Ereignisbasierte und konzeptuelle Schwachstellen in E-Learning-Systemen

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

Abstract: Undurchdachte Analogien zu traditioneller Lehre und vorschnelles Aufsetzen von E-Learning-Systemen begünstigen Sicherheitsprobleme. Dieser Artikel stellt Ergebnisse der Sicherheitsforschung vor und überträgt sie beispielhaft auf Bereiche des E-Learning. Fokus wird hierbei auf Kommunikation und Kollaboration gelegt, um konkret Konzeptschwächen und mögliche Angriffe zu benennen. Abschließend werden (Mindest-)Anforderungen präsentiert, die für sicheres E-Learning erfüllt sein sollten.

1 Motivation

E-Learning-Systeme werden oft mit Analogien zur traditionellen Lehre, z.B. in Schulen, in Beziehung gesetzt (vgl. [Cu02]), um Anforderungen und Aktivitäten zu diskutieren. Dieser Vergleich ist jedoch in vielerlei Hinsicht unpassend und schafft Probleme. Zum einen sind Lernmaterialien in webbasierten Systemen, die über das Internet verfügbar gemacht werden, einer nicht mehr überschaubaren Menge von Personen zugänglich, während Arbeitsblätter im Klassenverband nur einer begrenzten Anzahl Schülern zugänglich gemacht werden. Die (relativ) geringe Größe von Schulklassen sorgt dafür, dass keine Person anonym und unbekannt bleiben kann. Zum anderen werden Lernfortschritte, organisatorische Daten usw. zentral im System gespeichert und existieren nicht nur handschriftlich in Notizen der entsprechenden Lehrpersonen. Außerdem zeigt sich ein Problem bei Betrachtung verwendeter Rollen im E-Learning, wenn es darum geht, den Administrator einer physischen Person zuzuordnen. Ein Administrator kann weder exakt einem Hausmeister, der für die technische Einrichtung zuständig ist, aber keinen Zugang zu (abgeschlossenen) Aktenschränken mit Schülerdaten hat, entsprechen, noch einem Schulleiter, der zwar Einsicht in vertrauliche Daten bekommt, jedoch nichts mit der Infrastruktur zu tun hat. Ein rollenbasiertes Zugriffskonzept im E-Learning lässt sich folglich nicht exakt ohne Sicherstellung weiterer Sicherheitsmechanismen aus schulischen Szenarien extrahieren. Eine Übertragung auf E-Learning ist nur in Teilen möglich und sollte bezüglich möglicher Probleme klar durchdacht werden.

In diesem Artikel werden Gefahren und Probleme für praktische E-Learning-Systeme betrachtet – oftmals als Ergebnisse ungeeigneter Analogien. Hierfür wird ein zweistufiger

Ansatz verfolgt, der die konzeptuelle und ereignisbasierte Gefahrenlage unterscheidet. Der Artikel wurde so organisiert, dass zuerst im Stand der Forschung bisherige Arbeiten mit inhaltlicher Ähnlichkeit und Forschungsergebnissen zu sicherheitsrelevanten Aspekten betrachtet werden. Ausgehend von erziehungswissenschaftlichen Arbeiten werden anschließend in Abschnitt 3 Assets, d.h. zu schützende Güter, für E-Learning herausgestellt. In Abschnitt 4 werden beispielhaft Gefahren für das Asset „Kommunikation und Kollaboration" betrachtet. Für diese Analyse werden konzeptuelle und ereignisbasierte Gefahren getrennt betrachtet. Abschließend werden in Abschnitt 5 anhand aufgedeckter Probleme Minimalanforderungen für ein Sicherheitskonzept im E-Learning präsentiert.

2 Stand der Forschung

Auf der DeLFI 2008 wurden Designkriterien vorgestellt [Ei08a] für lerngerechte E-Learning-Angebote unter Berücksichtigung psychologischer und erziehungswissenschaftlicher Aspekte. Diese Kriterien sind in Lerntheorien verankert und führen Anforderungen an E-Learning-Systeme ein, die bei Sicherheitsüberlegungen zu berücksichtigen sind. Diese Anforderungen resultieren in erster Linie in Assets, d.h. zu schützende Daten und Prozesse im E-Learning, für die weitere Gefahrenanalyse. Zusätzlich zu diesen Kriterien lassen sich Ansätze in der Sicherheitsliteratur finden, um mögliche Assets und Gefahren zu identifizieren. Da es sich bei E-Learning-Systemen meist um webbasierte Systeme handelt, lässt sich neben allgemeinen Sicherheitsbetrachtungen im Netzwerk (vgl. [An01]) und Implementierungsproblemen (vgl. [Er03]) auch dedizierte Literatur zu webbasierten Problemen finden (vgl. [MK07]). In dieser allgemeinen Literatur wird kein besonderer Fokus auf E-Learning-Spezifika gelegt. Das Interesse an E-Learning-spezifischen Sicherheitsuntersuchungen hat jedoch in den letzten Jahren vornehmlich im internationalen Raum deutlich zulegen können, was in spezifischer Literatur resultierte, die sich mit diesem Thema befasst.

Nach von Solms [So05] gibt es aus konzeptueller Sicht eine grundsätzliche Notwendigkeit dafür, dass die organisatorische Sicherheit ausreichend Berücksichtigung findet und organisatorische Maßnahmen bzgl. Sicherheit bis auf die Führungsebene verankert sind. Er stellt in diesem Zusammenhang Anforderungen heraus, die an das Management gestellt werden, um eine tragfähige Basis für weitere Sicherheitsvorkehrungen und ein angemessenes Sicherheitskonzept zu erreichen. Ein konzeptuelles Problem ist hier vor allem in dem Konflikt zwischen Lehrenden und Lernenden zu finden (vgl. [Ei07]). Zwischen diesen Rollen zeigt sich eine Diskrepanz zwischen dem Wunsch nach Informationen aus didaktischen Gründen auf Seiten der Lehrenden und dem Wunsch nach Vertraulichkeit aus persönlichen Gründen auf Seite der Lernenden. Probleme, die sich hieraus praktisch ergeben, sind in [Ei08b] diskutiert. Anonymitäts- und Privacyforschung wurden von El-Khatib et al. in theoretischer Art und Weise auf E-Learning übertragen [El03]. Sie haben vorhandene E-Learning-Standards wie IEEE P1484.2 („Public and Private Information") des Learning Technology Standards Committee (LTSC) und IMS LIP („Learner Information Package") des IMS Global Learning Consortium bezüglich ihrer Anforderungen und Konzepte untersucht und anschließend Datenschutzaspekte herausgestellt und diskutiert.

Die Lösungsvorschläge zeigen jedoch aus praktischer Sicht nur wenig Berührungspunkte mit E-Learning und geben vorwiegend allgemeine Forschungsarbeiten zu Netzwerkanonymität wie den Mix-Ansatz von Chaum [Ch81] wieder. In den Arbeiten von Kajava und Varonen werden vornehmlich die Nutzer im E-Learning-System in den Fokus gestellt, da die Implementierung und Nutzung eines so verteilten und aufgrund moderner Lerntheorien sehr komplexen Systems ohne entsprechende Akzeptanz und ein Verständnis von Sicherheit bei den Nutzern nicht in dem nötigen Maße zu sichern wäre [KV02a, KV02b, Ka03]. Grenzen von Sicherheitmechanismen und ihrer Einflussnahme auf den praktischen Lernprozess[1] werden in [Ei09] behandelt. Hier wird herausgestellt, dass perfekte Sicherheit – speziell im E-Learning – nur in der Theorie denkbar ist und eine praktische Realisierung mit Rücksicht auf die Zielgruppe stattfinden muss, d.h. im Fall von E-Learning muss Rücksicht auf Lernende genommen werden, da diese sich nicht näher mit technischen Konzepten befassen wollen, sondern das Lernen neuer Inhalte im Vordergrund stehen sollte.

Bezüglich ereignisbasierter Gefahren für E-Learning lassen sich neben allgemeiner Sicherheitsliteratur auch spezifische Arbeiten finden, die entweder sehr konkrete Szenarien betrachten oder E-Learning als Ganzes untersuchen. Graf [Gr03] beispielsweise untersucht den sehr speziellen Bereich der webbasierten Prüfungssysteme. In seiner Dissertation werden jedoch auch allgemeine Problemsituationen von E-Learning, z.B. die Urheberrechtsverletzung durch unautorisiertes Verteilen von Lernmaterialien angesprochen und diskutiert. Die Herangehensweise zur Identifikation möglicher Gefahren ist jedoch unklar und wirkt unstrukturiert. Mit dem Vorsatz, das Feld E-Learning-Sicherheit vollständig abzudecken hat Weippl [We05] Anforderungen aus Sicht der beteiligten Rollen analysiert und diskutiert. Diese Herangehensweise wirkt sinnvoll, da hierdurch auch Rollenkonflikte offenkundig werden können. Aufgrund der sehr oberflächlichen und informatiknahen Herangehensweise ohne Berücksichtigung lerntheoretischer und psychologischer Hintergründe von Lernprozessen sind diese Erkenntnisse jedoch wenig praxistauglich. Für den Analyseansatz dieses Artikels wurde daher auf Verfahren gesetzt, die eine strukturierte Herangehensweise ermöglichen bei gleichzeitiger Abstufungsmöglichkeit bzgl. des Detailgrades. Ansätze zur Risikoanalyse bzw. des Risikomanagements, wie sie den Ergebnissen dieser Arbeit zugrunde liegen, sind vorrangig dem wirtschaftlichen Forschungsfeld entnommen (vgl. [HT83]). Investitionsrisiken müssen dort überschaubar gehalten werden im Vergleich zu möglichen Gewinnen, und negative Einflüsse sind im Vorwege zu identifizieren, um das einzugehende Risiko abschätzen zu können. Die Übertragung dieser Verfahren auf die Informatik (vgl. [Se06, SGF02]) erlaubt die bewusste Behandlung und Akzeptanz von Risiken im Bereich der Informationssicherheit. Als wiederkehrendes Muster für das Vorgehen bei der Risikoanalyse zeigen sich in [Se06, SGF02] sehr detailliert und in [An01, We05] vereinfacht folgende Schritte:

- identifizieren/klassifizieren von Assets und von möglichen Gefahren,
- beurteilen, d.h. analysieren und bewerten, von Gefahren mit Hilfe von Wahrscheinlichkeitsschätzungen und Schadensausmaß bei Eintreten,

[1] Lernprozess sei in diesem Artikel sehr allgemein verstanden. Dem Autor ist bewusst, das es hierzu diverse Sichtweisen und Interpretationen möglicher Phasen und Vorgehensweisen gibt.

- priorisieren von Risiken auf Basis dieser Schätzungen,
- festlegen und durchführen von Maßnahmen zum Abwenden/Mindern der Risiken,
- Beobachtung der Situation und möglicher neuer Risiken.

Es ist zu beachten, dass Risiko in der genannten Literatur immer als Produkt aus Wahrscheinlichkeit des Eintretens einer ungünstigen Situation und der Schadenswirkung dieses Ereignisses definiert ist. Mit Blick auf Informationssicherheit stellt vor allem die Einschätzung der Eintrittswahrscheinlichkeit ein großes Problem dar. Selbst in Katalogen wie Common Weakness Enumeration[2] (CWE), bei dem neben Sicherheitsexperten aus der Praxis in Form einer Community auch ausgewählte Expertengremien die Einschätzung vornehmen, zeigen sich Lücken in der Einschätzung. Viele der eingetragenen Sicherheitslücken und Angriffen weisen keine Schätzwerte auf. Mit Blick auf das Common Vulnerability Scoring System (CVSS)[3] wird diese Problematik deutlich: Die Einschätzung der risikorelevanten Eintrittswahrscheinlichkeiten basieren auf drei Teilschätzungen. Zu der „Base Metric Group“, die das grundsätzliche Risiko einer Schwachstelle schätzt und von Experten allgemein eingestuft werden kann, kommen noch die „Temporal Metric Group“ und die „Environmental Metric Group“ als Teilbereiche dazu. Die temporalen Aspekte betreffen hierbei die Schätzung der Aktualität und des Verbreitungsgrades von Wissen über das Ausnutzen einer bestimmten Schwachstelle. Das bedeutet, dass altbekannte Angriffstypen wahrscheinlicher sind in der Praxis als wohlmöglich gefährlichere, aber bislang kaum bekannte Angriffe. Diese Eigenschaft kann immer noch von Experten aus der Praxis unabhängig von der eigentlichen Implementierung getroffen werden. Um jedoch exakte Schätzungen für die eigene Infrastruktur zu erhalten, sind zusätzliche Teilschätzungen für die eigene Struktur notwendig, die als „Environmental Metric Group“ behandelt werden. Hierfür müssten Sicherheitsexperten aus dem eigenen Unternehmen herangezogen werden, da von außerhalb kein Einblick in lokale Besonderheiten bestehen. Zusammenfassend ergibt sich, dass eine exakte Schätzung kaum möglich ist und nur mit Näherungs- und Erfahrungswerten gearbeitet werden kann. Im Folgenden wird daher der Begriff der Gefahrenanalyse ohne die nähere Betrachtung der Eintrittswahrscheinlichkeit bevorzugt. Dies ist zudem ausreichend, da wir uns vorrangig mit der Aufdeckung und nicht der Priorisierung von Gefahren befassen wollen.

3 Identifikation von Assets

Bevor mit der Suche nach Gefahren begonnen werden kann, müssen die Assets, also die zu schützenden Elemente bekannt sein. Assets sind gewissermaßen orthogonal zu der Einstufung in konzeptuelle und ereignisbasierte Gefahren zu sehen. Beide Sorten von Gefährdungen richten sich gegen Assets, so dass hier eine übergeordnete und problemunabhängige Analyse gefordert ist.

Für E-Learning-Systeme ergibt sich eine Vielzahl von Möglichkeiten, nach denen Assets extrahiert werden können. Ansatzpunkte können Tätigkeiten einzelner Rollen im System,

[2] http://cwe.mitre.org
[3] http://www.first.org/cvss/

architekturelle Aufteilung bei einem verteilten E-Learning-System, Sicherheitsdienste wie Vertraulichkeit, Integrität, usw. oder der Abstraktionsgrad von zugrundeliegender Technik sein, d.h. technikunabhängige Prozesse werden mit anderen Assets abgedeckt als techniknahe, infrastrukturelle Aspekte. Um den Fokus auf E-Learning und die lernspezifischen Anforderungen nicht zu verlieren, wurde in dem hier zugrunde liegenden Forschungsprojekt eine Klassifikation nach dem erweiterten Informationssicherheitsmodell nach Åhlfeldt et al. [ÅSS07] verwendet. Dieses Modell erlaubt eine Einteilung in die Bereiche der technischen Sicherheit, der informal-administrativen (nutzerorientierten) Sicherheit und der formal-administrativen Sicherheit, die den organisatorischen Rahmen und das spezielle Anwendungsfeld hervorhebt. Im Folgenden werden wir auf die ersten beiden Bereiche verzichten und uns vornehmlich mit den anwendungsspezifischen, d.h. E-Learning-nahen Assets, beschäftigen. Für eine bessere Strukturierung wird als weitere Unterteilung eine Trennung von Assets mit Bezug zu Lerninhalten und Lernaktivitäten, sowie Assets mit vornehmlich organisatorischem Bezug vorgenommen.

Während des Lernprozesses fallen viele Daten an, die das weitere Vorgehen im System beeinflussen können. So kann z.B. das erfolgreiche Absolvieren eines Kurses als Einstiegsvoraussetzung in weitere Kurse dienen und somit eine Buchführung erfolgreich beendeter Kurse notwendig machen. Zudem erlauben Daten zum Lernfortschritt und zu möglicherweise aufkommenden Problemen Lehrenden, Lernende adäquat zu betreuen. Solcherlei Daten sind jedoch sehr sensibel, sofern sie Information über kognitive Probleme und Prüfungsergebnisse beinhalten. Folglich ist eine Berücksichtigung von Daten zum Lernfortschritt als Asset angebracht. Ein weiteres Asset ist durch die Lerninhalte selbst gegeben, für die selbstverständlich eine gewisse Zusicherung der Korrektheit gegeben sein sollte. Diese Inhalte werfen obendrein urheberrechtliche Fragen auf bzgl. der Verwendung fremden Materials in erstellten Inhalten und der Weiterverbreitung durch Lernende. Während des Lernprozesses sollten soziale Kontakte und Kommunikation unter Lernenden gefördert werden, um gegenseitige Motivation und Unterstützung bei Problemen zu ermöglichen [Li77, Hi79]. Kommunikationsinhalte und Zwischenergebnisse von Kollaboration sind jedoch nur für einen begrenzten Kreis von Rezipienten gedacht und daher besonders zu schützen, um nicht zwischenmenschliche Probleme zu provozieren.

Im Bereich der organisatorischen Assets, sind vor allem personenbezogene Daten, d.h. datenschutzrelevante Information, zu nennen. Hierbei werden Daten verstanden, die für organisatorische Zwecke benötigt werden, also nicht nur aufgrund der technischen Möglichkeiten aufgezeichnet wurden. Es ist dabei zu vermeiden, dass die Daten möglicherweise unautorisierten Personen zugänglich gemacht werden. Weitere Aspekte organisatorischer Art, sind in Prozessen und Gewährleistungen zu finden. Durch die fehlenden persönlichen Kontakte und damit auch einer gewissen persönlichen Verbindlichkeit sind alternative Wege in E-Learning-Systemen zu bieten, die (für alle Beteiligten) bei kritischen Aktionen Verbindlichkeit garantieren. Bezüglich der Mitbestimmungsmöglichkeiten und Transparenz im allgemeinen Ablauf ist darauf zu achten, dass technische Systeme bei Aktionen, die andere Benutzer im System betreffen, diese entsprechend informieren und ggf. um Einverständnis bitten. Ein Aspekt, der neben des organisatorischen Wertes ebenfalls aus technischer Sicht gesehen werden kann, ist die Zuverlässigkeit. Da die Lernenden evtl.

Tabelle 1: Assets für E-Learning-spezifische Bereiche.

	Bezeichnung	Beschreibung
lernbezogen	Lernfortschritte	Probleme beim Lernen und kognitive Barrieren berühren Privatsphäre und sollten nur auf Wunsch des Lernenden offengelegt und erörtert werden.
	Lerninhalte	Lernende investieren viel Zeit in das Lernen von angebotenen Inhalten. Korrektheit ist daher unabdingbar. Aus Sicht der Lehrenden sind urheberrechtliche Aspekte zu berücksichtigen.
	Kollaboration & Kommunikation	Kommunikation dient auch privaten Zwecken und gegenseitiger Motivation. Nachrichten bei Kollaboration enthalten unfertige Skizzen. Inhalte ausgetauschter Nachrichten sind daher vertraulich zu behandeln.
organisatorisch	Datenschutz	Dieser Aspekt betrifft den Verlust von Daten, die im System bzw. für die Kursverwaltung benötigt und daher erhoben werden.
	Verbindlichkeit, Rückmeldung	Abgaben von Prüfungsleistungen und Übermittlungen von kritischen Nachrichten sollen in alle Richtungen bestätigt und eventuelles Abstreiten verhindert werden.
	Transparenz & Mitbestimmung	Aktivitäten, die bestimmte Nutzer(gruppen) betreffen, dürfen nicht ohne deren Benachrichtigung bzw. Zustimmung endgültig erfolgen.
	Zuverlässigkeit	Benötigte Systeme müssen jederzeit verfügbar und möglichst frei von Beeinträchtigungen wie unzumutbaren Verzögerungen sein. Datenverlust ist zu minimieren.

nur über das E-Learning-System arbeiten und miteinander kommunizieren können, ist eine ausreichende Zuverlässigkeit unabdingbar, um Lernende nicht zu behindern.

Die hier aufgeführten Assets sind in Tabelle 1 zusammengetragen und kurz erläutert. Sie werden im folgenden Abschnitt weiterverwendet, um die beispielhafte Darstellung möglicher Gefahren zu unterstützen.

4 Beispiel: Gefahrenlage in kollaborativen Systemen

Für die Analyse wird ein zweistufiger Ansatz verwendet, der die (1) konzeptuelle und (2) ereignisbasierte Gefahrenlage unterscheidet. Es ist zu beachten, dass das Konzept alleine in der Regel noch keine konkrete Gefahr darstellt, sondern lediglich das Grundrisiko verändert und Angriffe, d.h. unerwünschte Ereignisse, möglicherweise begünstigt. Bei der ereignisbasierten Gefahrenlage werden neben der Ausnutzung konzeptueller Schwächen auch aktiv durchgeführte Angriffe auf das System berücksichtigt. Die ereignisbasierte Sicht lässt sich somit noch weiter unterteilen in (2a) konzeptbezogene und (2b) konzeptunabhängige Ereignisse. Letzteres betrifft allgemeine Gefahren, die z.B. durch die verwendete Infrastruktur und technische Unzulänglichkeiten bei Protokollen gegeben sind.

Im Folgenden werden konzeptuelle und ereignisbasierte Gefahrenlagen am Beispiel des Assets „Kollaboration und Kommunikation“ vorgestellt. Kollaboration eignet sich in diesem Zusammenhang besonders gut als Beispiel für eine Analyse, da hierbei eine große Vielfalt konzeptueller Aspekte angeschnitten werden und sich somit ein vergleichsweise guter Überblick ergibt. Berührungspunkte zu anderen Assets sind ebenfalls vorhanden, z.B. Verbindlichkeit.

Beginnend mit konzeptunabhängigen, ereignisbasierten Gefahren zeigt sich, dass diese Art der Gefahren und Angriffsvarianten nicht sehr spezifisch für das aktuell betrachtete Asset sind. Allgemeine Gefahren dieses Teilbereichs (2b) sind in der Regel technisch ausgerichtet und beziehen sich auf Schwachstellen der technischen Infrastruktur bzw. der zugrunde liegenden Technologien. Als Beispiel sei hier der häufige Programmierfehler fehlender Eingabeüberprüfung („Input Validation“, vgl. [MK07]) zu nennen. Als Unterkategorie kann man konkret SQL-Injection-Angriffe nennen, bei denen in Eingabefeldern auf Webseiten speziell geformte SQL-Statements angegeben werden, die durch eine Unachtsamkeit bei der Erstellung des Programms unverändert an die Datenbank weitergereicht werden. Laut CWE-Ranking [Ma09] ist diese Schwachstelle in den Top 25 der gefährlichsten Programmierfehler anzusiedeln. Die Relevanz für E-Learning-Systeme ergibt sich direkt aus der üblichen Kopplung an eine Datenbank als Speichermedium. Als Folge eines erfolgreichen Angriffs können Daten aus der Datenbank ausgelesen oder Daten eingefügt bzw. verändert werden. Diese Schwachstelle berührt daher alle Assets, die sich auf Daten beziehen – einschließlich Kommunikationsdaten, sowie Ergebnisse von Kollaboration.

Ein Hauptproblem bei der Konzeption von E-Learning-Systemen ist das Ziel, alle Aktivitäten und Kommunikationselemente innerhalb eines Systems anzubieten. Die Gestaltung eines E-Learning-Systems als monolithisches System mit engen Verzahnungen und auf Basis einer gemeinsamen Technologie kann zu dem Nachteil führen, dass die gemeinsame Basis nicht für alle Teilbereiche gleichgut geeignet ist. Im Fall webbasierter Systeme ist diese gemeinsame Basis die Verwendung des HTTP-Protokolls für den kompletten Datenaustausch. Die Nachteile von HTTP (vgl. [Fi99]), z.B. Zustandslosigkeit und fehlende Push-Möglichkeiten, begründen eine gewisse Starrheit und Unzuverlässigkeit der Übertragung, was gerade im Fall von Kommunikation und Kollaboration negativ auffällt. Nachrichten, die an eine komplette Gruppe von Empfängern gerichtet sind, werden nicht direkt an die Empfänger gesendet wegen fehlender Push-Funktionalität und der Beschränkung auf Client-Server-Kommunikation. Stattdessen werden die Daten von einem Server zwischengespeichert bis letztlich alle Empfänger diese Nachricht ihrerseits von diesem Zwischenspeicher abgerufen haben. Unnötige Zwischenknoten als Cache zu nutzen kann die Vertraulichkeit empfindlich stören. Da HTTP zudem keinerlei Fehlererkennungs- und -korrekturmechanismen implementiert, ist eine sichere und zuverlässige Übertragung nicht per se garantiert. Hierbei kommt ins Spiel, dass ebenfalls Zustände nicht existieren und damit eine clientseitige Sicherstellung der erfolgreichen Übertragung auf HTTP-Basis alleine nicht erfolgen kann. Die Übertragung ist auf TCP angewiesen, wobei folglich Datenverluste nur während der Übertragung gesichert werden können, nicht jedoch vor Verlust bzw. Verfälschung bei Übergabe innerhalb eines Systems zwischen den ISO/OSI-Schichten und speziell zwischen Anwendungen auf der Anwendungsschicht, z.B. Datenübergabe

zwischen Webserver (statisch) und Modulen zur Verarbeitung dynamischer Elemente wie Skripten in Webseiten.

Ein Problem, das sich weniger auf technische Konzepte als auf lehrbezogene Organisation bezieht, ist die Moderation und Beobachtung der Kommunikation von Lernenden. Moderatoren sind speziell für die Initialisierung von Arbeitsprozessen in Gruppen, bei denen sich die Teilnehmer bisher noch nicht kennen, sinnvoll. Manche Lernende könnten sich jedoch gerade durch diesen zusätzlichen Beobachter gestört fühlen. Zurückhaltung und künstliches Verhalten könnten die Folge sein, was den Kollaborationsprozess empfindlich beeinträchtigen und die Wahrscheinlichkeit erfolgreichen Lernens drastisch herabsetzen kann. Knowles et al. [KHS05] beschreiben Erfahrungen mit Gruppen, in denen Teilnehmer bei Betreuung auf Passivität zurückfallen und sich bewusst auf den Moderator verlassen, statt in Eigeninitiative Ergebnisse anzustreben. Ereignisse, die folglich für dieses Asset negativ wirken können, sind zu starke Eingriffe durch Betreuer und eine übermäßige Zensur und Einschränkung der Redefreiheit. Ein Ausweichen auf Alternativsysteme, die zum einen weniger protokollspezifische Einschränkungen, wie oben erwähnt, aufweisen, aber auch weniger Zensurmaßnahmen beinhalten, kann bei derartigen konzeptuellen Schwächen nicht ausgeschlossen werden. In Bezug auf die Betreuung und Unterstützung während kollaborativer Arbeiten im Lernprozess ergibt sich bei Ausweichen auf externe Systeme offensichtlich eine deutliche Erschwernis, da Lehrende nicht beliebig viele Systeme zusätzlich unterstützen können. Eine aktive Möglichkeit, Beobachtung zu unterwandern, könnte über sog. „Covert Channels“ umgesetzt werden (vgl. [LCC07]), wobei Lernende geheime Botschaften im offiziellen E-Learning-System ablegen und andere diese Daten interpretieren. Eine Absprache über solche Kanäle ist jedoch in der Regel stark beeinträchtigt.

Für den konkreten Fall des Arbeitens in Gruppen ergeben sich prinzipiell zwei zu unterscheidende Fälle: synchrones, also gleichzeitiges Arbeiten mit sofortigem Abgleich der Daten auf allen beteiligten Clients, und asynchrones Arbeiten mit zeitlich versetztem Datenabgleich und der Notwendigkeit, Änderungen zumindest nachvollziehen zu können. Erster Fall wird über sog. „Shared Applications“ umgesetzt, z.B. mithilfe von Shared Editors für einfache Textbearbeitung oder Shared Whiteboards für zusätzliche graphische Visualisierungsmöglichkeiten. Speziell gleichzeitiges Arbeiten auf denselben Daten[4] führt zu Problemen der Handhabung von Konflikten bei gleichzeitigen Änderungen an exakt der gleichen Stelle und zu dem Problem möglicher Priorisierung von einzelnen Änderungen gegenüber anderen. Hier spielt zum einen ein geeignetes Konzept für das Konfliktmanagement eine große Rolle, d.h. dass möglichst keine Daten ohne Weiteres verworfen werden, sondern im Fall von Konflikten beide Lösungen angezeigt werden oder sogar einzelne Lernende kurzzeitig geblockt werden, falls andere Teilnehmer an derselben Stelle aktuell Änderungen vornehmen. Aktiv können Probleme mit Simultanzugriffen über sog. „Race Conditions“ ausgenutzt werden. Diese Angriffe sind vergleichsweise schwer durchzuführen, da es auf genaues Timing ankommt. Sie können jedoch durch provozierte zeitliche Konflikte Ergebnisse einzelner Personen konsequent überschreiben und damit unbrauchbar machen. Der zweite Fall der asynchronen Bearbeitung von Daten sollte zumindest ein geeignetes Versionierungskonzept beinhalten, um Unterschiede zwischen

[4] Technisch gesehen liegen diese Daten natürlich als Kopie auf den Clients vor und werden nur ggf. abgeglichen.

einzelnen Versionen darstellen zu können und auch um ggf. ein Management für parallele Änderungen an derselben Datei durch verschiedene Teilnehmer zu gewährleisten. Die Software sollte folglich in der Lage sein, zu erkennen, ob Änderungen an verschiedenen Stellen in einer Datei vorgenommen wurden und diese Änderungen in einer gemeinsamen Ergebnisdatei zusammenbringen ohne einzelne Lösungen zu verwerfen. Da in kollaborativen Szenarien Konsens nicht immer per se zu erwarten ist, sind Möglichkeiten bereitzustellen, ältere Versionen wieder herzustellen, falls einzelne Lernende Veränderungen mit unangemessenen oder falschen Inhalten vorgenommen haben. Falls diese Möglichkeit nicht gegeben wird, könnten einzelne Lernende die komplette Gruppe sabotieren und sowohl die Integrität als auch die Verfügbarkeit bereits erreichter Zwischenergebnisse beeinträchtigen.

Da kollaborative Systeme neben der grundsätzlichen Unterstützung von Gruppenkommunikation und Gruppenarbeit auch für die Bearbeitung prüfungsrelevanter Arbeiten genutzt werden können, ergibt sich Bedarf nach Verbindlichkeiten. Diese Verbindlichkeiten schließen zum einen ein, dass Lösungsvorschläge klar einzelnen Personen zugeordnet werden können. Nachrichten an die Gruppe und Individualleistungen sollten nicht abgestritten oder verwehrt werden können. Dies ist vor allem relevant, wenn nicht die komplette Gruppe eine Gesamtnote erhalten soll, sondern ebenfalls Individualleistungen bewertet werden und die Integration einzelner Personen in die Gruppe berücksichtigt werden sollen. Im Fall von verdeckten Arbeiten innerhalb der Gruppe, so dass Lehrende nicht den Gruppenprozess überwachen und betreuen, tritt die Verbindlichkeit zumindest zum Zeitpunkt der Abgabe von Gruppenergebnissen auf. Hier ist darauf zu achten, dass Verbindlichkeit in beide Richtungen gewährleistet ist, d.h. die Gruppe der Lernenden sollte einen nichtabstreitbaren Hinweis auf das erfolgreiche Einreichen ihrer Lösung erhalten – möglichst mit Sicherstellung, dass die Lösung während des Einreichprozesses auch unverändert geblieben ist. Aus Richtung der Lehrenden ist eine Verbindlichkeit bzgl. des unveränderten Zustands der eingereichten Lösung sogar immens wichtig, da ansonsten Lernende abstreiten könnten, dass die vorgegebene Lösung in dieser Form von ihnen eingereicht wurde. Das Heranziehen der Korrekturergebnisse wäre damit für eine Bewertung nicht möglich aufgrund der Ungewissheiten eventueller, zwischenzeitlicher Manipulation. Speziell Angriffe gegen Einreichungssysteme, z.B. Man-in-the-Middle zum Abfangen und Verändern fremder Lösungen, wären fatal für die Nutzbarkeit eines webbasierten Einreichungssystems. Sicherungsmaßnahmen, die Veränderungen aufdecken, und die gewährleisten, dass Arbeiten tatsächlich eingereicht wurden, sind für diese Form der Bewertungsmöglichkeit unerlässlich.

5 Folgerungen für Konzept

Als Grundlage für die Erstellung von Anforderungen für ein geeignetes E-Learning-Konzept wird im Folgenden eine Strukturierung nach dem in Sicherheitskreisen weitverbreiteten CIA-Modell für Sicherheit verfolgt. Dieses Modell unterteilt den Begriff der Sicherheit in die drei disjunkten Bereiche Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability). Mit Rücksicht auf Mitbestimmungsmöglichkeiten und

Tabelle 2: Konzeptuelle Anforderungen bzgl. der Sicherheitsdienste.

Vertraulichkeit [Ei08b]	Verfügbarkeit
1. Authentifikation und Benutzeraccounts *2. Globale und lokale Rollen* *3. Klare Trennung der Zuständigkeiten* *4. Integriertes Nachrichtensystem* *5. Pseudonymisierung/Anonymisierung* *6. Zeitliche Begrenzung der Speicherung* *7. Transparenz*	*1. Geeignete Infrastruktur* *2. Datensicherung* *3. Verteilte Architektur* *4. Rückfallsysteme* *5. Lastausgleich* *6. Plausibilitätskontrollen*
Verbindlichkeit	**Integrität**
1. Kritische Aktionen aufzeichnen *2. PKI und Digitale Signaturen* *3. Trusted Third Party*	*1. Korrektheit von Lerninhalten* *2. Simultanzugriffe kontrollieren* *3. Zustimmung und Bestätigung* *4. Konsistenzprüfung*

verbindlich durchzuführenden Aktionen wird zusätzlich der Sicherheitdienst der Verbindlichkeit (Accountability) hinzugenommen.

Gefahren, wie sie für die Assets aus Abschnitt 3 zu finden sind, resultieren in Anforderungen für eine geeignete Sicherheitskonzeption. Diese Anforderungen sind in Tabelle 2 verteilt auf Sicherheitsdienste dargestellt. Vertraulichkeit baut hier vor allem auf ein geeignetes, flexibles Rechtemanagement mit entsprechender Trennung von Zuständigkeiten. Es sollten nicht mehr Daten als nötig aufgezeichnet und/oder preisgegeben werden. Im Falle notwendiger Datenerhebung sollen diese Daten möglichst anonym und nur zeitlich begrenzt gespeichert werden. Die Verfügbarkeit baut auf eine geeignete Infrastruktur, die auch hohen Lasten zu Zeiten großen Ansturms gewachsen ist, z.B. kurz vor Abgabeschluss von Arbeiten. Neben der obligatorischen Datensicherung sind hier Fehlverhalten von Anwendern zu berücksichtigen (bei Konfiguration: Plausibilitätskontrollen), sowie redundante Systeme, um sog. „Business Continuity“ (vgl. [An01, We05]) zu gewährleisten bei einzelnen Systemausfällen. Verbindlichkeit kann auf einfache Weise durch Aktionsprotokolle gegeben sein. Um die Verbindlichkeit jedoch auch juristisch zu sichern sind sog. „fortgeschrittene elektronische Signaturen“ nach Signaturgesetz vorgeschrieben. Dies kann über die Verwendung einer Public Key Infrastruktur (PKI) innerhalb der Bildungseinrichtung umgesetzt werden. Für besonders kritische Aktionen bzgl. des Empfangs einer Nachricht können zudem Trusted Third Parties verwendet werden, die als unabhängige Dritte Daten entgegennehmen und vermitteln. Die Integrität, die praktisch in kaum einem E-Learning-System bisher Einzug gehalten hat, stützt sich vor allem auf Korrektheitsforderungen. Das heißt, Lerninhalte und Inhalte von Kommunikation müssen unverändert übertragen werden, Zustände im System müssen konsistent bleiben und ggf. Aktionen widerrufen werden, die diese Tatsache beeinträchtigen. Lernende müssen kritischen Aktionen zustimmen können, um nicht Opfer fremder Inhaltsverfälschung zu werden, und Simultanzugriffe, z.B. bei Kollaboration, müssen vom System überwacht und gesichert werden, damit keine Daten verloren gehen aufgrund von zeitlichen Konflikten.

6 Zusammenfassung und Ausblick

In diesem Artikel wurden Assets für E-Learning eingeführt und mögliche konzeptuelle und ereignisbasierte Gefahren diskutiert. Aus Platzgründen wurde der Fokus auf Kommunikation und Kollaborationsdaten gelegt. Bei den aufgedeckten Gefahren zeigt sich, dass viele nicht ohne Weiteres lösbar sind und im E-Learning in gewissen Grenzen akzeptiert werden müssen, z.B. Unzulänglichkeiten bei zugrunde liegenden Technologien und Protokollen. Andere Gefahren wie Abschreckung und Passivität durch übermäßige Überwachung lassen sich durch Transparenz und geeignete Konzepte lösen oder zumindest deutlich abmildern. Um im E-Learning jedoch weiterhin den Fokus auf das Lernen setzen zu können, müssen die Ansprüche weg von perfekter, aber einschränkender Sicherheit, hin zu ausreichender und unterstützender Sicherheit.

Die hier vorgestellten Ergebnisse sind Teil eines noch laufenden Forschungsprojektes, das sich mit der Informationssicherheit im E-Learning als Ganzes befasst. Genannte Aspekte stellen somit nur einen Auszug aus dieser Problematik vor. Der Bedarf nach tiefergehenden Untersuchungen und Analyse der übrigen Assets ist mit diesem Artikel noch nicht behoben und bedarf weiterer Forschung.

Literaturverzeichnis

[An01] Anderson, R.J.: Security Enginieering: A Guide to Building Dependable Distributed Systems. Wiley Computer Publishing, New York, 2001.

[ÅSS07] Åhlfeldt, R.-M.; Spagnoletti, P.; Sindre, G.: Improving the Information Security Model by using TFI. In: [Ve07], Seiten 73–85.

[Ch81] Chaum, D.: Untraceable Electronic Mail, Return Address, and Digital Pseudonyms. Communications of the ACM, Vol. 24, No. 2, 1981, Seiten 84–88.

[Cu02] Cullen, J.; Hadjivassiliou, K.; Hamilton, E.; Kelleher, J.; Sommerlad, E.; Stern, E.: Review of current pedagogic research and practice in the fields of post-compulsory education and lifelong learning. Economic and Social Research Council, London, England, 2002.

[Ei07] Eibl, C.J.: Information Security in E-Learning. In: Abbott, C.; Lustigova, Z. (Hrsg.): Information Technologies for Education and Training. University of Prague, 2007, Seiten 204–213.

[Ei08a] Eibl, C.J.: Entwicklung von E-Learning-Designkriterien und Implikationen für die Informationssicherheit. In: [SLF08], Seiten 377–388.

[Ei08b] Eibl, C.J.: Vertraulichkeit persönlicher Daten in Lern-Management-Systemen. In: [SLF08], Seiten 317–328.

[Ei09] Eibl, C.J.: Privacy and Confidentiality in E-Learning Systems. In: Kellenberger, P. (Hrsg.): 2009 Fourth International Conference on Internet and Web Applications and Services (ICIW 2009). IEEE Computer Society Press, Mai 2009. In Druck.

[El03] El-Khatib, K.; Korba, L.; Xu, Y.; Yee, G.: Privacy and Security in E-Learning. Int. Journal of Distance Education, Vol. 1, No. 4, Oktober 2003, Seiten 1–19.

[Er03] Erickson, J.: Hacking: The Art of Exploitation. No Starch Press, Oktober 2003.

[Fi99] Fielding, R.; Gettys, J.; Mogul, J.; Frystyk, H.; Masinter, L.; Leach, P.; Berners-Lee, T.: Hypertext Transfer Protocol – HTTP/1.1. Request for Comments (RFC) 2616, 1999.

[Gr03] Graf, F.: Lernspezifische Sicherheitsmechanismen in Lernumgebungen mit modularem Lernmaterial. Dissertation, TU Darmstadt, 2003.

[Hi79] Hills, P.J.: Teaching and Learning as a Communication Process. Croom Helm London, 1979.

[HT83] Hertz, D.B.; Thomas, H.: Risk analysis and its applications. Wiley Computer Publishing, Chichester, 1983.

[Ka03] Kajava, J.: Security in e-Learning: the Whys and Wherefores. In: European Intensive Programme on Information and Communication Technologies Security (IPICS'2003), 4th Winter School, April 2003.

[KHS05] Knowles, M.S.; Holton, E.F.; Swanson, R.A.: The Adult Learner – the definitive classic in adult education and human resource development. Elsevier, Amsterdam, 6. Auflage, 2005.

[KV02a] Kajava, J.; Varonen, R.: Internet Security and E-Teaching. In: [Ri02], Seiten 57–66.

[KV02b] Kajava, J.; Varonen, R.: Towards a Transparent University: The Role of Cryptography, Control Measures and the Human Users. In: [Ri02], Seiten 67–76.

[LCC07] Luo, X.; Chan, E.; Chang, R.: Crafting Web Counter into Covert Channels. In: [Ve07], Seiten 337–348.

[Li77] Linskie, R.: The Learning Process: Theory and Practice. Litton Educational Publishing, New York, 1977.

[Ma09] Martin, B.; Brown, M.; Paller, A.; Christley, S.: 2009 CWE/SANS Top 25 most Dangerous Programming Errors. online: http://cwe.mitre.org/top25, Januar 2009. [20.02.2009]

[MK07] Meucci, M.; Keary, E. (Hrsg.): OWASP Testing Guide 2.0. Open Web Application Security Project (OWASP Foundation), 2007.

[Ri02] Riedling, E. (Hrsg.): VIEWDET' 2002. Vienna International Working Conference – eLearning and eCulture, Band 162. Oesterreichische Computer Gesellschaft (OCG), Dezember 2002.

[Se06] Seibold, H.: IT-Risikomanagement. Oldenbourg Wissenschaftsverlag, München, 2006.

[SGF02] Stoneburner, G.; Goguen, A.; Feringa, A.: Risk Management Guide for Information Technology Systems. Bericht Special Publication 800-30, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology (NIST), Juli 2002.

[SLF08] Seehusen, S.; Lucke, U.; Fischer, S. (Hrsg.): DeLFI 2008: Die 6. e-Learning Fachtagung Informatik, LNI Band 132, Bonn, September 2008. Köllen Druck+Verlag.

[So05] von Solms, S.H.: Information Security Governance in ICT Based Educational Systems. In: Fourth International Conference on ICT and Higher Education. Siam University, Bangkok, Thailand, September 2005.

[Ve07] Venter, H.; Eloff, M.; Labuschagne, L.; Eloff, J.; von Solms, R. (Hrsg.): New Approaches for Security, Privacy and Trust in Complex Environments. IFIP TC-11, Springer Science+Business Media, Boston, 2007.

[We05] Weippl, E.R.: Security in E-Learning. Springer Science+Business Media, New York, 2005.