Untis Whitepaper

November 2022

In Schulen darf Datensicherheit kein Zufall sein!

Eine Hilfestellung für die Auswahl einer sicheren und nachhaltigen Software-Lösung für Schulen

In den letzten Jahren erlebte der Bildungsbereich einen massiven digitalen Schub. Die Vielzahl an Anbietern von Software für Schulverwaltung, Unterrichtsgestaltung, Stunden- und Vertretungsplanung sowie Lernplattformen ist unüberschaubar geworden. Viele Entscheider fragen sich, nach welchen Kriterien sie die "richtige" Software für ihre Bildungseinrichtung auswählen sollen. Natürlich zuerst danach, was die Software können muss. Als Zweites sollte dann vor allem auf die Themen Datenschutz, Datensicherheit und Zertifizierungen geachtet werden, da Schulen mit sensiblen Personendaten arbeiten und verpflichtet sind, damit verantwortungsvoll umzugehen.

Warum sollten sich Schulen für eine Schul-Software entscheiden, die Wert auf die Sicherheit ihrer Kundendaten legt?

Michaela Escuyer, Geschäftsführerin der Untis Bayern GmbH, arbeitet seit über 30 Jahren in der IT-Branche, davon 20 Jahre im Markt für Bildungssoftware und kommt ursprünglich aus dem Bereich der Erwachsenenbildung. Sie und ihr Team betreuen aktuell 1.500 Schulen in Bayern und können die verstärkten Nachfragen zum Thema Datensicherheit aus Gesprächen mit Kund*innen bestätigen: "Sehr häufig wird gefragt, ob unsere Softwarelösung datenschutzkonform ist und ob die Server in Deutschland bzw. der EU stehen. Oftmals sind die Schulen schon mit einem einfachen 'Ja, sind wir.' zufrieden, obwohl hier ein genauer Blick hinter die Kulissen sinnvoll wäre." Es gibt zwar eindeutige Gesetze und Vorschriften der EU und der Länder, aber die Umsetzung in den Unternehmen ist oft sehr unterschiedlich. "Dennoch machen genau diese Kleinigkeiten am Ende den Unterschied", erklärt Michaela Escuyer. "Sich das Label 'datenschutzkonform' auf's Produkt zu kleben und die Daten in zertifizierten Rechenzentren in der EU zu hosten, sagt noch nichts über die Qualität und Sicherheit der Software aus."
Ein verantwortungsvoller Software-Anbieter beschäftigt eigene Mitarbeiter*innen (Datenschutzbeauftragte), die auf datenschutzkonforme Arbeitsweisen und Prozesse im Unternehmen achten. Außerdem sollte man als Käufer*in darauf achten, dass nicht nur das Produkt, sondern auch das Unternehmen selbst ISO27001 zertifiziert ist. Nur dann wird von unabhängigen Auditor*innen nachweislich ein verantwortungsvoller Umgang mit Unternehmens- und Kundendaten bescheinigt.
"Und genau aus diesen Gründen hat sich kürzlich ein kleiner Bildungsträger für WebUntis entschieden, nachdem er verschiedene Lösungen am Markt evaluiert hat. Sein Fazit lautete: 'Untis ist mehr als nur eine schöne Verpackung mit Schleife dran. Mit jahrzehntelanger Erfahrung im sicheren Umgang mit persönlichen Daten und regelmäßigem Austausch mit Datenschutzbeauftragen der Behörden ist Untis ein verlässlicher Partner für alle Bildungseinrichtungen.'"

Woran erkennt man ein sicheres Produkt und was ist heutzutage Standard?

“Zugegebenermaßen ist es nicht immer einfach auf den ersten Blick zu erkennen, ob ein Produkt oder ein Dienst sicher oder datenschutzkonform ist. Doch es gibt ein paar Indikatoren, die sich auch von außen gut überprüfen lassen”, erklärt Jürgen Pointinger, der neue Head of Technology der Untis GmbH.

1. Strenge Einhaltung der DSGVO
Alle am Schulalltag beteiligten Personen - Administrator*innen, Lehrkräfte, Schulleitung, Erziehungsberechtigte und Schüler*innen einer Bildungseinrichtung – haben natürlich das Recht auf den Schutz ihrer personenbezogenen Daten. Bei der Verwendung einer Schulsoftware werden diese Nutzerdaten von der Schuladministration an den Software-Hersteller übermittelt und dort gespeichert. Für diese Verarbeitung der Daten schreibt Artikel 28 der EU-Datenschutz-Grundverordnung vor, dass eine vertragliche Vereinbarung zwischen Schule und Hersteller getroffen werden muss. “Sollten Sie von einem Software-Anbieter keinen Auftragsverarbeitungsvertrag vorgelegt bekommen, sollten Sie stutzig werden”, warnt Jürgen Pointinger, der seit über 20 Jahren im IT-Bereich tätig ist.

2. Datenschutz ist nicht gleich Datensicherheit
Während es sich beim Begriff Datenschutz um den rechtlichen Schutz personenbezogener Daten und somit der Privatsphäre von Menschen dreht, geht es beim Begriff der Datensicherheit darum, mit technischen Maßnahmen die Manipulation, den Verlust oder den Zugriff Unbefugter auf Daten zu verhindern. Das Motto seriöser Software-Anbieter sollte lauten: ‘So viele anonymisierte Daten wie nötig, besser aber so wenig wie möglich’. Denn wo viele Daten gespeichert werden, können auch viele Daten verloren gehen oder gestohlen werden. “Nach diesem Prinzip funktioniert z.B. der Messenger von Untis, für den kein Austausch von privaten Daten wie Handynummern oder E-Mail-Adressen von Schüler*innen oder Lehrkräften notwendig ist.“

3. Serverstandorte in der Europäischen Union
Nach der Frage ”Welche Daten werden gespeichert?” sollte man sich sofort fragen “Wo werden die Daten gespeichert?”. Und heutzutage sollte man nicht nur darauf achten, in welchem Land die eigenen Daten landen, sondern auch welches Unternehmen dahintersteckt und ob ein Zugriffsrisiko auf diese Daten besteht. In mehreren Urteilen, u.a. auch vom Europäischen Gerichtshofs (EuGH), wurde das US-amerikanische Datenschutzniveau als nicht ausreichend eingeschätzt. Um auf Nummer sicher zu gehen, sollte man auf heimische, sprich europäische Hochleistungsserver z.B. in Deutschland oder Ö-Cloud-Dienste in Österreich setzen.

4. Regelmäßige ISO-27001-Zertifizierungen
Die ISO-27001-Zertifizierung ist der bekannteste, internationale Standard im Bereich der IT- und Informationssicherheit. Die Norm beschreibt wie ein Informationssicherheits-Managementsystem (ISMS) aufgebaut und betrieben wird, und definiert, was ein Unternehmen tun muss, um Risiken durch Datenmissbrauch, Hackerangriffe und Datenverlust zu minimieren. Ein verantwortungsvolles Software-Unternehmen wie die Untis GmbH lässt sich jährlich von unabhängigen Auditor*innen überprüfen und alle 3 Jahre rezertifizieren. Dieses enorme Engagement des Unternehmens, in puncto Daten- und Informationssicherheit immer am aktuellen Stand zu bleiben, zeugt von großem Verantwortungsbewusstsein für die Sicherheit der Kundendaten. Es ist also vor allem darauf zu achten, ob das Unternehmen an sich zertifiziert wurde und nicht nur Dienste oder beauftragte Partner, die jenes Unternehmen einbezieht.

5. Sichere Passwörter und Multifaktor-Authentifizierung
Wie bereits erwähnt sind personenbezogene Daten einem ständigem Missbrauchsrisiko von Unbefugten ausgesetzt. Um dem vorzubeugen, sollte man darauf achten, für verschiedene Dienste unterschiedliche Passwörter zu verwenden. Diese sollten sicher in einem Passwort-Tresor verwahrt werden und keine persönlichen Informationen enthalten, die man erraten oder durch soziale Manipulation herausfinden könnte, wenn man Sie näher kennt. "Am sichersten ist es, wenn der Software-Anbieter ein starkes Passwort verlangt, das mindestens 8, besser aber 10 Merkmale aufweist. Das Passwort sollte keine Muster und keine verbreiteten Wörterbucheinträge enthalten. Es sollte sich aus einer Mischung von Buchstaben, Zahlen, Sonderzeichen und einer Groß- und Kleinschreibung ergeben", sagt Jürgen Pointinger. "Auch Zwei- oder Multifaktor-Authentifizierung bietet einen erhöhten Schutz, da man hier neben Benutzername und Passwort noch eine zweite Information bestätigen muss. Das können z.B. Textnachrichten, Anrufe, Biometrie und einmalige Passcodes aus einer separaten App sein."

Untis Top 3 Tipps für die Auswahl einer sicheren und nachhaltigen Software-Lösung für Schulen

1. **Nicht von der Optik täuschen lassen**
   Auch wenn die Software auf den ersten Blick großartig aussieht und alle Funktionalitäten verspricht, die man sich wünschen kann. Testen Sie das Tool vorher ausgiebig und fragen Sie beim Hersteller konkret nach, ob das Tool alle Vorschriften Ihres (Bundes)Landes erfüllt.

2. **Qualität vor Quantität**
   Die User können sich neue Features wünschen, die bereits im nächsten Update enthalten sind? Davon lassen Sie sich besser nicht beeindrucken. Eine schnelle Umsetzung von neuen Funktionen zeugt eher davon, dass die Produktentwicklung nicht besonders stark reguliert ist und wenig Überprüfungsschritte im Prozess vorhanden sind.

3. **Wir sind jung und brauchen das Geld**
   In den letzten Jahren sind viele Start-ups mit guten Ideen am EdTech Markt erschienen, die Themen wie Datenschutz und Datensicherheit nicht von Anfang an mitbedenken. Sie verschwinden oftmals nach wenigen Jahren, weil ihnen entweder das Geld ausgeht oder sie von anderen Firmen geschluckt werden. Schulen brauchen aber einen verlässlichen Partner, der sie über viele Jahre begleitet und mit ergänzenden Dienstleistungen wie Support, Beratung, Schulung etc. versorgt. Untis steht seit über 50 Jahren an der Seite von Schulen und setzt auf eine vertrauensvolle Zusammenarbeit auf dem Weg in eine digitale Zukunft.

Weitere Informationen zur Datensicherheit bei Untis: https://www.untis.at/datensicherheit

Über Untis
Wir haben den (Stunden) Plan.

Wir bei Untis sorgen seit über 50 Jahren für einen reibungslosen Schulablauf. Um diese Mission zu erreichen, legen wir großen Wert auf Informationssicherheit und Datenschutz. Jährliche Überprüfungs-Audits und wiederholte ISO-27001-Zertifizierungen, stabile Serverstandorte in Deutschland und Österreich sowie ein lückenloser Datenschutz sind für uns selbstverständlich, damit unsere Kund*innen darauf vertrauen können, dass ihre Daten bestmöglich geschützt sind.