Sicherheitsaspekte von E-Learning

Edgar R. Weippl

Technische Universität Wien, Institut für Softwaretechnik und Interaktive Systeme
Favoritenstraße 9-11/188, 1040 Wien
weippl@ifs.tuwien.ac.at

Schlagworte: Sicherheit, Verlässlichkeit, E-Learning

Abstract: Sicherheitsaspekte von E-Learning-Systemen werden zunehmend wichtiger, weil immer größere Installationen auf Universitäten gemacht werden und der Lehr- und Lernbetrieb auf diese Infrastruktur mehr und mehr angewiesen ist.

1. Einleitung

Das Thema IT-Sicherheit wurde während der letzten Jahre zunehmend auch in populärwissenschaftlichen Medien behandelt. Die wichtigsten Grundlagen wurden im wissenschaftlichen Bereich in den 60er und 70er Jahren in den USA durch starke Förderung im militärischen Bereich gelegt. Mittlerweile gibt es eine große Anzahl an neuen Journals und Konferenzen, die IT-Sicherheit auch außerhalb militärischer Anwendungen behandeln.

Auch für Personen, die E-Learning-Content erzeugen, gewinnt das Thema Sicherheit zunehmend an Bedeutung, wobei sich hier zunächst einige grundsätzliche Fragen stellen: Berührt mich Sicherheit, obwohl das Lehrmaterial nicht geheim ist? In den klassischen militärischen Anwendungen ist „Geheimhaltung“ eine der Hauptanforderungen an Sicherheit. Auch wenn Geheimhaltung in der Lehre nicht oberste Priorität hat, so sind andere Sicherheitsaspekte (zB Datenintegrität und Verfügbarkeit) und Aspekte der Verlässlichkeit (Wartbarkeit, etc) essentiell.

Sicherheit für E-Learning ist nicht nur für Institutionen, die sich mit Fernlehre beschäftigen, relevant. Selbst bei klassischer Präsenzlehre an Universitäten und Fachhochschulen werden neue Medien meist als Ergänzung und Bereicherung des Unterrichts verwendet. In diesem Zusammenhang stellen sich trotz der Unterschiede im Lehrmodus sehr ähnliche Fragen in Bezug auf Sicherheit.

Da E-Learning-Plattformen einzelner Universitätsinstitute nun zunehmend integriert werden und fakultäts- oder universitätsweit

verwendet werden, gewinnt Systemsicherheit zusätzlich an Bedeutung.

2. Autoren

Für Autoren, die E-Learning-Content erstellen, sind meist folgende Anforderungen wichtig:

- Leser müssen vertrauen können, dass der Inhalt richtig ist
- Leser wollen unbeobachtet lesen
- Schutz vor unberechtigter Nutzung
- Schutz vor unberechtigter Veränderung und Verwendung
- Schutz vor Zerstörung und Datenverlust

3. Lehrende

Grundsätzliche Anforderungen an sichere Systeme sind Vertraulichkeit (secrecy), Integrität (integrity), Verfügbarkeit (availability) und Nachweisbarkeit (non repudiation).

Sicherheit in der Lehre darf sich nicht nur auf das IT-technische System beschränken. Es ist notwendig, das gesamte Umfeld, dh auch die organisatorische Abwicklung der Lehre und der Prüfungen, mit einzubeziehen. In diesem Abschnitt werden diese Kriterien für drei grundlegende Bereiche der Lehre beleuchtet.

- Vertraulichkeit von Kommunikation
- An- und Abmeldungen bei Lehrveranstaltungen
- Prüfungen

3.1. Vertraulichkeit von Kommunikation

Die Speicherung von Diskussionsbeiträgen in Foren, Annotationen in einem E-Learning-System und persönliche E-mails stellen ein Risiko für die Privacy von Lehrenden und Lernenden dar. Selbst wenn die Daten aus der E-Learning-Plattform gelöscht werden, existieren von den Daten üblicherweise Backups. In vielen Unternehmen werden monatliche oder jährliche Backups aufbewahrt, sodass auch Jahre später noch ein Zugriff auf die Daten möglich ist. Selbst wenn während der Lehrveranstaltung Studierende keinerlei Bedenken haben, ihre Meinung in dem Forum zu äußern, so könnten – nach einer Änderung der politischen Situation – kritische Äußerungen Jahre danach außerhalb des Kontexts der Lehrveranstaltung gesehen werden und Nachteile für ehemalige Studenten haben.

Selbst in stabilen Demokratien kann die jahrelange Speicherung von Daten einer E-Learning-Plattform als Sicherheitsrisiko empfunden werden. So können Universitäten und Unternehmen verpflichtet sein, auf Gerichtsbeschluss Daten von Backups wiederherzustellen und nach den gewünschten Informationen zu suchen, gleichgültig wie hoch die Kosten dafür sind.

3.2. An- und Abmeldungen bei Lehrveranstaltungen

Die An- und Abmeldung zu Lehrveranstaltungen ist eine von vielen administrativen Tätigkeiten an Universitäten. Bei kleinen Universitäten kann die Anmeldungen persönlich bei den Leitern einer Lehrveranstaltung durchgeführt werden. Die Risken sind im Allgemeinen eher klein, weil die Studierenden leicht überblickbar und bei Präsenzlehrveranstaltungen dem Lehrenden sogar persönlich bekannt sind.

Bei sehr großen Lehrveranstaltungen und in der Fernlehre wird dies meist über eine Anmeldefunktion eines E-Learning-System abgewickelt. Anonymität ist hier ein Risikofaktor. Wenn mit der Anmeldung Pflichten und bei Nichterfüllung Konsequenzen (negative Beurteilung, Kursgebühren etc) verbunden sind, so muss sichergestellt werden, dass die Anmeldung bewusst vorgenommen wurde und die Identität des Studierenden während der Anmeldung überprüft wurde. Eine weitere Anforderung ist, dass die Abmeldung von Lehrveranstaltungen von nicht-autorisierten Personen nicht möglich ist. Andernfalls ist es für unkollegiale Studenten sehr leicht, sich bei ausgebuchten Lehrveranstaltungen einen Platz zu beschaffen, in dem sie Kollegen ohne deren Wissen einfach abmelden.

3.3. Prüfungen

3.3.1. Übermittlung von Prüfungsnoten

Sicherheitsaspekte sind bei Prüfungen besonders relevant. Ein Angriffspunkt ist die Übermittlung und Speicherung von Prüfungsnoten und Zeugnissen. Die *Vertraulichkeit* der Daten ist gefährdet, wenn Lehrende die Daten unverschlüsselt via E-Mail übermitteln. Ebenso sind die *Integrität der Noten*, dh die Unverfälschtheit, und die *Authentizität des Absenders* wesentliche Anforderungen. Es ist allgemein bekannt, dass sich E-Mail-Absender sehr leicht fälschen lassen. Wenn nun das Sekretariat von einem Lehrveranstaltungsleiter

eine E-Mail bekommt, welche ein Notenkorrektur bei einem Studenten beinhaltet, so können sowohl der Absender dieser E-Mail als auch der Inhalt gefälscht sein.

Abgesehen von traditionellen Prüfungen, bei denen lediglich die Speicherung und Übermittlung von Noten besonders geschützt werden muss, werden zunehmend automatisch generierte Prüfungen verwendet.

Hier muss man schon vor Prüfungsbeginn sicherstellen, dass weder die Fragen bei der Übermittlung zu den Studierenden noch deren Antworten verändert werden.

Bei Prüfungen ist die spätere *Nachvollziehbarkeit* (non repudiation) von zentraler Bedeutung. Das heißt, dass die Fragen, die jeweils dazugehörigen richtigen Antworten, und die vom Studierenden gegebenen Antworten gespeichert werden müssen, sodass spätere Manipulation ausgeschlossen werden kann. Da falsche Auswertungen von Prüfungen sich leider nicht ganz vermeiden lassen, muss es eine Möglichkeit geben, Ergebnisse zu ändern. Es muss daher eine zuverlässige Möglichkeit geben, die Prüfung im Zweifelsfall händisch zu kontrollieren und zu bewerten. Sämtliche Änderungen an elektronischen Daten müssen klar erkennbar sein. Organisatorisch lässt sich dies über Ausdrucke auf Papier und rein technisch mit digitalen Signaturen lösen.

Bei Massenprüfungen ist *Verfügbarkeit* essentiell. Abgesehen von unbeabsichtigten Ausfällen darf man die Motivation Studierender nicht unterschätzen, Prüfungssysteme lahm zu legen, wenn sie dadurch eine negative Bewertung ihrer Prüfung verhindern können.

4. Ausblick

Durch eine Kombination von organisatorischen und technischen Maßnahmen lässt sich die Sicherheit und Zuverlässigkeit beim Einsatz von E-Learning verbessern. Zusätzliche Informationen finden interessierte Leser im Buch „Security in E-Learning“ von *Edgar R. Weippl*, auf http://www.e-learning-security.org und im Modul 9 der Lernplattform http://www.planet-et.at.