

Nahtloser Zugriff: Ein umfassender Leitfaden über SSO an Schulen

Einführung ★★☆☆

Jede Minute Unterrichtszeit zählt.

Dennoch beeinträchtigen Probleme beim Einloggen nach wie vor den Lernprozess im Schulwesen. Von verspätetem Unterrichtsbeginn über ungleichen Zugang für Schüler bis hin zu mehr IT-Aufwand: Authentifizierungsprobleme verursachen Kettenreaktionen, die sich auf die Lernergebnisse auswirken.

In diesem Leitfaden wird erläutert, wie Single Sign-On (SSO) einen nahtlosen Zugang zu Lernangeboten ermöglicht, die Komplexität verringert und wertvolle Lernzeit zurückgewinnt. Für IT-Administratoren bietet es einen klaren Weg, die Identitätsverwaltung zu vereinfachen, die Sicherheit zu erhöhen und Lehrkräfte sowie deren institutionelle Ziele besser zu unterstützen.

Wenn das Lernen warten muss

9:00 Uhr: Die Klassenlehrerin ist gerade die Anwesenheitsliste durchgegangen und blickt von ihrem Tablet auf in ein Meer strahlender Gesichter. Die Schüler sind gespannt darauf, etwas über das Sonnensystem zu lernen, nachdem sie am Abend zuvor den Start von Artemis II verfolgt haben. „Guten Morgen, liebe Astronauten, hier spricht euer Kommandant. Zeit, eure Weltraumausrüstung zu holen, denn heute ...*fliegen wir* zum Mond!“

Mit Weltraumausrüstung meint die Lehrerin, dass die Flugspezialisten ihre iPads herausholen und sich bei ihrem Portal anmelden sollen, um auf die heutige Einheit mit dem Titel „Ab zum Mond!“ zuzugreifen.

Gerade als die Lehrerin anfangen will, wird sie von Johann unterbrochen: „Frau Lehrerin, hier steht, mein Passwort ist ungültig.“ Jana sagt: „Bei mir auch. Ich kann mich auch nicht einloggen.“ Frau Aldrin seufzt leise, legt ihr iPad beiseite und geht zu den Schülern, um sich die für die Mission unverzichtbare Ausrüstung anzuschauen.

Während sie ihre Probleme beim Einloggen behebt, ist ein Teil der Crew startklar fürs Lernen, während andere in Wartestellung verharren, weil sie ihre Zugangsdaten vergessen haben, ein falsches Passwort eingegeben haben oder wegen nicht ladender Websites.

Was zu Beginn der Stunde noch T-30 Sekunden Lernzeit waren, hat sich nun zu T+6 Minuten (und es werden immer mehr) verlorener Lernzeit entwickelt.

Die versteckten Kosten von Anmeldeproblemen



In jedem Schuljahr reduzieren verschiedene technikbedingte Störungen die Unterrichtszeit. Dazu gehören unter anderem:



Budgets und Finanzierung



Risiko im Bereich der Cybersicherheit



Digitale Kluft



Ablenkungen im Internet



Bedenken zur Gerätesicherheit

Zwar wirken sich all diese Faktoren zweifellos auf die Bildungseinrichtungen aus, doch ein oft übersehener Aspekt, der sich ebenso stark auf die Lernergebnisse auswirkt, sind die Herausforderungen, die zu Reibungsverlusten beim Anmeldevorgang führen.

Beispielsweise benötigt ein Schüler etwa **30 Sekunden bis drei Minuten**, um sich bei einem Gerät oder auf einer Website anzumelden. Obwohl konkrete Statistiken meist nicht veröffentlicht

werden, ist dieser Richtwert eine gute Orientierung, die Faktoren wie Tippkomfort, Systemkenntnis, Geräteleistung und Internetgeschwindigkeit berücksichtigt.

Auch wenn das Einloggen auf einer Website jeweils nur wenige Sekunden und die Authentifizierung auf dem Mac nur wenige Minuten dauert, summieren sich diese Verzögerungen im Laufe eines Schuljahres und führen zu einem erheblichen Verlust an Lernzeit aufgrund von Problemen bei der Authentifizierung.

In diesem Zusammenhang sind folgende wichtige, zeitkritische Durchschnittswerte zu beachten:

- Reaktionszeiten auf IT-/Helpdesk-Supportanfragen für nicht kritische Probleme: **1–2 Tage**
- Zurücksetzen eines vergessenen Passworts oder Entsperren eines Accounts: **15–30 Minuten**
- Erhalt einer Benachrichtigung zur Überprüfung der Authentifizierung von MFA: **8 Sekunden**

Jeder Schüler braucht 30 Sekunden um sich auf einer Website anzumelden × 4 Stunden: **= 2 Min. pro Tag**

2 Min. × 5 Tage/ Woche: **= 10 Min./ pro Woche**

10 Min. × 36 Wochen: **= 360 Min.**

360 Min. / 60 Min.: **= 6 Std. pro Schuljahr**

Bevor wir die Mathematik hinter Anmeldeaufwand näher beleuchten, legen wir einige Variablen für Schulen fest:

- Die Schüler haben in der Regel **4 bis 8 Stunden pro Tag**.
- Ein typischer Schultag dauert **7 Stunden**
- Die Schulen sind **an fünf Tagen in der Woche** geöffnet.
- Ein Schuljahr umfasst im Durchschnitt **180 Tage** (bzw. 36 Wochen)
- Die Gesamtlernzeit pro Schuljahr beträgt **1.260 Stunden**
- Die durchschnittliche Schülerzahl pro Grundschule (USA) lag bei **470 Schülern**
- **780,85 Millionen Schüler in der Grundschulbildung weltweit im Jahr 2024**



Was bedeuten diese Zahlen?

Bei nur 30 Sekunden pro Anmeldung verliert jeder Schüler allein durch eine einzige Website etwa 6 Stunden Lernzeit pro Schuljahr. Lassen Sie das einmal auf sich wirken.

Das berücksichtigt weder erneute Anmeldeversuche nach Tippfehlern noch den Aufruf mehrerer Lernportale mit jeweils eigenen Zugangsdaten. Denn das könnte bei jedem Fehler oder jeder weiteren Website, für die eine separate Anmeldung erforderlich ist, weitere 30 Sekunden kosten.

Es berücksichtigt auch keine vergessenen Passwörter oder gesperrten Konten – die als Multiplikator wirken und zu

kumulierten Verzögerungen von durchschnittlich 15 Minuten (bei Erstgenanntem) bis zu einem Tag (bei Letztgenanntem, falls ein Support-Ticket nötig ist) führen.

30 Sekunden pro Website und Schüler entsprechen in den USA insgesamt 2.820 Stunden verlorener Lernzeit pro Bildungseinrichtung und Schuljahr; weltweit beläuft sich die insgesamt verlorene Lernzeit für Schüler in Schulen auf 4.680.510.000 Stunden.

Was wäre, wenn die Schwierigkeiten beim Einloggen – einschließlich Passwortzurücksetzungen und Sperrungen von Accounts – so weit minimiert werden könnten, dass die Schüler nur einmal eine Authentifizierung durchführen müssten und sofort auf alles zugreifen könnten, was sie zum Lernen benötigen?

Inhalt dieses Leitfadens

In unserem Einführungsleitfaden „**Identitäts- und Zugriffsverwaltung an Schulen für Einsteiger**“ haben wir erläutert, was IAM ist und warum es wichtig ist. Nun wollen wir uns eingehender mit einer der leistungsstärksten Anwendungen von IAM befassen: **dem nahtlosen Zugriff über Single Sign-On (SSO)**.



Wir werden Folgendes behandeln:

- Wie umständliche Anmeldeverfahren Unterrichtszeit rauben und Ungleichheit schaffen.
- Was nahtloser Zugang in der Praxis bedeutet.
- Auswirkungen in der Praxis: Zeitersparnis, weniger Tickets und wiederhergestelltes Lernen.
- Wie Sie herausfinden können, ob Ihre Schule für SSO bereit ist.

Kleine Störungen, große Verluste

Wir haben gesehen, wie Anmeldeprobleme die Lernumgebung pro Klasse und Schule weltweit beeinträchtigt. In diesem Abschnitt beleuchten wir die verschiedenen Ausprägungen dieses Phänomens und seine Auswirkungen auf die Leistung von Schülern, Lehrern und dem IT-Team.

Der wahre Preis für nur noch ein weiteres.

Schüler

- Ungleiche Zugangsmöglichkeiten (digitale Kluft) schränken ihre Teilnahme an modernem, kombiniertem Lernen ein.
- Verlust an Dynamik bei kritischen Lernübergängen erschwert das Einhalten des Lehrplans.
- Dies führt zu Lernlücken, wodurch sie im Unterricht und beim Lernen zu Hause weiter hinter ihre Mitschüler zurückfallen.
- Wenn kritische Fähigkeiten nicht entwickelt werden, führt dies zu Frustration im Umgang mit Technologie und zu Konzentrationsverlust.
- Die Entfremdung von Mitschülern und Lehrkräften behindert den Lernfortschritt zusätzlich und verstärkt das Desinteresse.

Lehrkräfte

- Der Unterricht beginnt später als geplant, wodurch sich die Unterrichtszeit erheblich verkürzt.
- Das personalisierte Lernen wird durch die begrenzte Zuverlässigkeit digitaler Tools beeinträchtigt.
- Zunehmende Störungen erschweren den Unterrichtsfluss und die Einbindung der Schüler.
- Wenn man den technischen Support übernimmt und Unterrichtspläne anpassen muss, muss man sich Umgehungslösungen ausdenken, anstatt zu unterrichten.
- Technikmüdigkeit oder Burnout aufgrund der zunehmenden psychischen Belastung durch digitale Anforderungen im Unterricht.

IT-Teams

- Zu Beginn jedes Schuljahres steigt die Zahl der Helpdesk-Tickets sprunghaft an, was zu einer höheren Arbeitsbelastung und mehr Stress führt.
- Durch Verzögerungen bei der manuellen Bereitstellung haben Schüler und Lehrer keinen Zugang zu den Lernmaterialien.
- Probleme im Zusammenhang mit Passwörtern überschwemmen den Helpdesk und beeinträchtigen die Produktivität aller Beteiligten erheblich.
- Sicherheitsvorfälle nehmen aufgrund schwacher Anmeldedaten und der gemeinsamen Nutzung von Passwörtern zu, was zudem Datenschutzrisiken mit sich bringt.
- Man verbringt zuviel Zeit damit, Probleme zu priorisieren und zu beheben, anstatt seine Fähigkeiten auf strategische Initiativen und die Verbesserung der Schülererfahrung zu konzentrieren.



Eine Frage der Gerechtigkeit

Stellen Sie sich einmal folgende Frage: Verlieren manche Schüler mehr Zeit durch Probleme beim Einloggen als andere?

Bevor Sie antworten, überlegen Sie bitte, wie sich die folgenden Punkte auf die Gerechtigkeit auswirken:

- Jüngere Schüler haben in der Regel größere Schwierigkeiten damit, sich Passwörter zu merken, als ältere Schüler.
- Unterschiedliche Lernpräferenzen erhöhen den kognitiven Aufwand, den Schüler aufbringen müssen, um Informationen zu verarbeiten.
- Englischlernende (ELL) müssen gleichzeitig sprachliche und technische Hürden überwinden, um schulische Erfolge zu erzielen.
- Schüler, die Geräte gemeinsam nutzen, haben oft größere Schwierigkeiten aufgrund wiederholter Authentifizierungsvorgänge.
- Bei einem höheren Schüler-Gerät-Verhältnis kommt es zu kumulierten Verzögerungen wie träger Leistung und technischen Störungen.

Rufen Sie sich nun noch einmal Ihre vorherige Antwort ins Gedächtnis – und berücksichtigen Sie dabei die oben genannten Aspekte der Chancengleichheit –, und beantworten Sie die folgende Frage: **Haben alle Schüler den gleichen Zugang zu technologiegestütztem Lernen?**

Die IT-Belastung, über die niemand spricht

Es steht außer Frage, dass eine der Kernaufgaben der IT darin besteht, Unterstützung für Schüler, Lehrer und die Schule selbst bereitzustellen. Von personalisierter Problemlösung über die Einbindung von Beteiligten bis hin zu herausragenden digitalen Erlebnissen und Infrastrukturverbesserungen – all das treibt moderne Bildungsumgebungen voran.

Und doch gibt es Bereiche des Supports, die häufig die IT-Ressourcen in Anspruch nehmen und dadurch einen Dominoeffekt auslösen, der den Umfang und die Tiefe des Supports einschränkt, den die IT den Schülern, Lehrkräften, Schulen, Schulbezirken und Bildungseinrichtungen bieten kann.

Allen voran: oft übersehene Passwortprobleme. Lassen Sie uns die versteckten Kosten aufdecken:

- Untersuchungen zeigen, dass bis zu **50 % aller IT-Helpdesk-Anfragen** die Zurücksetzung von Passwörtern betreffen.
- Laut **Forrester Research** kostet eine einzelne Passwortzurücksetzung etwa 70 US-Dollar. Dies bedeutet, dass während des gesamten Schuljahres viel Zeit und Geld für die Passwortverwaltung aufgewendet wird.
- Ressourcen, die besser für strategische Initiativen eingesetzt werden könnten, beispielsweise für eine engere Ausrichtung auf die Lernziele.

Das (unbeabsichtigte) Sicherheitsrisiko: Wenn Technologie zur Belastung wird, suchen die Beteiligten nach Ausweichlösungen. Dies gilt auch für Passwörter, was häufig zu Sicherheitslücken führt:

- Die Verwendung leicht zu erratender Passwörter: Fast **6 von 10 Passwörtern aus der Praxis lassen sich in** weniger als einer Stunde knacken, fast die Hälfte davon in nur wenigen Sekunden.
- Das gleiche Passwort für jeden Account verwenden: Angreifer **automatisieren das Testen gestohlener Anmeldedaten auf Hunderten von Websites**; dasselbe Passwort = mehr Zugriffsmöglichkeiten.
- Passwörter auf Haftnotizen notieren: Jeder weiß doch, **dass man das Passwort für den Computer auf einem gelben Haftzettel** unter der Tastatur aufbewahrt.
- Gemeinsame Nutzung von Accounts mit anderen Beteiligten: Untersuchungen haben ergeben, dass **16 % bzw. 22 % der Befragten ihre Passwörter an Freunde bzw. Kollegen weitergeben**.
- Nie geänderte Passwörter: Bei einem Datenleck im Jahr 2025 **wurden 16 Milliarden Anmeldedaten offengelegt**, die aus verschiedenen Sicherheitsverletzungen stammen und für Cyberangriffe verwendet werden können.

Warum haben riskante Verhaltensweisen im Umgang mit Passwörtern einen so großen Einfluss auf die Cybersicherheit im Schulbereich?

Zwei Worte: **Kompromittierte Anmeldedaten.**

Laut IBM liegt diese Hauptursache an dritter Stelle – weltweit macht sie etwas mehr als 10 % der ursprünglichen Angriffsvektoren aus. Auch wenn 10 % auf den ersten Blick als gering erscheinen – besonders verglichen mit Phishing oder Ransomware im Bildungsbereich –, gilt:

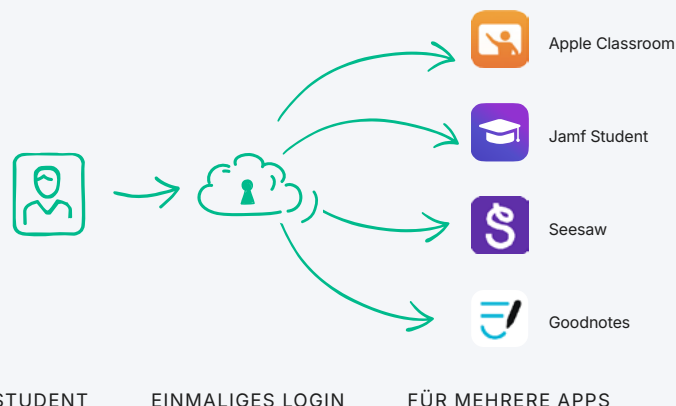
- Die meisten Phishing-Kampagnen dienen als Vorstufe zum Abgreifen von Zugangsdaten, bevor sie groß angelegte Cyberangriffe wie Malware und Datendiebstahl starten.
- Regulierte Branchen, wie beispielsweise das Schulwesen, unterliegen lokalen, bundesstaatlichen, nationalen und/oder regionalen Gesetzen zum Schutz sensibler und vertraulicher Informationen. PII und PHI sind für Angreifer besonders attraktiv – das macht den Bildungsbereich zum datenreichen Ziel für Cyberangriffe.
- Die durchschnittlichen Kosten eines einzelnen Sicherheitsvorfalls aufgrund kompromittierter Anmeldedaten werden laut einer Auswertung des „**Cost of a Data Breach Report 2025**“ auf 4,67 Millionen US-Dollar geschätzt.



Was versteht man unter nahtlosem Zugang?

Einmaliges Anmelden. Lernen ohne Ende.

Nahtloser Zugang – das Konzept sieht vor, dass sich die Beteiligten im Bildungsbereich zu Beginn ihres Tages einmalig für die Authentifizierung anmelden. Von dort aus wechseln sie mühelos zwischen digitalen Tools wie Apps, Bildungswebsites und Lernangeboten hin und her, ohne ihr Passwort erneut eingeben zu müssen.



Ein Tag im Leben eines Schülers



Ankunft am Morgen (8:15 Uhr):

Maya holt sich ein gemeinschaftlich genutztes iPad. Sie tippt auf ihr Bild und gibt einen einfachen vierstelligen Passcode ein. Sie hat Zugriff auf ihre altersgerechten Apps, die Einstellungen für Bedienungshilfen und ihre persönlichen Dateien.

1. Stunde – Deutsch (8:30 Uhr):

Sie ruft das Lernmanagementsystem auf – eine Authentifizierung ist nicht erforderlich, da sie bereits authentifiziert ist. Sie sieht sich die heutige Aufgabe an, wechselt nahtlos zum digitalen Lehrbuch, markiert eine Passage und fügt in Pages eine Notiz hinzu. Und das alles, ohne zusätzliche Passwörter eingeben zu müssen.

2. Stunde – Mathematik (9:30 Uhr):

Maya tippt auf die Mathe-App, um Bruchrechnen zu üben. Auch hier gibt es keinen Anmeldebildschirm. Sie fängt einfach direkt mit dem Lernen an und macht genau dort weiter, wo sie gestern aufgehört hat, denn die App weiß, wer sie ist.

Gemeinschaftsprojekt (10:30 Uhr):

Wenn es an der Zeit ist, gemeinsam mit drei Klassenkameraden an einer Gruppenpräsentation zu arbeiten, öffnet sie Keynote. Da die Authentifizierungen mit verwalteten Apple-Accounts verknüpft sind, können alle Benutzer gleichzeitig an derselben Datei arbeiten. Keine Weitergabe von Passwörtern, keine Zugriffsprobleme – einfach nahtlose Zusammenarbeit.

Ende des Tages (15:00 Uhr):

Bevor Maya das iPad wieder zurückbringt, meldet sie sich von ihrer Sitzung ab. Dadurch werden ihre Daten mit iCloud synchronisiert, und das iPad wird durch das Löschen der Sitzung für den nächsten Schüler vorbereitet. Morgen kann sie die gleiche Authentifizierung auf jedem iPad in der Schule durchführen und genau dieselbe personalisierte Sitzung nutzen.

Aus der Sicht der Lehrkraft

Vor dem Unterricht:

Den Unterrichtsplan durchgehen – keine Zeitverschwendung durch Probleme beim Einloggen oder bei der Vorbereitung der iPads, da SSO eingerichtet ist.

Während des Unterrichts:

Die Schüler melden sich an und sind innerhalb von 30 Sekunden lernbereit. Der Unterricht beginnt pünktlich, wodurch die Dynamik und das Engagement aufrechterhalten werden.

Nach dem Unterricht:

Der Schwerpunkt liegt auf dem Feedback zu den Arbeiten der Schüler – nicht darauf, als technischer Support zu fungieren oder Anfragen zu Accounts an die IT-Abteilung weiterzuleiten.

Wie funktioniert das alles? Die drei Säulen:

1.

Verwaltete Apple-Accounts:

Nahtlos in Ihren cloudbasierten Identitätsdienst (Google Workspace, Microsoft Entra ID oder RapidID) integriert – für automatische Bereitstellung und einheitlichen Zugriff auf Apple-Dienste.

2.

Passwortloser Arbeitsablauf:

Authentifizierung per Fingertipp, um die Effizienz zu steigern, die kognitive Belastung zu verringern und gleichzeitig die Sicherheit zu gewährleisten. Ideal für jüngere Schüler oder Benutzer mit einer Lernbehinderung.

3.

Single Sign-On:

Ein einziger Account, der nur einmal durch Authentifizierung bestätigt werden muss, ermöglicht den Zugriff auf alle verbundenen Anwendungen – sowohl webbasierte als auch native Apps.

Die praktischen Auswirkungen eines nahtlosen Zugangs

Gewonnene Unterrichtszeit

Die Unterrichtszeit ist begrenzt, und kleine Störungen summieren sich schnell. Schwierigkeiten beim Einloggen sind ein ständiges Hindernis, das den Unterricht verzögert und den Lernfluss im Klassenzimmer unterbricht. Durch die Reduzierung dieser Unterbrechungen können Lehrkräfte sich besser auf den Unterricht konzentrieren, während die IT-Abteilung effektivere und nahtlose Lernerfahrungen schaffen kann.

Daten zum Thema „verlorene Zeit“

Wie Sie sich vielleicht aus dem ersten Abschnitt erinnern, umfasst ein durchschnittliches Schuljahr 1.260 Stunden. Diese Zahl – die je nach Region variieren kann – veranschaulicht nachfolgend, wie kritisch die Rückgewinnung verlorener Unterrichtszeit ist.

Im Jahr 2024 stellten Forscher der Brown University fest, dass fast **25 % der Unterrichtszeit pro Schuljahr** unter anderem aufgrund von Unterbrechungen und Fehlzeiten verloren gehen. Auch wenn einige der in der Studie angeführten Beispiele – wie etwa eine 30-sekündige Störung der Lautsprecheranlage – zunächst unbedeutend erscheinen mögen, folgen darauf oft mehrere Minuten andauernde Unterbrechungen, in denen versucht wird, die Aufmerksamkeit der Schüler wiederzugewinnen.

Zeitverlust durch Technik

Im Rahmen einer ähnlichen Studie aus dem Jahr 2021 stellten die Forscher fest, dass technologiebedingte Unterbrechungen zu den häufigsten Arten von Unterbrechungen zählen. Mithilfe von Beobachtungs- und Umfragedaten stellten sie einen Zusammenhang zwischen den Auswirkungen fest, wie sich nachfolgende Störungen auch nach einer anfänglich noch so geringfügigen Unterbrechung weiterhin negativ auf die Chancen der Schüler auswirken.

Mehr als 50 % der Unterbrechungen führten zu einem längeren Lernverlust; die Forscher stellten fest, dass dies „dazu führte, dass die Schüler vom Unterricht abgelenkt wurden“ und „der Lehrer den Unterricht unterbrechen musste“.



In jeder Lernumgebung – sowohl auf dem Schulgelände als auch außerhalb – kommt es zu Problemen beim Einloggen. Typische Beispiele dafür gibt es jeden Tag, und irgendwann erlebt das jeder Schüler in folgender Form:

- Verzögerungen aufgrund nicht intuitiver Benutzeroberflächen
- Lange Ladezeiten aufgrund ineffizienter Verfahren zur Authentifizierung
- Passwortmüdigkeit durch das Jonglieren mit mehreren Accounts
- Zugriff verweigert, da ein falsches Passwort eingegeben wurde
- Ungültige Passwörter aufgrund unterschiedlicher Komplexitätsanforderungen
- Gesperrte Konten durch Auslösen einer Passwortrichtlinie

Was SSO kann

Einfach ausgedrückt: SSO reduziert Probleme, die durch Passwörter verursacht werden, und damit auch die durch die Technologie verursachten Störungen. Es handelt sich um den Kanal, über den sich die Schüler bei der ersten Anmeldung einmalig sicher authentifizieren und anschließend nahtlos zwischen den Apps, Websites und Diensten wechseln können, die sie für das Lernen nutzen.

In jeder Unterrichtsstunde, jeden Tag und im Laufe des Schuljahres summiert sich die eingesparte Zeit und führt zu:

- Effizienzsteigerungen bei der Produktivität im Unterricht und im Schulbetrieb
- Weniger Sicherheitsrisiken und -bedrohungen und weniger Schwachstellen
- Systematische Vereinheitlichung von Konformität und Governance über alle Institutionen hinweg
- Steigerung des ROI durch Senkung der Gesamtbetriebskosten

Was Lehrer mit der gewonnenen Zeit anfangen können

Dieser Leitfaden zeigt die häufigsten Bereiche für Zeitersparnisse bei Lehrkräften:

- Sie können sofort mit dem Unterricht beginnen und sorgen dafür, dass die Energie und die Motivation erhalten bleiben.
- Sie verbringen mehr Zeit mit dem Unterricht und weniger mit der Fehlerbehebung.
- Sie können den Unterrichtsstoff durchgehen, ohne sich zu sehr zu beeilen.
- Sie haben mehr Zeit für Fragen der Schüler und für einen differenzierten Unterricht.

Anstatt jedoch eine Aussage zu treffen, möchten wir den Akteuren im Bildungsbereich gern eine Frage stellen: Wenn Sie sich an den ersten Abschnitt erinnern, haben wir berechnet, dass jeder Schüler pro Schuljahr etwa 6 Stunden Unterrichtszeit verliert, ausgehend von einer 30-sekündigen Unterbrechung durch das Einloggen auf einer Website während jeder Unterrichtsstunde.

In dieser Zeit müssen die Lehrer ihren Unterricht unterbrechen und warten, bis die Schüler bereit sind, damit sie mit dem Unterricht fortfahren können. Die Frage lautet also:

Was können Ihre Lehrkräfte erreichen, wenn die Zeit, die durch tägliche Unterbrechungen, Störungen und längere Verzögerungen verloren geht, wieder gewonnen wird?

Auswirkungen auf die IT – vom Brandlöschen zur Strategieentwicklung

Neben Produktivitätsgewinnen und weniger passwortbedingten Sicherheitsrisiken hilft die SSO-Einführung gleichzeitig, **die Helpdesk-Kosten um durchschnittlich 40 % zu senken**.

Erwartete Auswirkungen von SSO

Schließlich bedeutet eine Reduzierung dieser Größenordnung – da die Hälfte aller Tickets auf Konto- und Passwortprobleme entfällt –, dass die IT-Abteilung nun in der Lage ist, sich schneller um wichtigere Probleme zu kümmern. Das heißt: Bei 10 Support-Tickets verschiebt sich das Verhältnis von kritischen zu unkritischen Problemen von 1:2 (ohne SSO) auf 7:3 (mit SSO).

Wo die IT die gewonnene Zeit investieren kann

Neben den Auswirkungen auf die Arbeitsbelastung wirkt sich dies auch positiv auf die Zeit aus. Durch die Automatisierung, Zentralisierung und Optimierung der Authentifizierungsprozesse mittels SSO kann die IT die dadurch gewonnene Zeit für strategische Ziele nutzen:

- Bessere Erfahrungen aller Stakeholder mit der Technik
- Optimierung der Produktions- und Betriebsabläufe
- Modernisierung und Verbesserung der IT-Infrastrukturen an den Schulen
- Aufbau von Kompetenzen der Interessengruppen durch technische Schulungen
- Bessere Abstimmung auf die angestrebten Lernergebnisse

Ergebnisse in Bezug auf die Gleichberechtigung

Zugangslücken

Die Schüler finden nicht alle gleichzeitig wieder ihren Fokus nach den alltäglichen Störungen. Im Jahr 2025 bestätigten Forscher dies, als **ihre Ergebnisse zeigten**, dass „*ein Schüler im Durchschnitt 25 Prozent der Unterrichtszeit durch diese zahlreichen Unterbrechungen verliert*“. Unterbrechungen wie:

- Schüler kommen zu spät
- Abwesenheiten von Lehrkräften
- Durchsagen über die Haussprechanlage
- Unterrichtsbesuche

Sind an Grund- und weiterführenden Schulen weltweit weit verbreitet. Wenn man unseren durchschnittlichen 7-stündigen Schultag zugrunde legt, verkürzt sich die Unterrichtszeit durch eine Kürzung um 25 % (1,75 Stunden) auf 5,25-stündige Schultage.

Dementsprechend wirken sich Probleme beim Einloggen nicht nur auf die Unterrichtszeiten aus – auch bei anderweitigen Störungen dauert es ähnlich lange, bis die Schüler sich wieder konzentriert haben.

Nicht alle Schüler erleben technische Probleme im gleichen Maße. Faktoren in Bezug auf die Gleichberechtigung, die den Unterrichtsausfall verstärken, sind Probleme mit:

- Auswendiglernen
- Kognitive Belastung
- Sprachbarrieren
- Körperliche Behinderung

🔧 Wie SSO hilft

Alle Schüler haben gleichberechtigten Zugang, was ihnen die Möglichkeit gibt, überall zu lernen, wo Lernen stattfindet – unabhängig von ihren technischen Fähigkeiten. Bei der Entwicklung von SSO wurden folgende Aspekte berücksichtigt:

- Die Schüler müssen sich die Anmeldedaten für einen einzigen Account merken.
- Die Sicherheit ist bereits integriert, sodass Passwörter komplex sein können (es lassen sich jedoch auch benutzerfreundliche Passwörter konfigurieren), ohne dass die Sicherheit darunter leidet.
- Die Authentifizierung ist optimiert, sodass sie für alle Benutzer jedes Mal gleich aussieht und gleich reagiert.
- Die Anmeldedaten werden zentral verwaltet und lassen sich ganz einfach im Self-Service oder – bei Bedarf – mit Unterstützung durch Lehrkräfte oder die IT-Abteilung verwalten.

👤 Der „Würdefaktor“

Wenn sich ein Schüler nicht einloggen kann, während seine Mitschüler dies können, ist das nicht nur ein technisches Problem – es ist auch ein emotionales. SSO beseitigt diese Quelle von Frustration und Verlegenheit und schafft so ein inklusiveres Unterrichtsumfeld.

Verbesserungen im Bereich der Sicherheit

Wussten Sie, dass „*Passwörter die Hauptursache für mehr als 80 Prozent der Datenlecks sind*“? Laut der Fast Identity Online (FIDO) Alliance ist dies eine bevorzugte Angriffsmethode von Angreifern, da diese **leicht durch Phishing erbeutet, abgefangen oder auf andere Weise geknackt werden können**.

@ Sicherheitsvorteile von SSO

Zu den wichtigsten Vorteilen zählt die Zentralisierung der Passwortrichtlinien auf IdP-Ebene. Dies trägt nicht nur zur Konformität bei (worauf wir im nächsten Abschnitt eingehen werden), sondern sorgt auch für eine umfassende Stärkung der Passwortsicherheit, indem die Sicherheitsstandards in der gesamten Infrastruktur der Schule vereinheitlicht werden – wodurch für jede App, jede Website und jeden Dienst das gleiche Maß an Zugriffsschutz gewährleistet wird. Darüber hinaus bietet SSO die folgenden Sicherheitsvorteile für das Schulwesen:

- Erspart das Erstellen und Merken mehrerer Passwörter
- Sie müssen nur einheitliche Richtlinie für starke Passwörter festlegen – statt vieler komplexer Regeln.
- Die Zugriffsrechte werden rollenbasiert anstatt einzeln oder manuell festgelegt.
- Die gemeinsame Nutzung von Accounts wird reduziert (eine gängige Praxis, wenn sich Beteiligte nicht anmelden können).
- Die Löschung inaktiver Accounts wird automatisiert, sobald ein Schüler die Schule verlässt.
- Erhöhte Sicherheit des Accounts durch die Verwendung von MFA, um unbefugten Zugriff zu minimieren.

🔍 Vertrauen in die Konformität

Die Umsetzung von Schutzmaßnahmen ist nur ein Aspekt der Sicherheit. Ein weiterer, ebenso wichtiger Punkt ist es, sicherzustellen, dass die mehrstufigen Kontrollmechanismen wie vorgesehen funktionieren. Darüber hinaus dient jede dieser Funktionen der Umsetzung Ihrer Betriebsstrategie in der Schule. Das bedeutet, die Konformität durchzusetzen und der IT-Abteilung standardisierte Mittel für folgende Aspekte zur Verfügung zu stellen:

- Zentrale Überwachung aller Zugriffsversuche
- Dokumentation von Zugriffskontrollen für Richtlinienprüfungen
- Eindeutiger Nachweis von angemessenen Schutzmaßnahmen
- Detaillierte Prüfpfade zur Einhaltung gesetzlicher Vorschriften



Gesamtbetriebskosten (TCO)

Das Gesamtbild

Die Technologiekosten im Bildungswesen gehen über den Listenpreis der Hardware selbst hinaus. Rechnet man die Backend-Kosten zusammen – darunter Softwarelizenzen, Garantie und Support, Schulungen, Wartung und Außerbetriebnahme –, steigen die Gesamtbetriebskosten über die gesamte Nutzungsdauer eines Geräts auf mehrere tausend US-Dollar pro Gerät. Je nach Größe Ihrer Einrichtung können Tausende von Geräten Gesamtkosten schnell über die **reinen Anschaffungskosten** treiben.

Betrachten Sie die folgende Grundformel zur Berechnung der TCO anhand von Branchendurchschnittswerten:

Preis eines Apple iPads (128 GB):	329 USD
AppleCare+ für Schulen (3 Jahre):	79 USD
iPad-Hülle (robust):	20 USD
329 USD + 79 USD + 20 USD	= 428 USD (pro Gerät)

Anzahl der Schüler (Einzelgeräte):	1.000
428 USD x 1.000	= 428.000 USD

Geschätzte Kosten pro Gerät (3 Jahre):	194 USD
194 USD x 1.000	= 194.000 USD

Gesamtbetriebskosten (TCO) (nur Hardware und Garantie):	
428.000 USD + 194.000 USD	= 622.000 USD
194.000 USD / 428.000 USD	= 0,45
0,45 x 100	= 45 %

Die Kosten für Softwarelizenzen, Schulungen, Wartung und Außerbetriebnahme variieren je nach den Anforderungen der einzelnen Schulen stark, sodass sie sich nur schwer beziffern lassen. Zudem gibt es je nach Institution und/oder Führungsstruktur Abweichungen bei den Variablen, die sich möglicherweise zusätzlich auf die Kostenunterschiede auswirken.

Möglichkeiten zur Kostensenkung

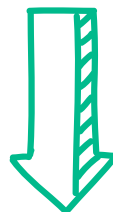
Angesichts der Kosten, die mit der Anschaffung, Verwaltung und Absicherung von Technologie verbunden sind, ist es nicht verwunderlich, dass Institutionen daran interessiert sind, Möglichkeiten zur Senkung der Gesamtbetriebskosten zu finden – und damit möglicherweise die Kapitalrendite (ROI) zu steigern.

Im Jahr 2023 führte Forrester Consulting eine Studie mit dem Titel **The Economic Impact of Microsoft Entra** durch, um den ROI der IdP-Lösung von Microsoft im Vergleich zum Einsatz mehrerer verschiedener Lösungen zu bewerten. Das Endergebnis lieferte zwei interessante Erkenntnisse:

- Die Modernisierung der Geräteverwaltung, der Identitätsverwaltung und der Sicherheit bedeutet, die Komplexität zu reduzieren und die Tools zu zentralisieren.
- Durch die Abkehr von einem „Flickenteppich“ (mehr dazu im nächsten Abschnitt) mit zahlreichen Einzellösungen wurde eine Kapitalrendite (ROI) von 240 % erzielt, wobei gleichzeitig die Sicherheit erhöht und die Kosten gesenkt wurden.

Weitere Kosten, die SSO reduzieren hilft:

- IT-Personal: Durch die standardisierte Verwaltung und Bereitstellung der Accounts lassen sich die Kosten im Zusammenhang mit passwortbezogenen Tickets und Zurücksetzungsanfragen erheblich senken.
- Unterrichtszeit: Schon die Rückgewinnung eines Teils der pro Schüler verlorenen Unterrichtszeit von 25 % bedeutet einen erheblichen pädagogischen Gewinn für alle Beteiligten.
- Lizenzoptimierung: Die automatisierte Freigabe führt dazu, dass nicht genutzte Lizenzen neu zugewiesen werden können



SSO für Laien

Die Technologie verstehen, ohne sich in der Komplexität zu verlieren

Man muss kein Experte für Cybersicherheit sein, um zu verstehen, dass SSO nicht nur den Zugriff auf Geräte und Ressourcen in Schulen schützt, sondern auch die Lernzeit vereinfacht durch:

- ✓ Minimierung der technologischen Komplexität
- ✓ Verbesserung der Transparenz bei der Authentifizierung
- ✓ Minimierung versteckter Schwachstellen
- ✓ Verbesserung des Sicherheitsstatus



- ✓ Reduktion menschlicher Fehler
- ✓ Automatisierte Verwaltung der Accounts
- ✓ Vereinfachung der Anmeldeprozesse
- ✓ Konsolidierung von IT-Tools

„Komplexität ist der Feind der Sicherheit.“
– Bruce Schneier

Lassen wir die Theorie einmal beiseite und betrachten wir ein praktisches Beispiel aus einem realen Anwendungsfall im Schulbereich, bei dem das Apple iPad zum Einsatz kommt.



Es klingelt und der Unterricht beginnt. Pünktlich wie ein Uhrwerk holen die Schüler ihre iPads heraus und melden sich über eine der SSO-Varianten auf ihren Geräten an, während der Lehrer den Unterricht vorbereitet. Nach wenigen Minuten ist die Klasse auf dem Gerät angemeldet.



Pause.

Die Schüler benötigen ein paar Minuten, um sich bei ihrem Portal anzumelden, das eine zweite SSO-Lösung nutzt. Im Portal folgen sie den Erklärungen des Lehrers bis der Unterricht endet. Nun öffnen die Schüler ihre Textverarbeitungs-App, um mit dem Schreiben zu beginnen.



Eine weitere Pause.

Es gibt ein drittes SSO-Produkt, das ausschließlich für diese App verwendet wird. Es entsteht noch eine Pause, bis sich alle zum dritten Mal authentifiziert haben.

Gut, wir sind jetzt in der Textverarbeitungs-App und beginnen mit der Arbeit an unserem Gruppenprojekt.



Oh nein, nicht schon wieder! Ja, schon wieder. Um in Echtzeit zusammenarbeiten zu können, müssen die Schüler auf die Kollaborations-App zugreifen, die – Sie haben es erraten – eine weitere SSO-Instanz nutzt. Die Schüler müssen ihre derzeitige Tätigkeit noch einmal unterbrechen, um sich zum fünften Mal anzumelden.

Leider ist die einstündige Unterrichtsstunde fast schon vorbei, bis die Schüler wieder den Anschluss gefunden haben, und sie haben etwa 15 Minuten – also 25 % der Unterrichtszeit – damit verbracht, sich bei verschiedenen SSO-Versionen zu authentifizieren, die in einem „Flickenteppich“ aneinandergereiht wurden, um Single Sign-On nachzuahmen.

Manche Produkte versprechen zwar SSO für iPadOS, doch echtes SSO bedeutet nahtlosen Lernzugang: Einmaliges Anmelden beim ersten Login auf dem iPad genügt. Danach können sie auf Folgendes zugreifen:

- Institutionelle Portale
- Schulmaterialien
- Bildungswebsites
- Cloud-basierte Dienste
- Geräte-Apps

Die Erstanmeldung erfolgt automatisch im Hintergrund und gewährt direkt nahtlosen Zugriff – ohne manuelles Eingreifen oder Verzögerung.

Kernkonzept

Ein Login, viele Apps:

SSO funktioniert wie ein Backstage-Pass bei einem Konzert. Wenn Sie Ihre Anmeldedaten einmal am Eingang vorzeigen, haben Sie Zugang zu allen Bereichen, ohne Ihren Ausweis erneut vorzeigen zu müssen. Ihr Identitätsdienst (Google Workspace, Microsoft Entra ID oder Okta) ist die Sicherheitsüberprüfung, die für Sie bürgt, egal auf welche jede App Sie zugreifen.



Sicherheit ohne Barrieren

SSO beeinträchtigt die Sicherheit nicht – es verbessert sie. Im Folgenden finden Sie eine kurze Übersicht darüber, wie SSO die Identität von Grund auf schützt:

1.

Der Stakeholder authentifiziert sich einmalig mit seinen Anmeldedaten beim IdP. (Dies passiert in der Regel bei der ersten Anmeldung auf dem Gerät.)

2.

Nach der Überprüfung der Anmeldedaten stellt der Identitätsdienst (IdP) ein digitales Token aus, das die Identität des Beteiligten kryptografisch sichert.

3.

Wenn der Stakeholder zu einem Dienstanbieter (SP) navigiert, beispielsweise zu einer geschützten Ressource, sendet der IdP das digitale Token an den Anbieter.

4.

Der SP überprüft die Gültigkeit des Tokens und gewährt dem Beteiligten den sicheren Zugriff auf die Ressource – ganz ohne Passwort!

Es funktioniert überall



Für webbasierte Apps:

Lernmanagementsysteme, Canvas, Khan Academy, BrainPOP – die Schüler klicken einfach darauf und schon sind sie drin.

Bei nativen iPad-Apps:

Bei Pages, Keynote, GarageBand und Bildungs-Apps wie Seesaw und Goodnotes wird der verwaltete Apple-Account des Schülers für die automatische Anmeldung erkannt.

Bei gemeinsam genutzten iPads:

Jeder Schüler erhält auf jedem Gerät in der Schule sein individuelles Nutzererlebnis. Wenn sie sich abmelden, endet die temporäre Sitzung, ihre Arbeit bleibt jedoch sicher in iCloud gespeichert.

IT-Kontrollebene

Ein hervorragendes SSO-System ermöglicht Schülern und Lehrkräften einen reibungslosen Zugriff, während die IT-Abteilung hinter den Kulissen die Kontrolle über Sicherheit und Konformität behält. Als Teil einer umfassenden „Defense-in-Depth“-Strategie – die Integration von Geräteverwaltung, Identitäts- und Zugriffsmanagement sowie Endpunktsicherheit – fungiert SSO als Kontrollebene zum Schutz von Benutzern, Geräten und sensiblen Daten in Schulen. Das hat die IT mehrere Vorteile:



Überblick in Echtzeit

darüber, wer auf welche Ressourcen zugreift



Richtlinienbasierte Zugriffskontrollen

(nach Klassenstufe, Rolle oder Bereitstellung)



Systematische Bereitstellung

beim Registrieren von Schülern oder beim Wechsel der Klassenstufe



Automatische

Deaktivierung bei Abschluss oder Wechsel der Schüler



Robuste

Sicherheitsprotokolle zur Gewährleistung einer sicheren, plattformübergreifenden Kommunikation

Ist Ihre Schule bereit für SSO?



Bewertung der SSO-Bereitschaft

Nutzen Sie diese Checkliste, um zu beurteilen, wo Sie derzeit stehen und welche Schritte Sie unternehmen müssen, um einen nahtlosen Zugang zum Lernen zu realisieren.

Identitätsinfrastruktur

- ☐ Cloud-basierter Identitätsdienst (Google Workspace, Microsoft Entra ID, RapidID)
- ☐ SIS mit IdP-Integration
- ☐ Die Identitätsdaten sind systemübergreifend konsistent
- ☐ Einrichtung von Apple School Manager
- ☐ Für Schüler und Mitarbeiter werden (bzw. können) verwaltete Apple-Accounts angelegt (werden)

Geräteverwaltung

- ☐ Einrichtung einer MDM-Lösung (Jamf School oder Jamf Pro)
- ☐ MDM mit IdP-Integration
- ☐ Gemeinsam genutzte iPads, Einzelgeräte oder Hybridmodell
- ☐ In Apple School Manager registrierte Geräte

Anwendungsbereitschaft

- ☐ Ermittlung der 10 meistgenutzten Lern-Apps
- ☐ Ermittlung von Apps, die SAML, OAuth (oder andere SSO-Protokolle) unterstützen
- ☐ Erstellung eines Plans für Apps, die SSO nicht unterstützen
- ☐ App-Lizenzierung und -Nutzung verstehen

Organisatorische Bereitschaft

- ☐ Die Leitung erkennt die Bedeutung von Lernzeit und Chancengleichheit für SSO
- ☐ Zustimmung der Beteiligten (IT-Admins, Verwaltungsangestellte & Lehrkräfte)
- ☐ Bereitschaft, vor dem Rollout einen Pilotversuch mit einer Testgruppe durchzuführen
- ☐ Ressourcen (Zeit und Budget) für die Umsetzung
- ☐ Schulungen für Lehrkräfte und Schüler

Basiskennzahlen

- ☐ Ermittlung, wie viel Unterrichtszeit durch Probleme beim Einloggen verloren geht
- ☐ Erfasste Tickets zur Passwortzurücksetzung und Leistungskennzahlen für den IT-Support
- ☐ Feedback von Lehrkräften zu aktuellen Problemen beim Zugang
- ☐ Ermittlung von Schülergruppen, die mit den meisten Problemen konfrontiert sind

Punktestand:

12–15 Kästchen angekreuzt:

Sie können SSO nun implementieren. Die Daten belegen einen eindeutigen ROI, und die technologische Grundlage ist bereits vorhanden.

8–11 Kästchen angekreuzt:

Sie haben es fast geschafft. Konzentrieren Sie sich darauf, die Lücken in Ihrer Identitätsinfrastruktur zu schließen, bevor Sie mit einem Pilotprogramm fortfahren.

4–7 Kästchen angekreuzt:

Sie müssen erst eine geeignete Grundlage schaffen. Beginnen Sie mit unserem Leitfaden „Identitäts- und Zugriffsverwaltung an Schulen für Einsteiger“, um sich mit den wesentlichen Komponenten vertraut zu machen, und kehren Sie anschließend zur SSO-Planung zurück.

0–3 Kästchen angekreuzt:

Fangen Sie mit den Grundlagen an. Richten Sie zunächst Ihre Identitätsinfrastruktur und den Apple School Manager ein, bevor Sie mit der SSO-Einführung beginnen.



Fazit

Schwierigkeiten beim Einloggen zehren unbemerkt an der Unterrichtszeit, verstärken Ungleichheiten beim Zugang und belasten die IT. Jede Verzögerung bremst den Lernfluss, schränkt das Engagement ein und vergrößert die Lernlücken in den unterschiedlichen Klassen.

Und das summiert sich. 30 Sekunden pro Anmeldung, multipliziert mit jeder Klasse, jedem Schüler und jedem Schultag – das sind Tausende von Stunden Lernzeit, die nie wieder zurückkommen.

Single Sign-On ist der Motor für den nahtlosen Zugang zu Lernangeboten – und dieser nahtlose Zugang verändert alles. Durch eine vereinfachte Authentifizierung, verbesserte Sicherheit und die Rückgewinnung von Unterrichtszeit in jeder Stunde verwandelt SSO den Zugriff von einem täglichen Problem in etwas, das Schüler und Lehrer gar nicht mehr wahrnehmen – weil es einfach funktioniert.

In solchen Fällen können sich die Lehrkräfte auf den Unterricht konzentrieren, anstatt Probleme zu beheben. Der Unterricht beginnt pünktlich. Die IT wechselt vom Reagieren zum aktiven Gestalten – für bessere Erlebnisse, schlankere Abläufe und Technologie, die optimal auf das Lernen abgestimmt ist.



Mit Jamf sorgt die IT für einen sicheren und skalierbaren Zugang, der es jedem Schüler ermöglicht, kontinuierlich zu lernen.

www.jamf.com/de/

© 2026 Jamf, LLC. Alle Rechte vorbehalten.

Entdecken Sie, wie ...