Vertraulichkeit persönlicher Daten in Lern-Management-Systemen

Christian J. Eibl
Lehrstuhl Didaktik der Informatik und E-Learning
Universität Siegen
eibl@die.informatik.uni-siegen.de

Abstract: Vertraulichkeit persönlicher Daten lässt sich aufteilen in Datensparsamkeit bei der Erhebung und dem Schutz der Daten im System. Dieser Artikel beschäftigt sich daher zuerst mit der Frage, welche Daten für die Lehre mit E-Learning-Systemen sinnvoll sind mit Blick auf die Zielgruppe. Anschließend werden Anforderungen für einen angemessenen Umgang mit diesen Daten diskutiert. Eine Untersuchung von Lern-Management-Systemen bzgl. Datenerhebung und potentieller Probleme schließt die Arbeit ab. Exemplarisch wird dabei eine Auswahl von Fehlern im Design diskutiert.

1 Motivation

Die Erhebung von Daten und die damit verbundene Pflicht zur Wahrung der Vertraulichkeit ergibt sich im Bildungskontext vor allem bei Bewertungen von Lernfortschritten und Leistungen. Dies lässt sich am Beispiel von Schulen illustrieren: In klassischem Präsenzunterricht an Schulen sollen mündliche Leistungen, d.h. kontinuierliche Beteiligung und Darstellung von Lernerfolgen, sowie weiche Kriterien wie Arbeitsmoral und Teamfähigkeit (vgl. „Kopfnoten“) ebenso bewertet werden wie Leistungen in schriftlichen Prüfungen, d.h. punktuelle Lernerfolgskontrolle. Solch kontinuierliche Leistungen sind jedoch aufgrund hoher Teilnehmerzahlen und eingeschränkter Möglichkeiten der Lehrperson trotz des persönlichen Kontaktes und der damit verbundenen Nähe oft nur sehr schwer zu beurteilen. In der Regel fließt ein überwiegend subjektiver Eindruck, den ein Schüler beim Lehrer hinterlässt, in die Bewertung ein. Ein Übertragen dieser Punkte auf E-Learning führt daher verständlicherweise oft zu dem Wunsch objektiver Aktivitätsaufzeichnungen und statistischer Auswertungen, die die Beteiligung während des Lernprozesses und deren Qualität widerspiegelt. Bei Verwendung von Lern-Management-Systemen (LMS) ergibt sich der Vorteil, dass diese Systeme bereits in der Grundkonfiguration solche Erhebungen anbieten. Über das Verfolgen von Aktivitäten kann ein Lehrender feststellen, ob alle Lernenden bereitgestellte, relevante Materialien geladen und sich damit über entsprechende Thematiken informiert haben. Es stellen sich jedoch die Fragen:

- Welche Daten sind wirklich notwendig, um den Lernprozess zu unterstützen, und welche schießen über das Ziel hinaus?
- Wer darf auf diese Daten zugreifen? Hat ein Zugriff auf diese Daten möglicherweise nicht gerechtfertigte, negative Folgen für Lernende?

Die Datensammlung und die Erhebung personenbezogener Daten zum Zwecke der besseren Personalisierung und Sozialisierung unter den Lernenden ist nicht unproblematisch. Es gibt hitzige Diskussionen zu den Themen des Datenschutzes und der Vertraulichkeit solch persönlicher Daten wie Lernfortschritt und Lernerfolg[1]. Fakt ist, dass Lehrende nur dann rechtzeitig und zielgerichtet in den Lernprozess eingreifen können, wenn sie mit ausreichend Daten versorgt werden. Gerade diese Häufung von Daten könnte jedoch unangenehm für Lernende sein und sogar zu Nachteilen führen, wenn z.B. geringe (erfasste) Beteiligung und offensichtlich zu kurzfristige Beschäftigung mit einem Thema vor einer Prüfung von Lehrenden für die Notengebung negativ bewertet wird. Dass sich ein Lehrender im Präsenzunterricht notiert, welcher Schüler wann gefehlt hat und wer sich wann auf welche Weise auch immer am Unterricht beteiligt hat, ist grundverschieden von einem Informatiksystem, das alle Aktivitäten von Benutzern objektiv protokolliert. Weiterhin existieren oftmals keine Alternativen zu dem E-Learning-System, so dass ein Nutzungszwang die Situation einer exzessiven Datenerhebung verschärft.
Die vorab angesprochene Subjektivität und damit verbunden auch die Vergesslichkeit einer Lehrperson entschärfen den Datenschutz-Aspekt in Präsenzlehre erheblich im Vergleich zu nicht vergesslichen Informatiksystemen. Speziell bei Übertragung des Präsenzbeispiels auf Hochschulen, bei denen die Dozierenden in der Regel nicht alle Studierenden namentlich kennen, und so deren Arbeitsmoral nicht z.B. in Klausurbewertungen einfließen kann, entsteht hier eine andere Situation – die der Anonymität gegenüber den Lehrenden.
Der vorliegende Artikel beschäftigt sich mit der Frage der Sinnhaftigkeit von Datenerhebung im E-Learning und einer angemessenen Zugriffskontrolle zur Sicherstellung der Vertraulichkeit. Ausgewählte, konzeptuelle Probleme in verbreiteten LMS werden diskutiert.

2 Stand der Forschung

Gudjons führt drei „Einsichten“ als „Ergebnisse der empirischen Unterrichtsforschung“ wie folgt auf [5, S. 251ff]:

1. „Jeder braucht seine eigenen Lernwege“
2. „Der Weg zur Autonomie führt über die Anleitung“
3. „Die Lernmethoden müssen den Schülerfähigkeiten angepasst werden“

Jeder dieser Punkte erfordert eine Form der Rückmeldung an Lehrende, um diesen geeignete Reaktionen auf Ereignisse zu ermöglichen. Übertragen auf E-Learning stellt sich die Situation grob in zwei Ebenen dar: interne Vorgänge im Lernenden selbst und externe Vorgänge in Form von Interaktion mit dem System. Kognitive Fortschritte und Prozesse des Lernenden ohne Interaktion mit dem System werden nicht aufgezeichnet und an Lehrende als Rückkopplung übertragen. Diese Vorgänge im Lernenden selbst können also nicht ohne weiteres nachvollzogen werden von Lehrenden. Aktivität im System auf der

[1] vgl. Datenschutz-Forum zu Moodle: `http://moodle.org/mod/forum/view.php?id=2662`

anderen Seite, d.h. Ereignisse wie Fortschritte im Lernmaterial, Zugriffe oder Nutzungsintensität können ohne Verluste und subjektive Filterung im System abgelegt und für spätere Analysen aufbereitet werden. Diese Aufzeichnungen eines Lernprozesses spiegeln Aktivitäten, jedoch nur in begrenztem Maße kognitive Fortschritte wider. Ihre Auswertung kann folglich sehr einfach zu negativen Konsequenzen für Lernende führen bei Missinterpretation durch Lehrende. Betrachtet man Schulmeister, so stellen Werkzeuge zur Aufzeichnung und statistischen Erhebung von Aktivitäten (vgl. „1.1.1. Logging (Aktionen der Benutzer werden gespeichert)“ in [13, S. 58, Tab. 15]), ebenso wie eine „Anwesenheitsstatistik“ [13, S. 63, Tab. 15] K.O.-Kriterien für Lern-Management-Systeme dar.
Dass eine derartige, statistische Erhebung ohne den Spielraum der „menschlichen Vergesslichkeit“ und Subjektivität nicht allen Lernenden passen dürfte, ist offensichtlich (vgl. [8]). Vor allem die zweite „Einsicht“ nach Gudjons ist hierfür ausschlaggebend. Es wird betont, dass Autonomie beim Lernen zu vermitteln ein hohes Ziel von Lehrenden sein sollte. Folglich wäre es fatal, wenn unabhängig von geistiger Entwicklung und psychologischer Reife derselbe Grad von Überwachung und Eingriff in den Lernprozess erfolgen würde. Eine Anpassung an die Zielgruppe ist unumgänglich. Nach Knowles et al. [8] entwickelt sich in Heranwachsenden ein immer stärkerer Drang nach Unabhängigkeit und Einflussnahme in Dinge, die einen selbst betreffen – folglich auch im Lernprozess. Die Akzeptanz externer Überwachung und Eingriffe schwindet, der Wunsch nach eigenen Kontakten und der Möglichkeit, selbstbestimmt Fragen zu stellen, steigt. Erwachsene müssen zuerst verstehen, dass ein bestimmtes Thema für sie relevant ist, damit sie es bereitwillig lernen und im Fall von Problemen auch auf Hilfe zurückgreifen. Eine externe Kontrolle wird hierbei häufig missinterpretiert als mangelndes Vertrauen in ihre eigene Entscheidungsfähigkeit und führt daher eher zur Ablehnung der Hilfestellung bis hin zu einer Verweigerung des Lerninhaltes. Rogers spricht hierbei von „Schaffung einer Atmosphäre des Akzeptierens“ [12, S. 341], bei der diese psychologischen Entwicklungen und neuen Forderungen entscheidenden Einfluss haben auf die Akzeptanz von Lernumgebungen und Lehrpersonen selbst. Weippl vergleicht in diesem Zusammenhang E-Learning mit einem Buch, das man ungestört zu Hause lesen möchte, mit der Erkenntnis „readers want to read unobserved“ [15, S. 15].
Zu erwähnen ist in diesem Zusammenhang jedoch der Zeitgeist, der sich gerade in der neuen Offenheit im sog. „Web 2.0“ zeigt. Viele junge Erwachsene zeigen wenig Scheu bei der Veröffentlichung privater Meinungen und Daten im Internet, obwohl sie es in anderen Bereichen evtl. nicht veröffentlichen würden. Ein Artikel in USA-today befasste sich mit dieser Thematik unter dem Titel „Online privacy? For young people, that's old-school“ [9]. Inwiefern sich das jedoch als zeitgeschichtlicher Wandel in den Ansichten oder doch eher als leichtsinnige Freizügigkeit mit späterer Reue herausstellt, bleibt zu klären.
Für E-Learning bleibt festzustellen, dass aufgrund der unterschiedlichen Forderungen von Zielgruppen E-Learning-Systeme flexibel konfigurierbar sein müssen, um allen Anforderungen zu genügen. Anpassbarkeit und eigene Einflussnahme können hierbei sehr motivierende Faktoren sein. Da der Autor keinerlei juristische Ausbildung besitzt, wird die rechtliche Seite im Folgenden nur sehr marginal behandelt und stattdessen auf Dokumente wie [6] verwiesen. Es sei jedoch erwähnt, dass das deutsche Bundesdatenschutzgesetz (BDSG) eine klare Zweckbindung für erhobene Daten verlangt und in §3a explizit zur „Datenvermeidung und Datensparsamkeit“ mahnt:

„Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."

3 Anforderungen für Vertraulichkeit

Technisch gesehen sind durch mächtige Zugriffskontrollmechanismen und moderne Kryptographie nahezu alle Probleme für Vertraulichkeit lösbar. Es sind jedoch meist organisatorische Dinge, die zu realen Problemen führen (vgl. Abschnitt 4.2), beispielsweise weil gewisse Aspekte im Design der Software nicht berücksichtigt wurden. Speziell hierfür stellen sich Anforderungen, die zu den folgenden Punkten zusammengefasst werden:

1. *Authentifikation und Benutzeraccounts*
   Es ist darauf zu achten, dass der Authentifikationsprozess sicher und zuverlässig abläuft. Da aufgrund hoher Kosten von fortgeschritteneren Systemen meist auf passwortbasierte Systeme zurückgegriffen wird, sollte zumindest auf eine verschlüsselte Datenübertragung höchster Wert gelegt werden. Benutzeraccounts sind hierbei eindeutig einer realen Person zuzuordnen. Sammelaccounts für Gruppen von Lernenden und Möglichkeiten der Verwendung von Fremdaccounts, z.B. für Lehrende, erhöhen die Komplexität von Zugriffskontrollen immens und erlauben ggf. ein Unterwandern von Schutzmechanismen.

2. *Globale und lokale Rollen*
   In LMS haben sich rollenbasierte Zugriffsmechanismen als sinnvoll erwiesen, da sich über diese Verfahren feine Abstimmungen und kursabhängige Zugriffsmöglichkeiten ergeben. Die meisten modernen LMS unterscheiden hierbei globale und lokale Rollen. Während jeder Benutzer des Systems einer globalen Rollen zugeordnet ist, z.B. Administrator, Dozent oder Student, kann sich die Zuweisung in der lokalen Rolle davon unterscheiden. Es ist auf diesem Wege möglich, global als Lernende definierte Nutzer in einem bestimmten Kurs anderen Lernenden im Sinne eines Tutors zu überstellen. Je feiner sich Rollen aufgliedern lassen, desto präziser können die Zugriffskontrollen greifen und entsprechend Daten geschützt werden. Rollen besitzen in der Regel durch ihre zugeordneten Rechte eine implizite hierarchische Ordnung untereinander. Diese ist zu berücksichtigen bei Rollenwechseln innerhalb des Systems.

3. *Klare Trennung der Zuständigkeiten*
   Im Zusammenhang mit Rollen ist darauf zu achten, dass im System eine klare Trennung der Zuständigkeiten vorgesehen ist. Ein Lehrender zum Beispiel sollte lediglich für die Verwaltung eines Kurses mit ausreichend Rechten ausgestattet werden. Die Verwaltung von Personen, also auch Lernenden in dem Kurs des genannten

Lehrenden, ist den Administratoren vorbehalten. Hier kommt vor allem das Problem zum Tragen, dass es eine hierarchische Ordnung zwischen den verschiedenen Rollen gibt, die es einem Lehrenden erlauben könnte, ohne Berechtigung an die Daten von „untergebenen“ Lernenden zu gelangen. Obwohl diese Anforderung für kleine Einrichtungen relativiert werden kann, sollte das Konzept des Systems im Sinne der Skalierbarkeit diesen Punkt berücksichtigen.

4. *Integriertes Nachrichtensystem*
   Kontaktdaten sind wertvoll u.a. für Versender von Werbemails und Callcentern. Trotz der Notwendigkeit der Erfassung dieser Daten für Verwaltungszwecke muss die Vertraulichkeit gewahrt bleiben. Ein LMS sollte daher die Möglichkeit bieten, eine Auswahl von Personen direkt über das System zu kontaktieren statt freizügig solcherlei Daten für verschiedene Rollen preiszugeben.

5. *Pseudonymisierung und Anonymisierung*
   Viele Daten, vor allem statistische Erhebungen, kommen auch ohne direkten Personenbezug aus, ohne an Wert zu verlieren. Es sollte versucht werden, Daten nur anonymisiert abzulegen, oder, falls nicht anders möglich, nur anonymisiert bzw. pseudonymisiert wieder an bestimmte Personen auszugeben. Beispielsweise macht es Sinn, Daten zum Zugriff auf bestimmte, kritische Teile des Systems, sowie den Aktivitäten dort, mit Personenbezug aufzuzeichnen, um ggf. Fehlverhalten verfolgen zu können. Eine Ausgabe an Lehrende hingegen in Form einer Statistik über diese Zugriffe kann ohne weiteres anonymisiert erfolgen.

6. *Zeitliche Begrenzung der Speicherung*
   Da viele Statistiken lediglich der Bestimmung dienen, zu sehen, wie gut frequentiert bestimmte Kurse sind, ist nach Beendigung eines Kurses diese Datensammlung sinnlos und kann aus dem System entfernt werden. Ebenso ist bei Inhalten asynchroner Kommunikation zu verfahren, um später zeitlich bereits überholte Aussagen nicht mehr gegen die Kommunikationsteilnehmer verwenden zu können. Daten mit längerer Aufbewahrungsfrist, z.B. Inhalte bewertungsrelevanter Sendungen, sollten losgelöst vom System archiviert und ebenfalls aus dem LMS gelöscht werden.

7. *Transparenz*
   Dieser Punkt ist in Bezug auf die Akzeptanz von Nutzern vermutlich mit Abstand der wichtigste. Viele Teilnehmer akzeptieren Funktionen zur Aufzeichnung, sofern sie darüber informiert wurden und es nicht heimlich geschieht. Hierbei wird Transparenz im Sinne der Aufklärung und Information über die Art und Weise, sowie den Umfang von Datenerhebung verwendet. Prinzipiell sollte der Grundsatz der Datensparsamkeit eingehalten werden, um selbst bei verwundbaren Systemen (vgl. [1, 4]) die Fülle an Offenlegung zu minimieren. Aus rechtlicher Sicht hat die Transparenz der Datenerhebung die Bewandtnis, dass Nutzer der Speicherung bestimmter Daten explizit zustimmen müssen.

4 Betrachtung von LMS

Die folgenden Betrachtungen von Lern-Management-Systemen werden sich überwiegend auf die beiden Open-Source-Systeme Moodle[2] (in Version 1.8) und Ilias[3] (in Version 3.8.3) in der Grundkonfiguration ohne spezielle, weitere Sicherheitseinstellungen beziehen. Diese beiden Systeme sind in einer vergleichenden Studie [10] als Empfehlungen hervorgegangen und werden zunehmend an deutschen Hochschulen, sowie anderen, nationalen und internationalen Bildungseinrichtungen eingesetzt. Beide Systeme sind alltagstauglich und verfügen über ausreichend Funktionen, um E-Learning anzubieten. Die Betrachtung dieser beiden Systeme in Bezug auf Vertraulichkeit soll daher keinerlei Minderschätzung im Vergleich zu anderen verfügbaren Systemen darstellen – im Gegenteil.

4.1 Datenerhebung

Prinzipiell ist bei der Datenerhebung im Sinne der Transparenzforderung (siehe Anforderung 7) zwischen wissentlicher Datenerhebung, z.B. Benutzerdaten, und unwissentlicher, z.B. Log-Daten, zu unterscheiden. Es ist zu beachten, dass es sich bei den meisten E-Learning-Systemen um webbasierte Systeme handelt, die folglich von Drittsystemen wie Webservern, Datenbankservern und natürlich dem Betriebssystem des Servers abhängen. In all diesen beteiligten und angebundenen Systemen werden in der Regel eigenständig Daten erhoben und langfristig gespeichert. Ein Zusammenschluss dieser Log-Daten kann ausführliche Informationen zu den Vorgängen innerhalb des E-Learning-Systems liefern. Dies führt zu der Forderung nach einem vertrauenswürdigen Administrator, der diese Daten nicht unbefugt zusammenführt und Diskretion walten lässt. Es muss hierbei sichergestellt sein, dass solche Daten nicht für andere Personen lesbar sind. Dies ist ein organisatorisches sowie technisches Problem, das unabhängig vom LMS zu lösen ist und damit außerhalb des Fokus' dieses Artikels liegt.
Die für Benutzer wissentliche Speicherung und Erhebung von Daten betrifft vor allem das Benutzerprofil mit allen persönlichen Angaben je nach Forderung des Systems und der Verwaltung hinter dem System. An der Universität des Autors wird hierbei explizit darauf geachtet, dass keine Pseudonymisierung bei Profileinträgen (vgl. Anforderung 5) gemacht wird von Seiten der Studierenden, damit Lehrende und andere Kursteilnehmer über den Realnamen leichter Kontakt herstellen können. Im Falle einer Pseudonymisierung durch Studierende, d.h. entgegen dieser Anweisung, würde der Account als letzte Konsequenz gelöscht, was den Lernenden aus dem System ausschließen würde. Diese Richtlinie hat jedoch rein organisatorische Gründe in Hinblick auf vereinfachte Kontaktbildung. Pseudonymisierung bzw. Anonymisierung im Profil ist für das Rechenzentrum meist ohne Bewandtnis, da von dort Zugangskennungen verteilt werden und im Fall der genannten Universität eine Authentifikation mit Hilfe eines zentralen Servers erfolgt, auf dem alle Kennungen (namentlich) verwaltet werden. Eine Identifikation von Benutzern ist damit aus sicherheitstechnischer Sicht jederzeit möglich, lediglich die Erscheinung im LMS würde keinerlei Rückschlüsse auf den Lernenden erlauben.

[2] `http://moodle.org`
[3] `http://www.ilias.de`

Eine nicht-wissentliche Datenerhebung findet in vielen Systemen meist in Form von Aufzeichnungen von Benutzeraktionen, d.h. Logs, statt. Nach Schulmeister sind diese Zugriffsstatistiken und Aktivitätsaufzeichnungen überaus wichtig: „Der Dozent kann jederzeit eine Statistik der Aktivitäten im virtuellen Kurs und ein Leistungsprofil seiner Teilnehmer erhalten und daran erkennen, ob und wo eventuelle Probleme auftreten“ [13, S. 8]. Mit solchen Statistiken ist es in begrenztem Maße möglich, zu klären, welche Kurse beliebt sind, wie hoch die Nutzung des LMS ist, ob jeder Lernende eine bestimmte Datei bereits gelesen bzw. heruntergeladen hat, oder ob irgendwo gehäuft Probleme auftreten. Moodle und Ilias bieten beide diese Statistiken. Während bei Moodle Statistiken als optionale Einstellung gelten, werden Aktionsprotokolle in Form von Logs in jedem Fall geführt – lediglich eine anschauliche Statistik wird nicht gegeben. Ilias hingegen stellt es zur Wahl, ob derartige Aufzeichnungen und Statistiken erhoben werden sollen bzw. welche Daten in eine solche Statistik einfließen. Eine Anonymisierung von Zugriffen ist in Moodle nicht vorgesehen, in Ilias jedoch besteht zumindest die Option der anonymisierten Ausgabe. Im Allgemeinen gilt zu beachten, dass Aktionsaufzeichnungen und Statistiken wenig Aussagekraft haben in Bezug auf Beliebtheit von Material und Probleme beim Bearbeiten dieser Daten. Die Lernenden könnten sich bereits beim ersten Anmelden alle relevanten Daten lokal herunterladen. Ebenso ist es denkbar, dass sich mehrere Lernende zusammen vor einen Rechner setzen um gemeinsam zu lernen. Eine genaue Interpretation von Aufzeichnungen im System wird damit unmöglich. Folglich scheint eine Trennung in reine, anonymisierte Zugriffsstatistik, z.B. für Werbezwecke oder technische Anpassungen gemäß der Nachfrage, und einer separaten Lehrevaluation aussagekräftiger und damit sinnvoller als eine Interpretation wenig aussagekräftiger Aktionsaufzeichnungen. Aufgrund von zeitlich beschränkter Nützlichkeit solcher Aufzeichnungsdaten kann eine befristete Datenhaltung einfach implementiert werden (vgl. Anforderung 6).
Neben allgemeinen Statistiken über Aktionen im System verfügen beide LMS über Funktionen zur Speicherung des letzten Zugriffs auf das System. Diese Funktion ist notwendig, um zu sehen, wer zurzeit angemeldet ist, d.h. wer innerhalb einer gewissen Zeitspanne Aktivitäten im System ausgeführt hat, und wer damit über das System erreichbar ist für Mitteilungen. Für Lehrende kann die Anzeige des letzten Zugriffs in begrenztem Maße Rückmeldungen bzgl. des Nutzungsverhaltens im System liefern. Diese Interpretation ist nicht ganz unproblematisch bei möglicherweise negativer Wertung von Passivität. Moodle zeigt den Zeitpunkt des letzten Zugriffs sowohl über Ausgaben von Aktivitätslogs als auch im Profil der jeweiligen Person an. Ilias hält diese Daten nur für Administratoren innerhalb der Benutzerverwaltung verfügbar.
Weitere mögliche Bereiche für Datenerhebungen und -aufzeichnungen sind Undo/Redo-Funktionen, um Aktionen rückgängig zu machen. Ebenso verfügen manche fortgeschrittenere Systeme über Profiling-Mechanismen, die sich in begrenztem Maße automatisiert auf die Gewohnheiten und Bedürfnisse von Benutzern einstellen können, oder zumindest die letzte Position im Lernmaterial speichern beim Ausloggen, um später an dieser Stelle fortzusetzen. Hierfür werden Verhaltensmuster der Anwender gespeichert und ausgewertet. Da keine dieser weiteren Aspekte von Moodle und Ilias unterstützt werden, wird hierauf nicht weiter eingegangen.

4.2 Konzeptuelle Problemfelder

Information ist unabhängig von deren augenscheinlicher Bedeutung von Wert, da sich oftmals kleine Brocken von Daten zu großen Bausteinen für mehr Information zusammensetzen und für deren Gewinnung verwenden lassen [11]. Das Sicherheitskonzept von Lern-Management-Systemen sollte auf derartige Problematiken hin untersucht und entsprechend organisiert werden. Beispielsweise ermöglichen viele LMS, auch Moodle und Ilias unter bestimmten Konfigurationen, das Sammeln von Benutzerkennungen, so dass Brute-Force-Angriffe vereinfacht werden und sich auf Passwörter beschränken können.
Neben diesen Informationen ergeben sich jedoch auch konzeptuelle Probleme, von denen ausgewählte Fälle im Folgenden näher ausgeführt werden. Es ist zu beachten, dass es sich bei den folgenden Fällen um Fehler bzw. Probleme im Design handelt, die es deutlich schwerer machen, sich dagegen zu schützen als reine Implementierungsfehler. Da ein Teil dieser Probleme jedoch mittlerweile von den Entwicklern erkannt wurde, sind zumindest „Work-arounds“ in aktuellen Versionen der genannten LMS verfügbar.

4.2.1 Einladung in Kurse

Wie bereits erwähnt, besitzen Rollen in der Regel eine inhärente, hierarchische Ordnung, d.h. Administratoren haben mehr Rechte als Lehrende und Lehrende mehr Rechte als Lernende oder sogar Gäste. Da sich die Rolle jedoch nicht an den Personen alleine festmachen lässt, sondern an Kurse gebunden ist, folgt durch die Möglichkeit, dass Lehrende andere Nutzer im System als Lernende in ihre Kurse eintragen können, eine Zwangsunterordnung. Sofern das LMS jedoch diesen Fall nicht berücksichtigt und die hierarchische Unterordnung mit Privilegien derart belohnt, dass auch kursunabhängige Dinge konfiguriert werden können, so gehen Daten an unbefugte Personen verloren oder können sogar böswillig verändert werden (vgl. Anforderung 3). Ilias ist auf dieses Problem vorbereitet und erlaubt nur kursbezogene Änderungen, Moodle hingegen ermöglicht in älteren Versionen (bis 1.7) das Verändern und Einsehen des kompletten Profils eines (lokalen) Lernenden einschließlich der Optionen, Passwörter zu verändern. Weiterhin besteht die Möglichkeit, E-Mail-Adressen von „untergebenen Personen“ für Benachrichtigungen durch das LMS systemweit zu deaktivieren! Diese Option besteht auch bei Administratoren, die in den eigenen Kurs eingetragen sind, so dass Fehler und sogar Warnungen an diese Personen nicht mehr zugestellt werden können. Das wiederum kann die Gesamtsicherheit des Systems enorm gefährden und Ausfallzeiten unnötig erhöhen! Die Lernenden werden über eine Zwangsaufnahme und ggf. ein direkt anschließendes Austragen aus dem Kurs nicht informiert, so dass eine derartige Manipulation der Daten ohne Aufsehen zu erregen möglich ist.

4.2.2 Anmeldung als anderer Benutzer

Moodle bietet Personen mit höheren, globalen Rollen an, sich mit dem Account eines Teilnehmers im eigenen Kurs anzumelden. Diese Option dient vermutlich vor allem dazu, bei technischen Problemen zu unterstützen und dabei die gleiche Ansicht zu erhalten,

die auch ein entsprechender Lernender erhält. Weiterhin bietet sich so die Möglichkeit für Lehrende, den eigenen Kurs aus Sicht eines Lernenden zu betrachten, um ggf. einen besseren Blick für noch notwendige Anpassungen zu erhalten. Schulmeister fordert diese „Debugfunktionen (Student-Ansicht für Autoren)“ sogar mit einem Wert von 5, was dem höchstmöglichen Wert für SOLL-Kriterien bei ihm entspricht [13, S. 59, Tab. 15]. Die Problematik, die sich bei einem vollwertigen Login-Wechsel ergibt, ist die eines sehr vereinfachten Identitätsdiebstahls, was überaus bedenklich erscheint (vgl. Anforderung 1). Lehrende können so alle privaten Notizen, Profildaten, und sogar fremde Kurse einsehen, sowie im Namen des Lernenden agieren und Nachrichten verfassen. Obwohl die Moodle-Entwickler diesen Missstand mittlerweile etwas abgedämpft haben und in der Grundkonfiguration in aktuellen Versionen diese Aktion nicht mehr für alle Lehrenden anbieten, existiert zumindest für Administratoren weiterhin eine derartige Möglichkeit. Als Lösung für einen Sichtenwechsel, also der „Debugfunktion“ nach Schulmeister, bieten sich Ansätze, bei denen Lehrende kurzzeitig Privilegien abwerfen bzw. die Rolle wechseln. Hierbei ist selbstverständlich darauf zu achten, dass nach einem etwaigen Rollenwechsel nicht mehr Rechte vorhanden sind als vorher. Ilias bietet für derartige Zwecke eine sog. „Lerneransicht“ in Kursen.

4.2.3 Kommunikationsinhalte

Ein grundsätzliches Problem, das sich bei Verwendung von monolithischen Lernplattformen ergibt, ist, dass alle Hilfsmittel und Werkzeuge gewissen Zwängen unterworfen sind, die das System festlegt. Bei webbasierten LMS ist dies in der Regel die Verwendung des Hypertext Transfer Protocol (HTTP). Dieses Protokoll bietet keinerlei Push-Funktionalität, so dass z.B. Chat-Nachrichten an andere Lernende notwendigerweise auf dem zentralen Server, d.h. LMS, zwischengespeichert werden müssen, bis alle beteiligten Kommunikationspartner diese Nachricht abgerufen haben. Da dieses Protokoll zustandslos arbeitet, ist selbst der Umstand, dass alle Personen eine bestimmte Nachricht abgerufen haben, nicht ohne weiteres sichergestellt. Konsequenz hieraus ist, dass jemand, der Zugriff auf das LMS besitzt, die Kommunikation selbst nach geraumer Zeit noch nachvollziehen und mitlesen könnte. Eine Löschung nach begrenzter Zeit ist daher obligat, vgl. Anforderung 6. Chat-Nachrichten werden in Moodle und Ilias beispielsweise in der Datenbank abgelegt, die mit der entsprechenden Berechtigung sogar über das System selbst wieder ausgelesen werden kann. Von privater Kommunikation kann in so einem Fall folglich nur sehr bedingt gesprochen werden. Als Lösung empfiehlt sich eine Lernumgebung in Form einer „Menge gekoppelter Werkzeuge“ [7, S. 3], wobei z.B. für Kommunikation Software und Protokolle verwendet werden können, die nicht den Zwängen von HTTP unterworfen sind und daher ihre Aufgabe auch im Sinn der gesteigerten Vertraulichkeit erfüllen können. Weiterhin besteht Uneinigkeit, ob Anonymität bei der Verwendung von Kommunikationsmitteln wie Foren sinnvoll oder gar störend ist. Ilias bietet die Option bestimmte Kommunikationsforen als anonyme Foren zu führen, bei denen Benutzernamen als freiwillige Angabe geführt werden und auch beliebige Pseudonyme zulässig sind. Laut einer (nicht-repräsentativen) schriftlichen Befragung in der E-Learning-Vorlesung am Institut des Autors ist diese Option zumindest von ca. 50% der Studenten als sinnvolle Erweiterung gesehen worden. Der Rest betrachtet Anonymität bei Kommunikation als störend, da

sich die Sender von Nachrichten hinter dieser Anonymität verstecken könnten und somit eher störende Nachrichten erwartet werden. Die Vorteilhaftigkeit bleibt also noch in der Praxis zu klären.

4.2.4 Persönliche (Kontakt-)Daten

Um Benutzer von Seiten der Verwaltung bzw. Lehrenden kontaktieren zu können, sind gewisse Kontaktdaten zu hinterlegen. Diese Daten sind jedoch nicht für alle Beteiligten im System relevant und daher auch nicht immer frei zugänglich zu handhaben. Im Sinne der benutzerfreundlichen Gestaltung von Schnittstellen nach Shneiderman [14] ist das Gefühl der Einflussmöglichkeit bei Benutzern erstrebenswert. Manche LMS, z.B. Ilias, bieten feingranulare Freigabemöglichkeiten persönlicher Daten im Profil, so dass – obwohl alle notwendigen Daten im System stehen – diese Daten nicht notwendigerweise publiziert werden. Jeder Nutzer des Systems kann entscheiden, was für Daten er anderen zugänglich macht, um kontaktiert zu werden.
Um Kontaktdaten, z.B. E-Mail-Adresse, auch vor Lehrenden zu schützen, bieten sich integrierte Nachrichtensysteme an, die es erlauben ganze Benutzergruppen oder einzelne Personen zu kontaktieren, ohne deren Kontaktdaten an den Sender zu übermitteln (vgl. Anforderung 4). Die Nachrichten werden vom System als Absender versandt. Sollte ein direkter Kontakt erwünscht sein, könnten die angeschriebenen Personen so auch direkt mit dem Absender – sofern seine Kontaktdaten wiederum bekannt gemacht wurden – auf eigene Initiative hin Kontakt aufnehmen. Ein Leck bzgl. E-Mail-Adressen kann vor allem in Bezug auf unerwünschte Werbemails negative Konsequenzen haben, da so auf einfache Art und Weise sehr viele E-Mail-Adressen gesammelt werden könnten. In Moodle werden beispielsweise Benutzer anhand ihrer E-Mail-Adresse identifiziert, was bei der Suche nach neuen Teilnehmern für den eigenen Kurs und dem manuellen Eintragen dieser Lernenden die Möglichkeit bietet, an Adressen aller Studenten zu kommen, die gewissen Suchkriterien entsprechen. Die Adressen werden ohne Verschleierung angezeigt. Dieses Problem wird dadurch verschärft, dass Lernende auch private E-Mail-Adressen angeben können, statt zwangsweise die automatisch vergebene Uni-Mail-Adresse zu verwenden, die zum einen nur begrenzte Zeit gültig ist, d.h. nur während des Studiums, und zum anderen durch das Rechenzentrum hinreichend gut gefiltert werden kann, damit Spam und Malware nicht in dem Maße an die Lernenden herankommen wie bei manch kostenlosen privaten Mailaccounts.

5 Zusammenfassung und Ausblick

Die Zuverlässigkeit eines Systems und das Vertrauen, das Nutzer in ein System bereit sind zu investieren, ist direkt verbunden mit Aspekten der Informationssicherheit (vgl. [3]). Hierbei spielt vor allem die Vertraulichkeit privater Daten eine große Rolle. Die in diesem Artikel aufgezeigten Problemfelder sind nicht nur in den genannten Lern-Management-Systemen zu finden und sind keineswegs von allen Lehrenden gleichermaßen als Probleme verstanden. In Diskussionen zwischen Lehrenden ist oft eine deutliche Polarisation zu

erkennen, was den Grad der nötigen bzw. störenden Vertraulichkeit angeht (vgl. Abschnitt 2). Moodle und Ilias zeigen deutlich unterschiedliche Ausrichtungen. Während Moodle aktivitätsorientiert ist und auf Schulen ebenso abzielt wie auf Hochschulen, hat Ilias einen deutlich stärkeren Fokus auf Hochschulen und die Organisation des eigenen Lernprozesses. Hier werden die Lernenden autonomer verstanden und weniger stark während des Lernprozesses überwacht, sind jedoch dadurch auch weniger gut zu betreuen. Letztlich bleibt jedoch festzuhalten, dass beide Herangehensweisen für die jeweilige Zielgruppe Sinn machen und vor allem auf Transparenz geachtet werden sollte. Zufällige Aufdeckung von Überwachungsmaßnahmen werden aller Wahrscheinlichkeit nach niemals positiv aufgefasst werden, obwohl sich die Aktion als solches ggf. motivieren ließe.
Neben der Vertraulichkeit sind auch andere Aspekte der Informationssicherheit zu gewährleisten, um Nutzer langfristig an E-Learning-Angebote zu binden. Hierfür sei unter anderem der Aspekt der Integrität genannt, um sicherzustellen, dass Lerninhalte nicht verfälscht wurden [2], sowie Aspekte der Verfügbarkeit, auf die Lernende vor allem dann angewiesen sind, wenn keinerlei Präsenzunterstützung vorgesehen ist. Die Informationssicherheit mit Blick auf Anforderungen in Bildungsszenarien wird daher vermutlich in den kommenden Jahren noch stark an Bedeutung gewinnen für E-Learning, um diese Form des Lehrens und Lernens auf lange Sicht in der Praxis etablieren zu können.

Literatur

[1] Anderson R.: Security Engineering – A Guide to Building Dependable Distributed Systems. Wiley Computer Publishing, New York, 2001.

[2] Eibl, C.J.; von Solms, S.H.; Schubert, S.: Development and Application of a Proxy Server for Transparently, Digitally Signing E-Learning Content. In: Venter, Hein (Ed.): New Approaches for Security, Privacy and Trust in Complex Environments. IFIP sec2007, Springer Verlag, 2007.

[3] Eibl, C.J.: Information Security in E-Learning. In: Abbott, C.; Lustigova, Z. (eds.): Information Technologies for Education and Training (iTET), IFIP Proceedings, Prag, 2007, pp. 204-213.

[4] Erickson, J.: Hacking: The Art of Exploitation. No Starch Press, Oktober 2003.

[5] Gudjons, H.: Pädagogisches Grundwissen. 7. Auflage, Klinkhardt Verlag, Bad Heilbrunn, 2001.

[6] Hoeren, T.: Internetrecht. Skriptum, Stand: September 2007, online, URL: `http://www.uni-muenster.de/Jura.itm/hoeren/material/Skript/skript_September2007.pdf` [21.02.2008]

[7] Kerres, M.; Nattland, A.; Weckmann, H.-D.: Hybride Lernplattformen und integriertes Informationsmanagement an der Hochschule. In: Dittrich, K.; König, W.; Oberweis, A.; Rannenberg, K.; Wahlster, W. (Hrsg.): Informatik 2003. Innovative Informatikanwendungen, Bd. 2, S. 90-96.

[8] Knowles, M.S.; Holton, E.F.; Swanson, R.A.: The Adult Learner – the definitive classic in adult education and human resource development. 6th Edition, Elsevier, Amsterdam, 2005.

[9] Kornblum, J.: Online privacy? For young people, that's old-school. Artikel für „USA today", online, URL: `http://www.usatoday.com/tech/webguide/internetlife/2007-10-22-online-privacy_N.htm` [18.02.2008]

[10] Maier-Häfele, K.; Häfele, H.: Open-Source-Werkzeuge für e-Trainings. managerSeminar Verlag, Bonn, 2005.

[11] Mitnick, K.; Simon, W.: Die Kunst der Täuschung. mitp-Verlag, Bonn, 2003.

[12] Rogers, C.R.: Die klientenzentrierte Gesprächspsychotherapie. 3. Auflage, Kindler Verlag, 1978.

[13] Schulmeister, R.: Lernplattformen für das virtuelle Lernen. Oldenbourg Verlag, München, 2003.

[14] Shneiderman, B.; Plaisant, C.: Designing the user interface: strategies for effective human-computer interaction. Fourth Edition, Addison-Wesley, Pearson Education, Boston, MA, USA, 2005.

[15] Weippl, E.R.: Security in E-Learning. Springer Verlag, New York, 2005.