Angriff überhaupt nicht erkannt hat. Dies spiegelt die Gesamtbefragung wider (61 %, 32 % und 7 %) mit einer leichten Verschiebung hin zu den beiden Enden des Spektrums.

Welche Rolle spielte Ihre Firewall bei der Identifizierung des Angriffs?



Welche Rolle spielte Ihre Firewall bei der Identifizierung des Angriffs? Kombination aus Hochschulen sowie Grund- und weiterführenden Schulen. Anzahl=226.

In Fällen, in denen der Angriff frühzeitig erkannt wurde, wurden die Daten der Betroffenen im Bildungswesen dennoch in 51 % der Fälle verschlüsselt.

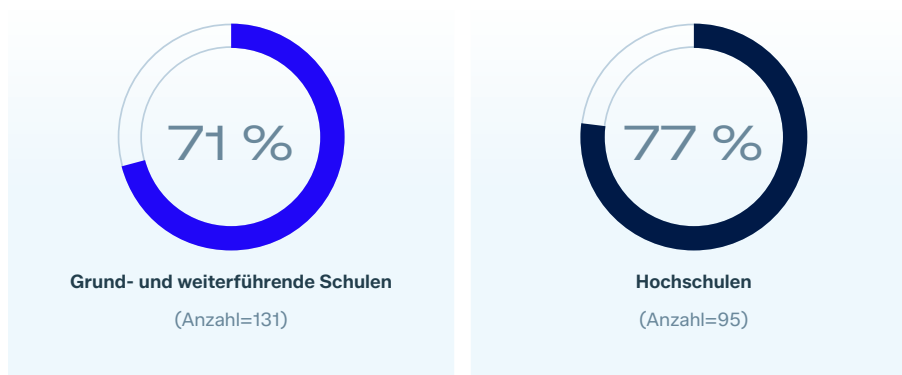
Firewalls sammeln zwar gute Daten, um Angriffe zu identifizieren, aber Angriffe werden nicht in dem Maße gestoppt, wie sie erkannt werden. Firewalls protokollieren häufig die Daten, die zur Erkennung und Abwehr eines Angriffs erforderlich sind, aber sie verbinden sich möglicherweise nicht tief genug mit anderen Systemen, um die Bedrohung zu erkennen und rechtzeitig zu reagieren.

Verbindung zwischen Identität und Ransomware

Einer der eindeutigsten Befunde der Umfrage ist der direkte Zusammenhang zwischen Identitätsangriffen und Ransomware. Branchenübergreifend bestätigten zwei Drittel der von Ransomware betroffenen Unternehmen (67 %), dass der Ransomware-Vorfall auch ihr bedeutendster Identitätsangriff war. Das Bildungswesen liegt jedoch über dieser Marke: 71 % in Grund- und weiterführenden Schulen und 77 % in Hochschulen (73 % im kombinierten Bildungswesen).

Obwohl nicht alle Angriffe zur Datenverschlüsselung führten, zeigt der Befund eine starke Überschneidung zwischen Identitätsangriffen und Ransomware im Bildungswesen.

Ransomware-Angriff war auch der schwerwiegendste identitätsbezogene Angriff



War Ihr Unternehmen/Ihre Organisation von einem Ransomware-Angriff betroffen, der auch ein Identitätsangriff war? Von Ransomware betroffene Unternehmen Basiszahlen in Abbildung.

73 %

Der Anteil der Bildungsoffer, deren Ransomware-Vorfall dasselbe Ereignis war wie ihr schwerwiegendster Identitätsangriff, liegt über der Gesamtumfragequote von 67 %.

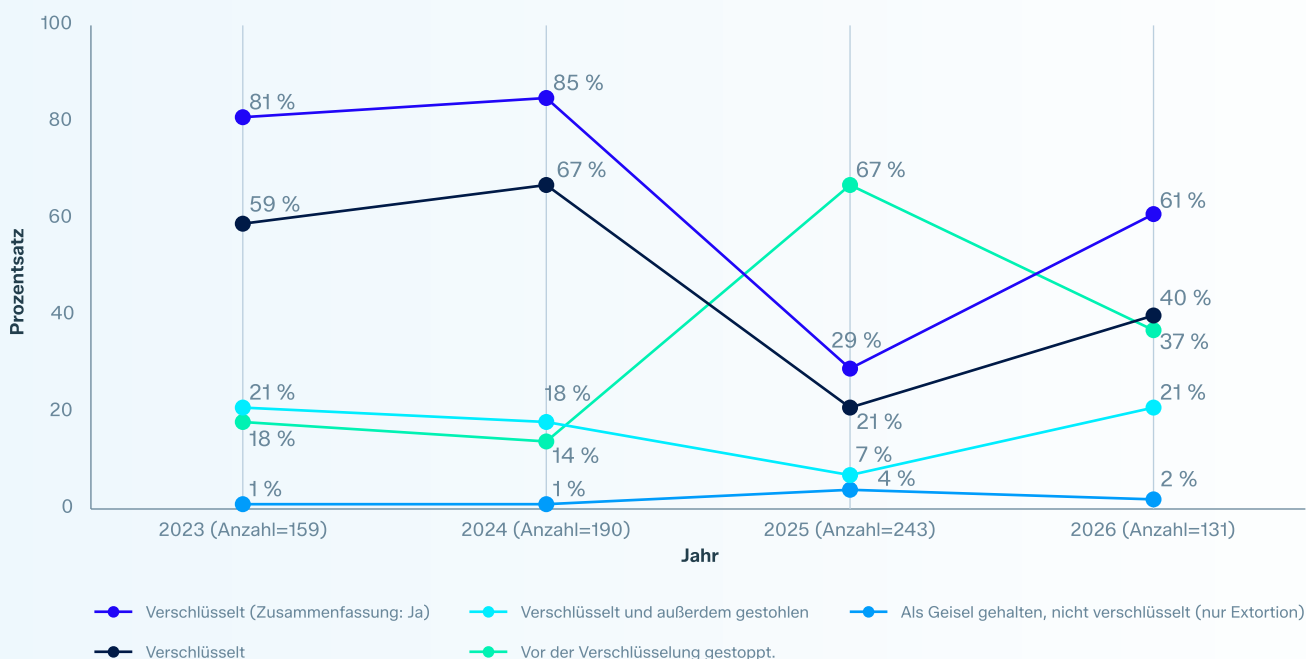
Datenverschlüsselung und -wiederherstellung

Datenverschlüsselungsrate

Die Ergebnisse für Grund- und weiterführende Schulen im Ransomware-Report 2025 waren sehr positiv. Leider zeigt der diesjährige Report, dass sich die Grund- und weiterführenden Schulen wieder näher an ihren früheren Trend annähern.

Nachdem die Verschlüsselungsrate der Grund- und weiterführenden Schulen im Bericht 2025 auf 29 % gefallen war – der niedrigste Wert aller Sektoren in diesem Jahr – mehr als verdoppelte sich **der Anteil der Angriffe auf diese Schulen, bei denen es gelang, Daten zu verschlüsseln, und erreichte im Jahr 2026 mehr als 61 %** (über der Gesamtumfragequote von 56 %). Nur 37 % der Angriffe wurden in diesem Jahr von den Grund- und weiterführenden Schulen gestoppt, bevor Daten verschlüsselt wurden – verglichen mit 67 % im Vorjahr.

Datenverschlüsselungsrate im Zeitverlauf: Grund- und weiterführende Schulen

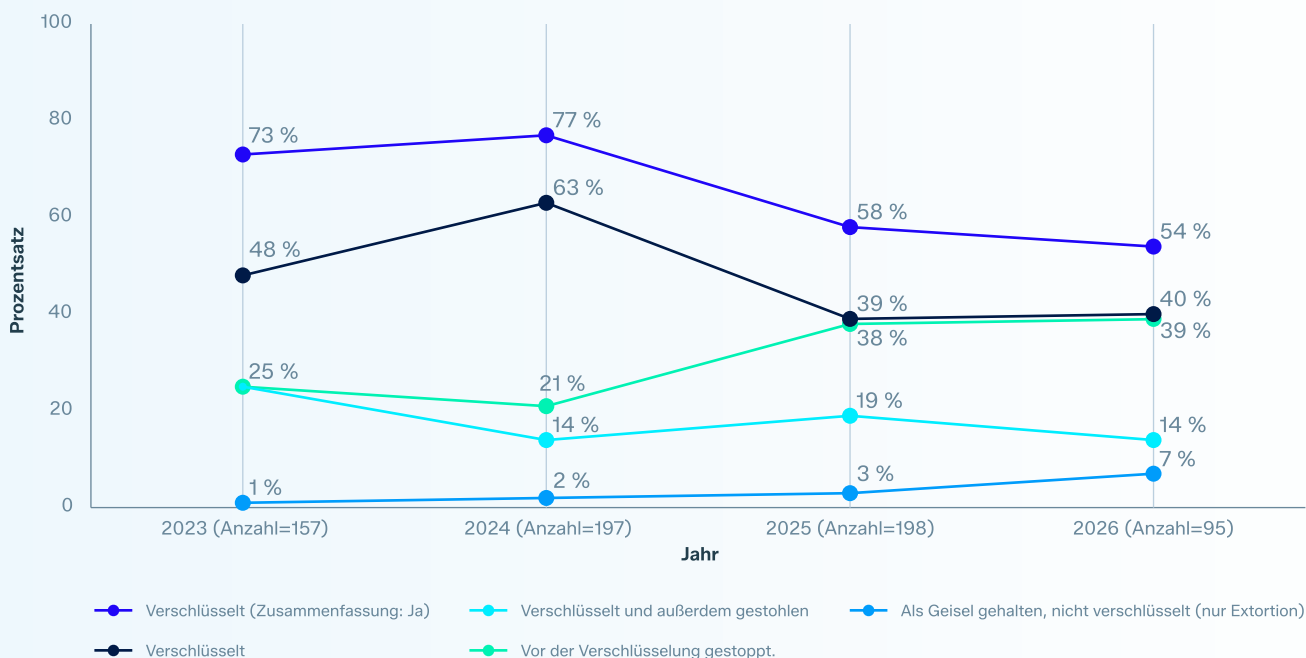


Konnten Cyberkriminelle bei dem Ransomware-Angriff die Daten Ihrer Organisation verschlüsseln? Anzahl der erhaltenen Antworten jeweils in Klammer. Die „Verschlüsselt (Zusammenfassung: Ja)“ Zeile in diesem Diagramm ist die Summe der Antworten „Verschlüsselt“ und „Verschlüsselt und auch gestohlen“.

Double Extortion (bei der Daten sowohl verschlüsselt als auch gestohlen werden) nahm in den Grund- und weiterführenden Schulen wieder zu und stieg von 7 % im Jahr 2025 auf 21 % im Jahr 2026, was dem Niveau vor 2025 entspricht. Diese Angriffe bieten Angreifern einen zweiten Hebel. Extortion-only-Angriffe (**Lösegelderpressung ohne Verschlüsselung**) gingen in Grund- und weiterführenden Schulen leicht von 4 % auf 2 % zurück.

In Hochschulen blieben die Zahlen stabiler. Ihre Verschlüsselungsrate sank leicht auf 54 % im Jahr 2026, gegenüber 58 % im Jahr 2025, was sie nahe an der Gesamtumfrage hält.

Datenverschlüsselungsrate im Zeitverlauf: Hochschulen



Konnten Cyberkriminelle bei dem Ransomware-Angriff die Daten Ihrer Organisation verschlüsseln? Anzahl der erhaltenen Antworten jeweils in Klammer. Die „Verschlüsselt (Zusammenfassung: Ja)“ Zeile in diesem Diagramm ist die Summe der Antworten „Verschlüsselt“ und „Verschlüsselt und auch gestohlen“.

Bei Hochschulen stiegen Extortion-only-Angriffe auf 7 %, gegenüber 3 % im Jahr 2025, was es auch bei einem vergleichsweise geringen Anteil wert ist, beobachtet zu werden.

Das Bild von 2026 zeigt auch, dass das Bildungswesen zu seinem längerfristigen Muster zurückkehrt. 2023 und 2024 lag die Verschlüsselungsrate in Grund- und weiterführenden Schulen über derjenigen von Hochschulen; 2025 war die Ausnahme, als die Verschlüsselungsrate in Grund- und weiterführenden Schulen kurzzeitig einbrach. Die diesjährige Verschlüsselungsrate von 61 % bei Grund- und weiterführenden Schulen im Vergleich zu 54 % bei Hochschulen stellt den langfristigen Trend wieder her.

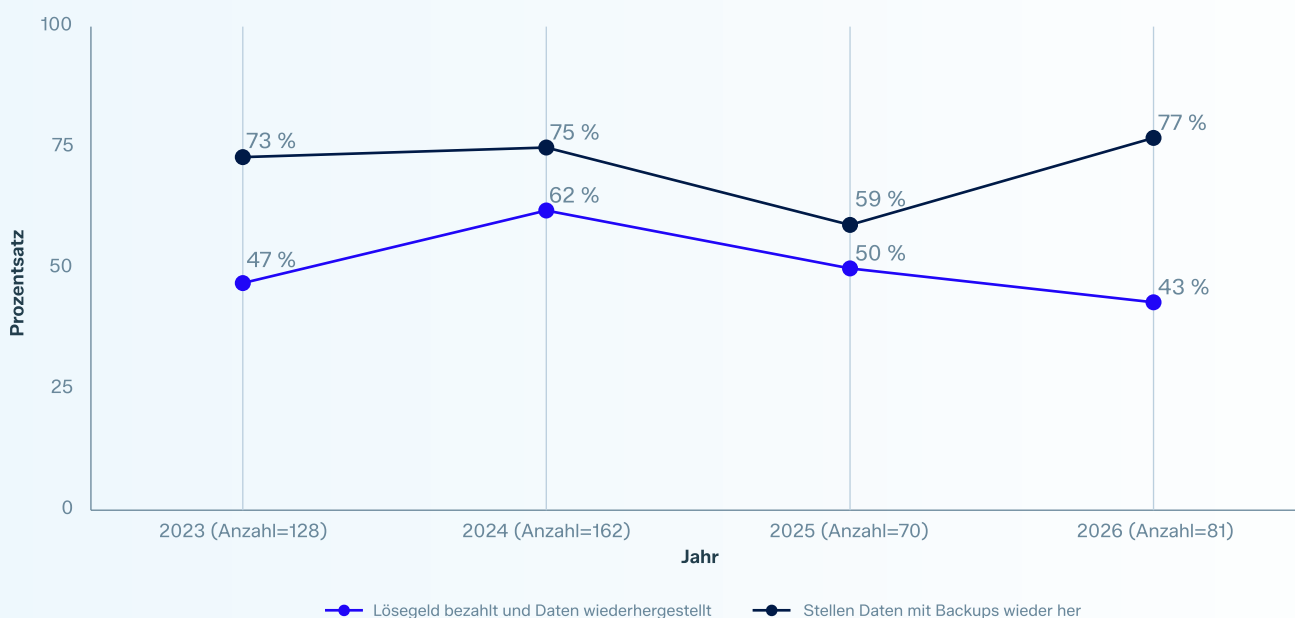
Wie Unternehmen und Organisationen verschlüsselte Daten wiederherstellen

Backups waren 2026 das wichtigste Hilfsmittel zur Wiederherstellung im Bildungswesen. Nach einem Rückgang im Jahr 2025 (Grund- und weiterführende Schulen 59 %, Hochschulen 47 %) nahm die Backup-basierte Wiederherstellung in diesem Jahr wieder zu. **77 % der Grund- und weiterführenden Schulen und 69 % der Hochschulen stellten Daten aus Backups wieder her**, beides über der Gesamtumfragequote von 66 %. Die Erholung deutet darauf hin, dass Bildungseinrichtungen ihre Investitionen in Backup-Infrastrukturen erneuert und die Resilienz gegen Lösegeldforderungen wiederhergestellt haben.

77 %

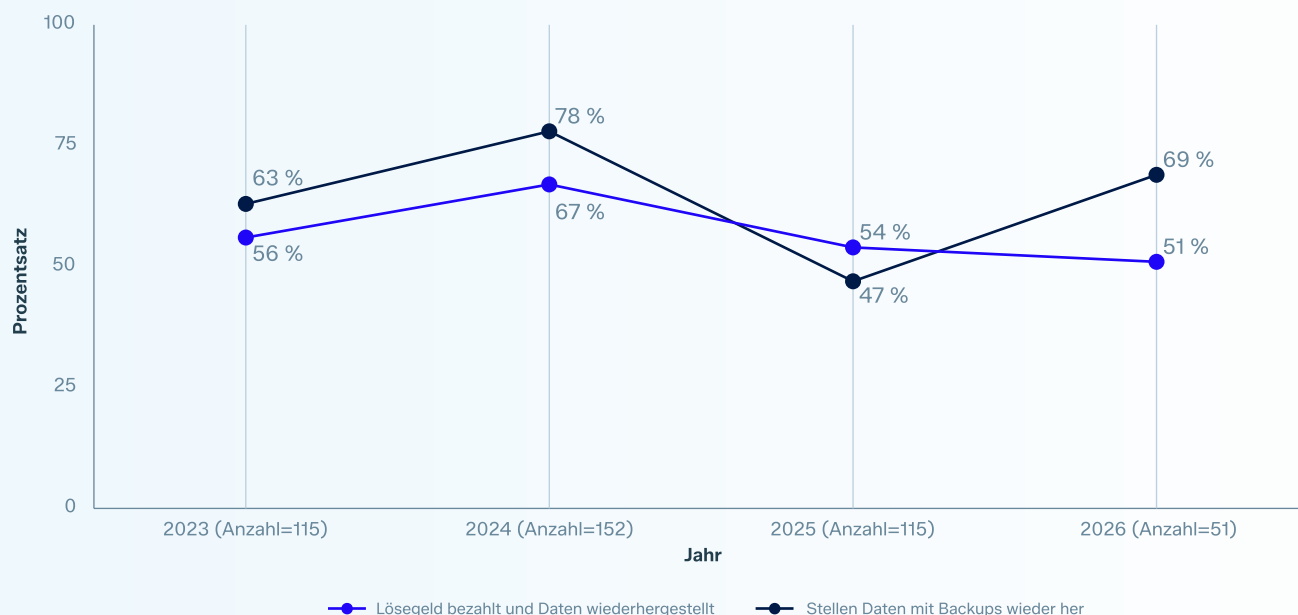
Der Anteil der Grund- und weiterführenden Schulen, die im Jahr 2026 verschlüsselte Daten aus Backups wiederherstellten, liegt über der Gesamtumfragequote von 66 %.

Methoden zur Datenwiederherstellung im Zeitverlauf: Grund- und weiterführende Schulen



Wie hat Ihr Unternehmen/Ihre Organisation die Daten zurückerhalten? Mehrere Antworten zulässig. Anzahl der erhaltenen Antworten jeweils in Klammer.

Methoden zur Datenwiederherstellung im Zeitverlauf: Hochschulen



Wie hat Ihr Unternehmen/Ihre Organisation die Daten zurückerhalten? Mehrere Antworten zulässig. Anzahl der erhaltenen Antworten jeweils in Klammer.

Gleichzeitig zahlen Bildungseinrichtungen seltener Lösegeld. **Der Anteil der Anbieter, die das Lösegeld zahlten und Daten zurückerhielten, ist zwei Jahre in Folge gesunken**, von 62 % (2024) auf 50 % (2025) auf 43 % (2026) in den Grund- und weiterführenden Schulen bzw. von 67 % auf 54 % auf 51 % in den Hochschulen.

Da die Backup-Wiederherstellung steigt und die zahlungsbasierte Wiederherstellung sinkt, erholt sich das Bildungswesen mehr aus eigener Kraft als durch die Kooperation der Angreifer.

Lösegeldforderungen und -zahlungen

Lösegeldforderungen

Im Bildungswesen wurden im Vergleich zu anderen Branchen in der Gesamtumfrage höhere Lösegeldforderungen gestellt. Die Median-Lösegeldforderung an eine Bildungseinrichtung lag bei 775.200 US-Dollar und damit über dem Medianwert von 698.000 US-Dollar für alle Branchen. Auch die Verteilung stieg: **Die Hälfte der Lösegeldforderungen (50 %) entfielen auf 1 Mio. US\$ oder mehr und ein Viertel (25 %) auf 5 Mio. US\$ oder mehr**, verglichen mit 46 % bzw. 23 % in der gesamten Branchenstichprobe.

Hinweis: Ausreißerwerte bei den Lösegeldforderungen ab 40 Mio. US\$ wurden aus diesen Daten entfernt.

Lösegeldforderung (Medianwert)

	2025	2026
Bildungswesen	0,98 Mio. \$ (Anzahl=185)	0,78 Mio. \$ (Anzahl=132)
Alle Branchen	1,32 Mio. \$ (Anzahl=1.700)	0,70 Mio. \$ (Anzahl=1.214)

Wie viel Lösegeld forderten die Angreifer? Basis: Unternehmen und Organisationen, deren Daten verschlüsselt wurden. Anzahl der erhaltenen Antworten jeweils in Klammer.

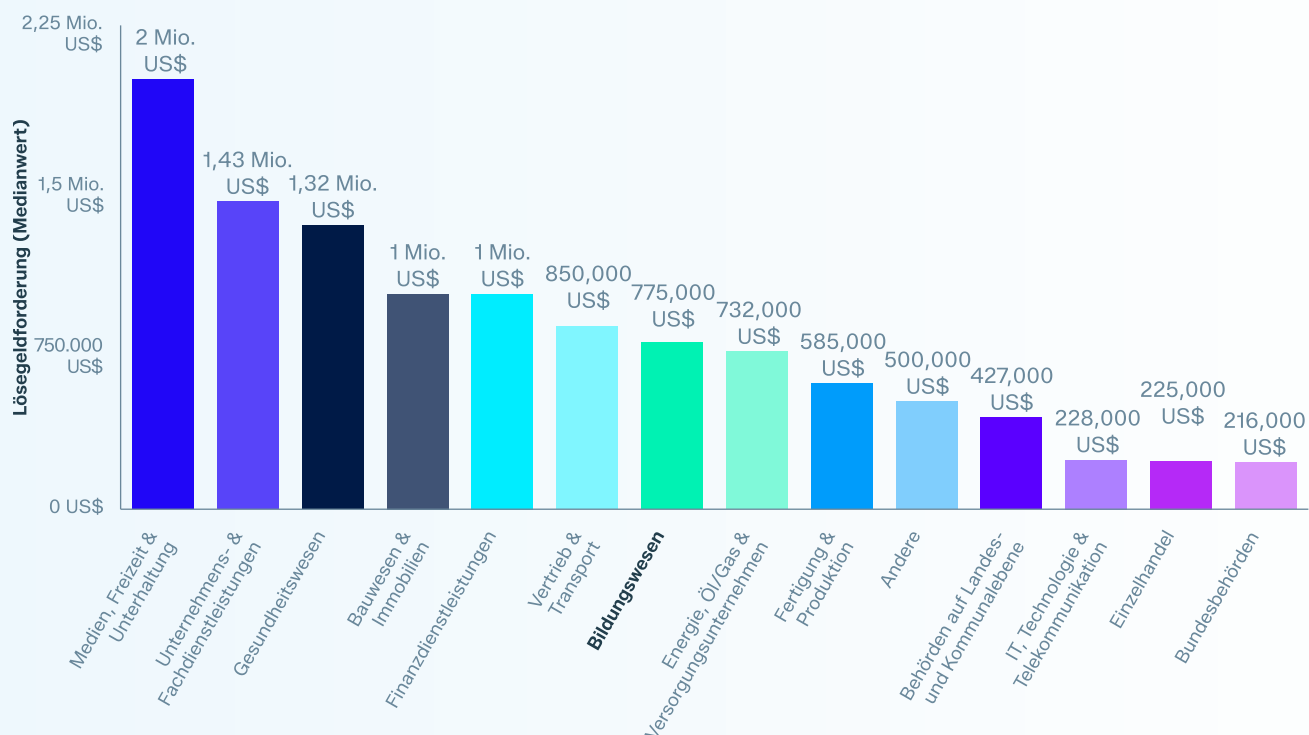
Im Vergleich zu anderen Branchen liegt das Bildungswesen im Mittelfeld. Die durchschnittlichen Lösegeldforderungen liegen unter den Sektoren mit der höchsten Nachfrage, wie etwa Medien, Freizeit und Unterhaltung (2 Mio. US\$) sowie Unternehmens- und Professional Services (1,43 Mio. US\$), liegen aber deutlich über Sektoren mit geringerer Nachfrage wie der Zentralregierung (216.500 US\$) und dem Einzelhandel (225.000 US\$).

755.000 US\$

Die durchschnittlich von Bildungseinrichtungen geforderte Lösegeldsumme (Medianwert) – liegt über dem Durchschnitt der Umfrage von 698.000 US\$.

Die Hälfte aller Lösegeldforderungen im Bildungswesen betrugen 1 Mio. US\$ oder mehr.

Lösegeldforderungen nach Branche (Medianwert)



Wie viel Lösegeld forderten die Angreifer? Basis: Unternehmen und Organisationen, deren Daten verschlüsselt wurden. Anzahl=1.141

Die Trends im Jahresvergleich sind gut und schlecht. Die durchschnittliche Nachfrage im kombinierten Bildungswesen sank von 976.000 US\$ im Jahr 2025 auf 775.200 US\$ im Jahr 2026. Dieser Rückgang war vor allem auf die Grund- und weiterführenden Schulen zurückzuführen, wo die durchschnittliche Nachfrage von 1,03 Mio. US\$ auf 737.600 US\$ sank, während die Hochschulen diesem Trend zuwiderliefen: Ihre durchschnittliche Nachfrage stieg von 697.086 US\$ auf 889.200 US\$.

Lösegeldzahlungen

Die höheren Bildungsanforderungen führten nicht zu höheren Zahlungen.

Obwohl sie höhere Lösegeldforderungen sahen, fiel die durchschnittliche Lösegeldzahlung im Bildungswesen im Vergleich zu anderen Branchen in der Gesamtumfrage geringer aus. Die durchschnittliche Lösegeldzahlung einer Bildungseinrichtung betrug 515.000 US\$ und lag damit unter dem Durchschnitt der Umfrage von 769.000 US\$.

Die Zahlungen im Bildungswesen konzentrierten sich auf Bereiche unterhalb der höchsten Kategorie, umfassten jedoch einen größeren Anteil an Zahlungen von über 5 Mio. US\$. 39 % der Bildungszahlungen beliefen sich auf 1 Mio. US\$ oder mehr und lagen damit unter dem Gesamtumfragewert von 44 %. 23 % lagen jedoch bei 5 Mio. US\$ oder mehr und damit über dem Gesamtumfragewert von 16 %. Wenn Bildungseinrichtungen zahlen, zahlen sie in der Regel weniger als andere Branchen, aber eine nennenswerte Minderheit zahlt sehr hohe Summen.

515.000 US\$

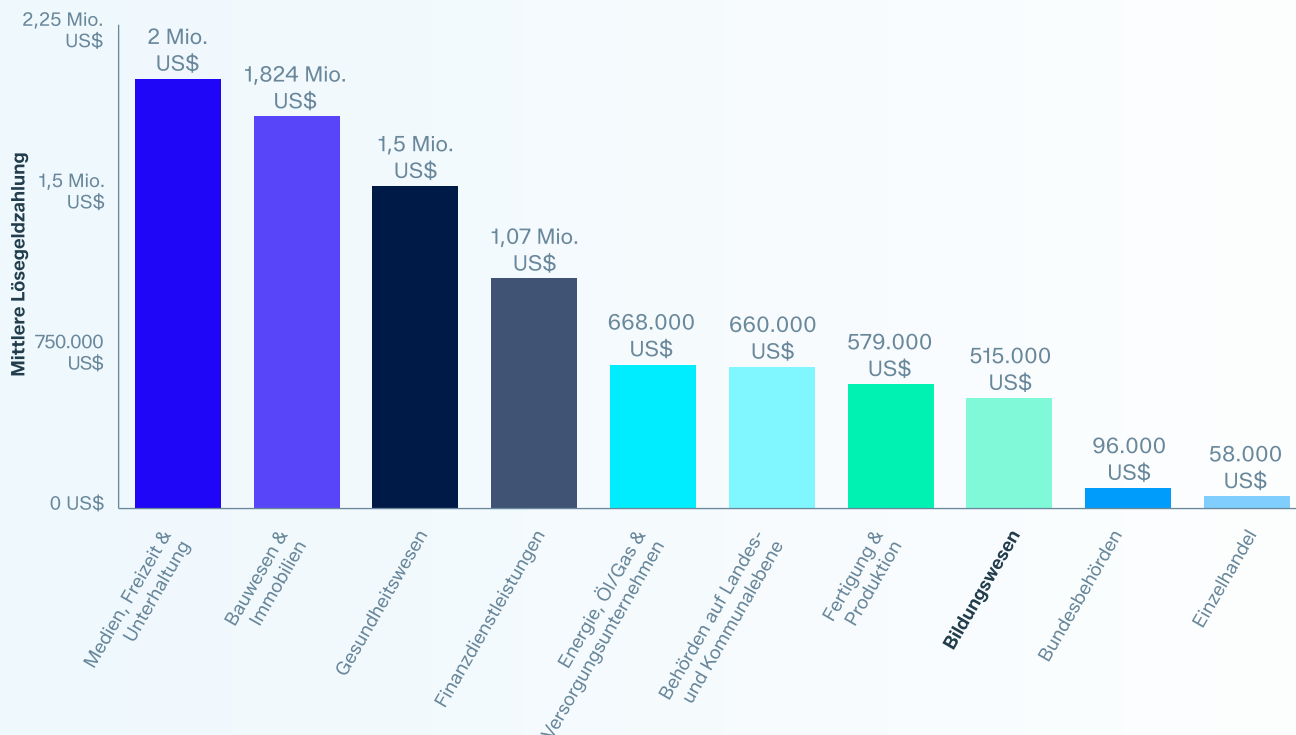
Das von Bildungseinrichtungen durchschnittlich gezahlte Lösegeld (Medianwert) liegt – trotz höherer Lösegeldforderungen – unter dem Durchschnitt der Umfrage von 769.000 US\$.

Mittlere Lösegeldzahlung

	2025	2026
Bildungswesen	0,50 Mio. \$ (Anzahl=100)	0,52 Mio. \$ (Anzahl=62)
Alle Branchen	1,00 Mio. \$ (Anzahl=847)	0,77 Mio. \$ (Anzahl=587)

Wie viel Lösegeld wurde Angreifern ungefähr gezahlt? Basis: Unternehmen und Organisationen, die das Lösegeld zahlten. Anzahl der erhaltenen Antworten jeweils in Klammer.

Durchschnittliche Lösegeldzahlungen nach Branche (Medianwert)



Wie viel Lösegeld wurde Angreifern ungefähr gezahlt? Basis: Unternehmen und Organisationen, die das Lösegeld zahlten. Anzahl=587. Branchen mit weniger als 30 Befragten zu dieser Frage wurden nicht berücksichtigt.

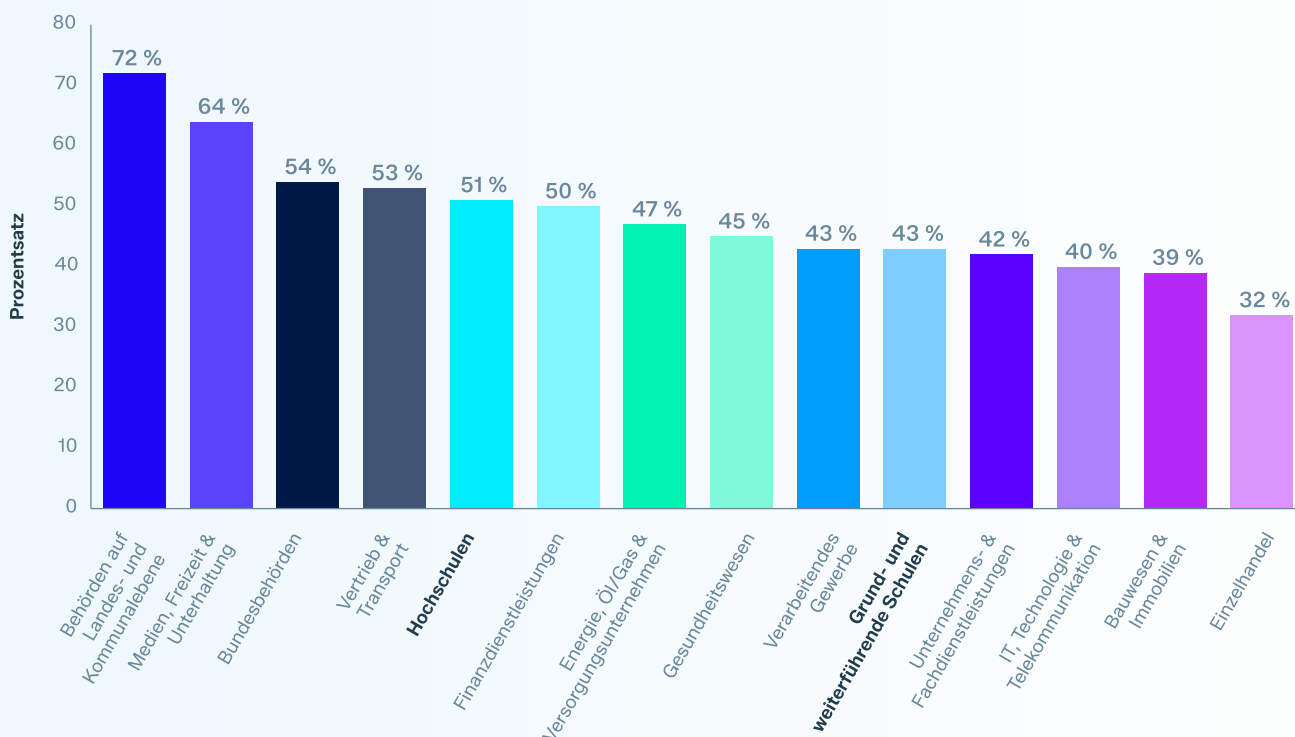
Auch bei den Lösegeldzahlungen waren die Trends im Vergleich zum Vorjahr gemischt. Die durchschnittliche Zahlung im kombinierten Bildungswesen war im Wesentlichen flach und stieg leicht von 500.000 US\$ im Jahr 2025 auf 515.000 US\$ im Jahr 2026. Die durchschnittliche Zahlung der Grund- und weiterführenden Schulen sank im selben Zeitraum drastisch von 800.000 US\$ auf 320.000 US\$. Der leichte Anstieg auf der kombinierten Ebene war daher auf die Hochschulen zurückzuführen.

Da in diesem Jahr weniger als 30 Hochschulen einen Zahlungsbetrag meldeten (n=27), können wir keine verlässliche eigenständige Trendlinie für Hochschulzahlungen darstellen. Daher empfehlen wir, die kombinierten Bildungszahlungen zu berücksichtigen.

Prozentsatz der Unternehmen und Organisationen, die das Lösegeld zahlten, nach Branche

Die Zahlungsbereitschaft unterschied sich zwischen den beiden Bildungssegmenten. 51 % der Hochschulopfer zahlten das Lösegeld – über der Gesamtumfragequote von 48 % – während 43 % der Opfer im Bereich der Grund- und weiterführenden Schulen das Lösegeld zahlten, was darauf hindeutet, dass sie sich häufiger gegen die Zahlung sträubten als im Gesamtdurchschnitt.

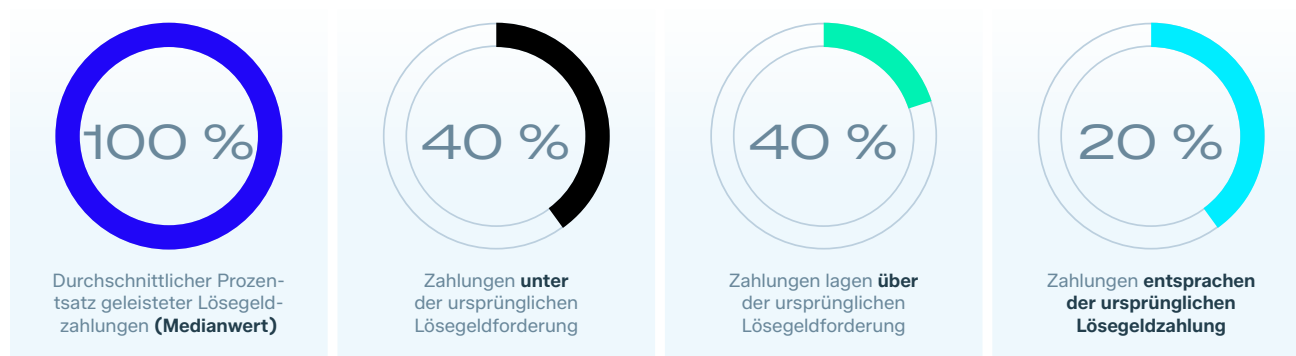
Prozentsatz der Unternehmen und Organisationen, die das Lösegeld zahlten, nach Branche



Wie hat Ihr Unternehmen/Ihre Organisation die Daten zurückerhalten? Basis: Unternehmen, deren Daten verschlüsselt wurden. Anzahl=1.214

Tatsächliche Zahlungen vs. ursprüngliche Forderungen

Von den Bildungseinrichtungen, die das Lösegeld zahlten, zahlten 40 % weniger als die ursprüngliche Forderung, 40 % mehr und 20 % zahlten genau das, was gefordert wurde. Die mittlere Bildungseinrichtung zahlte 100 % der ursprünglichen Forderung, gegenüber 82 % im Jahr 2025. Während also ein beträchtlicher Teil der Institute den Zahlungsbetrag erfolgreich verhandelte, endete ein ebenso hoher Anteil damit, mehr als die ursprünglich geforderte Summe zu zahlen.



War die tatsächlich gezahlte Lösegeldsumme niedriger als, genauso hoch wie oder höher als die ursprüngliche Lösegeldforderung? Ohne Extremwerte. Kombination aus Hochschulen sowie Grund- und weiterführenden Schulen. Anzahl=58.

Wirtschaftliche Folgen und Auswirkungen auf Mitarbeitende

Ransomware-Bereinigungskosten

Die Bereinigungskosten im Bildungswesen waren überdurchschnittlich hoch.

Die durchschnittlichen Kosten für die Bereinigung eines Ransomware-Angriffs lagen ohne Lösegeldzahlung bei 2,46 Mio. US\$ im Grund- und Hochschulwesen. Beides liegt über dem Gesamtdurchschnitt von 1,7 Mio. US\$.

Grund- und weiterführende Schulen trugen zwei Jahre in Folge die größte Last. Die durchschnittlichen Bereinigungskosten stiegen von 2,28 Mio. US\$ im Jahr 2025 auf 2,46 Mio. US\$ im Jahr 2026, was sie zum teuersten Bildungssektor macht und deutlich über der Gesamtumfrage (1,7 Mio. US\$) liegt.

Durchschnittliche Bereinigungskosten

	2025	2026
Grund- und weiterführende Schulen	2,28 Mio. \$ (Anzahl=243)	2,46 Mio. \$ (Anzahl=131)
Hochschulen	0,90 Mio. \$ (Anzahl=198)	1,99 Mio. \$ (Anzahl=95)
Alle Branchen	1,53 Mio. \$ (Anzahl=3.400)	1,70 Mio. \$ (Anzahl=2.158)

Wie hoch waren die ungefähren Kosten, die Ihrem Unternehmen/Ihrer Organisation durch den schwersten Ransomware-Angriff entstanden sind? Durchschnittliche Bereinigungskosten, ohne gezahltes Lösegeld. Anzahl der erhaltenen Antworten jeweils in Klammer.

Im Hochschulbereich sind die Kosten am stärksten in die Höhe geschnellt. Die durchschnittlichen Bereinigungskosten haben sich von 0,9 Mio. US\$ im Jahr 2025 auf 1,99 Mio. US\$ im Jahr 2026 mehr als verdoppelt. Im Bericht 2025 wurde im Hochschulbereich einer der niedrigsten Wiederherstellungskosten aller Sektoren verzeichnet. In diesem Jahr nähert sich der Wert dem Niveau der Grund- und weiterführenden Schulen an. Beide Bildungssegmente liegen nun über dem Gesamtdurchschnitt der Umfrage, der seinerseits leicht von 1,53 Mio. US\$ auf 1,7 Mio. US\$ angestiegen ist.

1,09 Mio. US\$

Der Anstieg der durchschnittlichen Bereinigungskosten von Ransomware für Hochschulen von 2025 bis 2026.

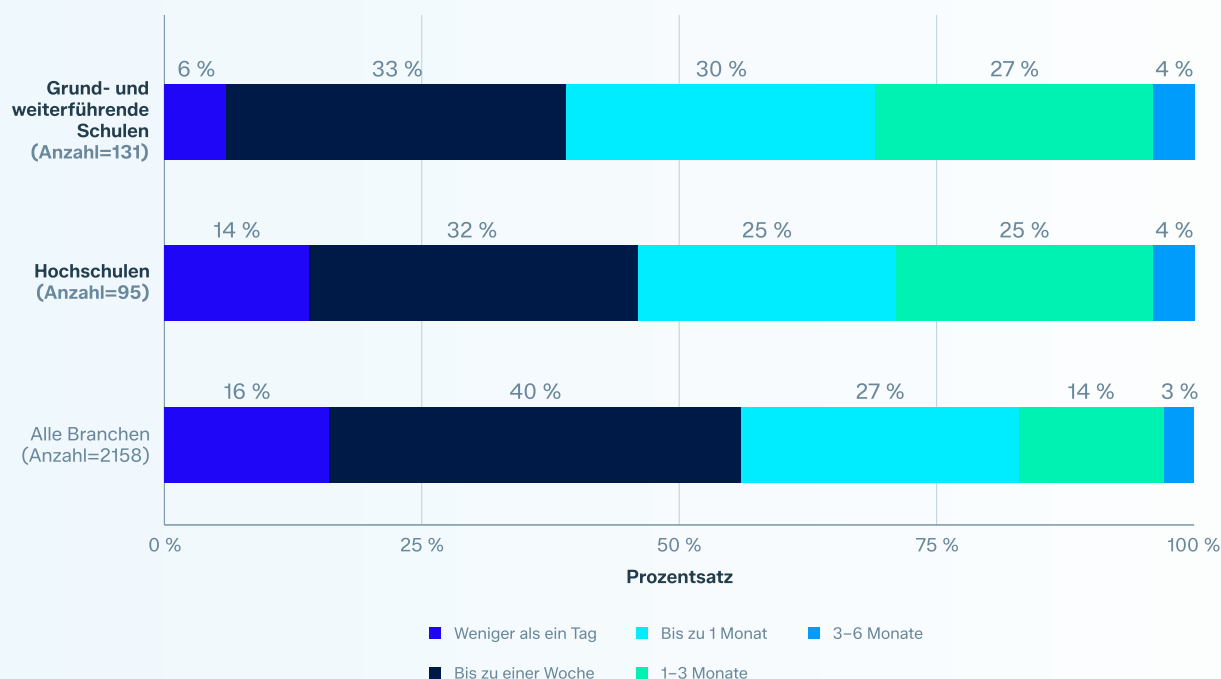
Ausfallzeiten

Bildungseinrichtungen zahlten nicht nur mehr für die Wiederherstellung, sie benötigten auch länger dafür. Die deutlichste Kluft besteht im ein- bis dreimonatigen Recovery-Band: 27 % der Grund- und weiterführenden Schulen und 25 % der Hochschulen benötigten so lange, um sich vollständig zu erholen, verglichen mit nur 14 % aller Befragten. **Im Bildungsbereich war die Wahrscheinlichkeit, dass sich die Erholung einen Monat oder länger hinzog, fast doppelt so hoch.**

31 %

Der Anteil der Grund- und weiterführenden Schulen, die mindestens einen Monat brauchten, um sich zu erholen, mehr als jeder andere Sektor.

Wie lange es gedauert hat, sich von Ransomware zu erholen



Wie lange hat es gedauert, bis sich Ihr Unternehmen vollständig von dem Ransomware-Angriff erholt hat? Anzahl der erhaltenen Antworten jeweils in Klammer.

Am schnellen Ende der Skala zeigt sich dasselbe Bild in umgekehrter Reihenfolge. Nur 6 % der Grund- und weiterführenden Schulen erholten sich in weniger als einem Tag, im Vergleich zu 16 % aller Befragten und 14 % der Hochschulen.

Kein Sektor hatte einen größeren Anteil an langen Erholungsphasen als die Grund- und weiterführenden Schulen, wo 31 % der Einrichtungen mindestens einen Monat benötigten, um sich vollständig zu erholen.

Auswirkungen auf Mitarbeitende

Die Auswirkungen auf Menschen im Bildungswesen waren ausgeprägter als im Gesamtdurchschnitt, und jeder Bildungssektor nahm diese Belastung auf unterschiedliche Weise wahr. Im Hochschulwesen kam der entscheidende Druck von oben: 53 % der Teams berichteten von erhöhtem Druck durch Führungskräfte, 13 Punkte über der Gesamtumfragequote von 40 %. In Hochschulen waren auch Veränderungen im Team oder in der Organisationsstruktur häufiger (43 % ggü. 32 % in allen Branchen).

In Grund- und weiterführenden Schulen konzentrieren sich die Erfahrungen auf Anerkennung und Arbeitsbelastung. Fast die Hälfte der Teams der Grund- und weiterführenden Schulen (49 %) meldete eine höhere Anerkennung von Führungskräften und lag damit über der Quote von 36 % aller Befragten. Anerkennung kann positiv sein, erhöhte Arbeitsbelastung jedoch nicht. 43 % der Einrichtungen im Bereich der Grund- und weiterführenden Schulen berichteten von einem kontinuierlichen Anstieg der Arbeitsbelastung, verglichen mit 31 % in allen Branchen. Die Aufmerksamkeit war also zweischneidig: mehr Sichtbarkeit, aber auch eine schwerere und dauerhaftere Belastung.

53 %

Der Prozentsatz der Hochschul-IT- und Sicherheitsteams, die nach einem Angriff einem erhöhten Druck von Führungskräften ausgesetzt waren, im Vergleich zu 40 % aller Befragten.

Auswirkungen auf Mitarbeitende

Auswirkungen	Grund- und weiterführende Schulen (Anzahl=81)	Hochschulen (Anzahl=51)	Alle Branchen (Anzahl=1.214)
Mehr Stress oder Angst vor künftigen Angriffen	40 %	33 %	41 %
Mehr Druck aus der Führungsetage	48 %	53 %	40 %
Mehr Anerkennung aus der Führungsetage	49 %	29 %	36 %
Veränderungen an der Struktur des Teams/ Unternehmens	33 %	43 %	32 %
Veränderungen der Prioritäten/ Fokusbereiche im Team	33 %	35 %	32 %
Schuldgefühle, weil sie den Angriff nicht gestoppt haben	31 %	25 %	31 %
Höhere Arbeitslast	43 %	31 %	31 %
Fehlzeiten bei Mitarbeitenden wegen Stress/ psychischen Problemen	40 %	39 %	29 %
Austausch der Teamführung	27 %	29 %	21 %

Welche Auswirkungen hatte der Ransomware-Angriff auf die Mitarbeitenden in Ihrem IT-/Cybersecurity-Team? Basis: Unternehmen/Organisationen, deren Daten verschlüsselt wurden. Anzahl der erhaltenen Antworten jeweils in Klammer.

Das Wohlergehen der Mitarbeitenden litt in beiden Bildungssegmenten. 39 % der Hochschulen und 40 % der Teams der Grund- und weiterführenden Schulen berichteten von Fehlzeiten aufgrund von Stress oder psychischen Gesundheitsproblemen, was deutlich über der Gesamtumfragequote von 29 % liegt.

Auch die Fluktuation der Führungskräfte stieg: 29 % der Hochschulen und 27 % der Teams der Grund- und weiterführenden Schulen sahen ihre Führung nach dem Angriff ersetzt, verglichen mit 21 % insgesamt.

Empfehlungen

Stärken Sie die Identitätssicherheit zum Schutz vor Ransomware. 73 % der Ransomware-Opfer bestätigten, dass ihr Ransomware-Vorfall gleichzeitig ihr schwerwiegendster Identitätsangriff war, was den engen Zusammenhang zwischen Identitätskompromittierung und Ransomware unterstreicht. Bildungseinrichtungen sollten Identity Threat Detection and Response (ITDR) priorisieren, Multi-Faktor-Authentifizierung über alle Zugangspunkte hinweg durchsetzen und regelmäßig sowohl menschliche als auch nicht-menschliche Zugangsdaten prüfen.

Aktivieren Sie MFA umfassend, speziell Phishing-resistente MFA. Die Umfrage ergab, dass 98 % der Bildungseinrichtungen mit kompromittierten Anmeldedaten zum Zeitpunkt ihres Angriffs MFA in irgendeiner Form aktiviert hatten, wobei die Verschlüsselungsraten dennoch hoch blieben. MFA allein reicht nicht aus, um Angriffe zu verhindern, und muss durchgängig aktiviert sein – anstatt nur bei den SaaS-Anwendungen, die MFA erzwingen, während VPN-Anmeldungen, Firewall-Admin-Konsolen und Legacy-Anwendungen ungeschützt bleiben.

Verstärken Sie den Endpoint-Schutz für Frontier-KI-Modelle. Auch wenn die Zahl der ausgenutzten Schwachstellen in diesem Bericht zurückgegangen ist, rechnen [Sophos-Experten mit einem erneuten Anstieg von Exploits](#), da Unternehmen und Organisationen Schwierigkeiten haben, mit Patches für von Frontier AI gefundenen Schwachstellen Schritt zu halten. Eine starke Endpoint-Abwehr, die Exploit-basierte Angriffe automatisch stoppt, ist unerlässlich.

Ziehen Sie fachliche Unterstützung oder MDR hinzu. Der Mangel an Kapazitäten, Fähigkeiten und Fachwissen ist ein anhaltendes Thema im Bildungswesen, insbesondere an Hochschulen, wo mangelndes internes Fachwissen als eine entscheidende Schwäche hervorgehoben wurde. Der Umgang mit KI-gestützten Bedrohungen wird diese Bereiche noch stärker belasten, da Sicherheitsteams versuchen, mit der sich schnell verändernden KI-Technologie Schritt zu halten. Sofern Sie nicht in der Lage sind, ein eigenes Security Operations Team aufzubauen, sollten Sie die Lücke mit einem externen Spezialisten schließen – entweder direkt mit einem MDR-Anbieter mit 24/7-Abdeckung oder mit einem Managed Service Provider. Anbieter, die mehr Vorfälle durchgängig mit KI und Automatisierung beheben, fungieren als Kraftmultiplikator, der hilft, Kompetenz- und Kapazitätslücken zu schließen.

Investieren Sie in Backup- und Wiederherstellungsinfrastrukturen. Backups waren der dominante Wiederherstellungsweg für Grund- und weiterführende Schulen sowie Hochschulen (77 % bzw. 69 %, beide über dem Gesamtdurchschnitt). Backups sollten regelmäßig getestet, offline oder in unveränderlichen Formaten gespeichert und in einen dokumentierten Incident-Response-Plan integriert werden, der unter Druck ausgeführt werden kann.

Unterhalten Sie Exposure Management-Programme. Ausgenutzte Schwachstellen bleiben ein wichtiger Angriffsvektor und werden wahrscheinlich zunehmen, da innovative KI-Modelle in der Lage sind, neue Schwachstellen schneller zu identifizieren. Bildungseinrichtungen sollten einen straffen Zeitplan für das Patchen internetausgerichteter Geräte einhalten und sich auf Schutzmaßnahmen wie Netzwerksegmentierung, Zero Trust Network Access sowie die Implementierung von MFA und kontinuierlicher Authentifizierung konzentrieren.

Reduzieren Sie die Exposition auf Firewall-Ebene und nutzen Sie Firewall-Telemetrie, um Angriffe frühzeitig zu erkennen. Die Daten aus dem Jahr 2026 zeigen, dass Firewalls Anzeichen von Ransomware gut erkennen können: 65 % verfügen über genügend Daten, um einen Angriff zu erkennen, bevor die Ransomware ausgelöst wurde. Aber selbst bei diesen Fällen der frühen Erkennung wurden die Daten von Opfern im Bildungswesen 51 % der Fälle verschlüsselt, da die Firewall einen Angriff oft nicht bestätigen oder stoppen kann, ohne Telemetriedaten von anderen Kontrollpunkten zu erhalten. Stellen Sie sicher, dass Ihre Firewall schnelle – idealerweise automatisierte – Updates erhält, und minimieren Sie internetbasierte Dienste wie Admin-Zugriffe und Benutzerportale. Verbinden Sie Firewalls mit XDR und MDR, damit Ransomware-Angriffe mithilfe von Firewall-Telemetriedaten erkannt werden können, bevor Payloads ausgeführt werden. Ein Cybersecurity-Abwehrsystem, bei dem Kontrollen Signale austauschen, ist die Lösung.

Handlungsempfehlungen auf einen Blick:

1. Segmentierung zur Verlangsamung von Angreifern
2. ZTNA, um veraltete VPNs zu ersetzen und App Exploits einzudämmen
3. Identity Threat Detection and Response (ITDR) zur Härtung der Identitätsinfrastruktur
4. Phishing-resistente MFA als Ziel und nicht als Ausgangspunkt
5. Diszipliniertes Patching von mit dem Internet verbundenen Geräten
6. 24/7 Erkennung und Reaktion

Fazit

Der „Ransomware-Report 2026: Bildungswesen“ offenbart eine Bedrohungslandschaft im Wandel.

Es gibt Anzeichen von Fortschritten: Die Lösegeldforderungen gehen zurück, die Backup-basierte Wiederherstellung hat fast Rekordniveau erreicht und die Lösegeldzahlungen von Bildungseinrichtungen sind im Vergleich zu anderen Branchen niedrig.

Gleichzeitig sind die verbleibenden Herausforderungen erheblich. Mehr als die Hälfte der Ransomware-Angriffe auf Bildungseinrichtungen führen weiterhin zur Verschlüsselung von Daten, die durchschnittlichen Bereinigungskosten belaufen sich auf 2,26 Mio. \$ pro Vorfall (höher als im Gesamtdurchschnitt), und Grund- und weiterführende Schulen hatten den größten Anteil an Wiederherstellungen, die einen Monat oder länger dauerten.

Im Bildungswesen konzentriert sich das Risiko vor allem auf die Identität. Ein höherer Anteil der Bildungseinrichtungen bestätigte, dass ihr Ransomware-Vorfall dasselbe Ereignis war wie ihr schwerwiegendster Identitätsangriff im Vergleich zur Gesamtumfrage. In einem Sektor, in dem die Wiederherstellung ohnehin langsamer und kostspieliger ist, macht diese enge Kopplung die Identitätsinfrastruktur zum Investitionsbereich mit der größten Hebelwirkung.

Bildungseinrichtungen müssen sich zudem auf die entscheidendste Cybersecurity-Herausforderung des nächsten Jahrzehnts vorbereiten: KI-gestützte Bedrohungen. Die Daten deuten bereits darauf hin, warum: 62 % der Bildungseinrichtungen nannten eine bekannte oder unbekannte Sicherheitslücke als einen Faktor für ihren Angriff, und 63 % wiesen auf einen Mangel an Fachkräften oder Expertise hin. Beide Faktoren gewinnen zunehmend an Bedeutung, da KI die Geschwindigkeit und das Ausmaß von Angriffen erhöht und Angreifer KI nutzen, um Schwachstellen schneller aufzuspüren und Angriffe auf mehrere Kontrollpunkte in maschineller Geschwindigkeit zu koordinieren.

Auch in den Ursachendaten dieses Jahres verbirgt sich ein tiefergehendes Signal. Das wahrgenommene Ursachegefüge gleicht sich an; in allen Branchen, einschließlich Bildungswesen, dominiert kein einziger Vektor. Das macht eine zu enge Fokussierung der Abwehr auf eine Ursache riskant, da Angreifer über mehrere Vektoren erfolgreich sind.

Das Muster der diesjährigen Ergebnisse, insbesondere der geringen Auswirkungen der Firewall-Erkennung und der MFA-Aktivierung auf die Ergebnisse, zeigt in eine einheitliche Richtung: Wenn Abwehrmaßnahmen in Isolation arbeiten, sind Sie nicht geschützt. Um die Lücke zu schließen, die durch Angriffe im KI-Zeitalter entstanden ist, kommt es weniger darauf an, weitere Tools hinzuzufügen, sondern vielmehr darauf, die bereits vorhandenen miteinander zu vernetzen, damit Kontextanalyse, Erkennung und Reaktion mit der Geschwindigkeit erfolgen können, die heutige Bedrohungen erfordern.

Bildungsanbieter, die das Thema Ransomware kontinuierlich im Fokus der Führungsetage halten und gleichzeitig integrierte, KI-gestützte Abwehrsysteme einführen, werden in den kommenden Jahren am besten gegen Ransomware gewappnet sein – wobei sie nicht nur in Technologie und Prozesse, sondern auch in die Mitarbeitenden investieren, die diese Bedrohungen tagtäglich abwehren.



Mehr über Ransomware
und effektiven Schutz
durch Sophos erfahren
Sie auf [unserer Website](#).

Sales DACH (Deutschland, Österreich, Schweiz)

Tel.: +49 611 58580

E-Mail: sales@sophos.de

© Copyright 2026. Sophos Ltd. Alle Rechte vorbehalten.

Eingetragen in England und Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, GB

Sophos ist die eingetragene Marke von Sophos Ltd. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken der jeweiligen Inhaber.

2026-09-12 DE (DD)