Entwicklung von E-Learning-Designkriterien und Implikationen für die Informationssicherheit

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

Abstract: Dieser Artikel präsentiert Designkriterien für E-Learning basierend auf erziehungswissenschaftlichen Erkenntnissen und bringt diese in Verbindung mit Aspekten der Informationssicherheit. Es wird hierbei besonderer Wert auf den Lernprozess und die speziellen Anforderungen von Lernenden gelegt, um das Lernen gegenüber der bloßen Verwendung eines Informatiksystems zu priorisieren. Implikationen für Sicherheitsüberlegungen durch herausgestellte Probleme werden in ihrer theoretischen Realisierung diskutiert. Als Proof-of-Concept wird eine Proxy-Server-Implementierung vorgestellt.

1 Motivation

Sicherheit und Zuverlässigkeit sind wichtige Qualitätsfaktoren nahezu aller Informatiksysteme in Produktivumgebungen. Technische Realisierungsfaktoren alleine betrachtet, ohne den Einsatzkontext oder weitere Anpassungen an die Anwendergruppe zu berücksichtigen, implizieren jedoch keine dauerhafte Akzeptanz auf Client-Seite. Bei einer Definition von E-Learning, weg vom „elektronischen Lernen“, hin zu einem „enhanced learning“ mit Hilfe von Informatiksystemen, sehen wir uns mit zwei sehr verschiedenen Disziplinen konfrontiert. Die Anforderungen für Informatiksysteme können überwiegend durch technisch orientierte Fachgebiete wie Softwaretechnik einschließlich der Software-Ergonomie, Computernetze, Datenbankentwicklung oder Betriebssysteme mit Zugriffskontrollmechanismen geregelt werden. Weitaus schwieriger sind Aspekte, die durch den Anwendungskontext impliziert werden, d.h. in diesem Fall dem „Lernen“. Erziehungswissenschaftliche Forschung bringt meist abstrakte, theoretische Themen zu Tage wie Lerntheorien, didaktische Prinzipien wie Anwendungs- oder Handlungsorientierung, sowie verschiedene Unterrichtsmethoden. Solche Themen führen zu Anforderungen, die nicht mehr technisch greifbar und ohne Weiteres in technischen Systemen umsetzbar sind.
Das Forschungsprojekt des Autors beschäftigt sich mit den Beziehungen dieser beiden Disziplinen. Hierfür sind bestimmte Probleme zu untersuche, die die Interdisziplinarität von E-Learning betreffen:

- Welche Disziplin ist primär und im Fokus für Sicherheitsuntersuchungen?
- Wie interagieren diese Disziplinen und inwiefern implizieren sie einander?

- Was ist gutes E-Learning, wenn alle beteiligten Disziplinen eigene Kriterien hierfür ansetzen?

Im Folgenden werden wir basierend auf Anforderungen aus der Erziehungswissenschaft Designkriterien und deren Folgerungen für Sicherheitsüberlegungen in Hinblick auf eine geeignete Sicherheitsarchitektur für E-Learning präsentieren.

2 Stand der Forschung und Forschungsmethodik

Weippl [20] gibt einen Überblick über Sicherheitsanforderungen und Themen im Kontext von E-Learning in oberflächlicher Art und Weise. Er betrachtet Risikoanalyseverfahren, sowie informelle, subjektive Anforderungen aus Sicht verschiedener Rollen im System, d.h. nach seiner Aufteilung: Autoren, Manager, Lehrende und Lernende. Er liefert eine allgemeine Einführung in Zugriffskontrollmechanismen und beschreibt kryptographische Verfahren. Vorgestellte Problemfelder und Lösungsmöglichkeiten werden nur sehr grob skizziert ohne weiterführende Diskussion der Komplexität ihrer Anwendung und des Aufwands ihrer Implementierung in E-Learning-Umgebungen. Graf [8] präsentiert ein Framework für webbasierte Prüfungen und diskutiert Anforderungen und Schwierigkeiten bei solchen Systemen. Sein Framework zielt auf kontrollierte Umgebungen, z.B. Rechnerpool mit Aufsichtsperson, wobei für die Vermeidung aufgezeigter Probleme RMI-Nachrichten (RMI = Remote Method Invocation) zwischen den Java Applets auf Client-Seite und der Java Anwendung auf dem Prüfungsserver ausgetauscht werden. Mit diesem Ansatz kann er kritische Elemente wie Zeit-Fairness und Fortsetzung nach temporärer Unterbrechung, sofern noch innerhalb der Prüfungszeit, sicherstellen. Sein Beitrag trägt vergleichsweise wenig zur Problematik allgemeiner Informationssicherheit in E-Learning-Systemen bei, da er sehr stark auf Prüfungsszenarien ausgelegt ist. Allgemein notwendige Untersuchungen bzgl. Datenschutz und Kommunikation sowie Kooperationsmöglichkeiten im E-Learning wurden explizit vernachlässigt [8, S. 2]. Überlegungen bzgl. Datenschutzanforderungen im Bildungsbereich lassen sich in [2] finden. Alicia Anderson untersucht hierbei den Datenschutz in mehreren amerikanischen Präsenzuniversitäten, die Informatiksysteme für die Verwaltung und Speicherung persönlicher Daten verwenden. Als Hauptproblem stellte sie dabei Folgendes heraus: „the academic culture often puts a lower priority on information security in relation to openness“ [2, p. 16]. Diese „culture of openness“ verstehe ihrer Meinung nach Sicherheit und Datenschutz oftmals als störende Techniken, obwohl es bereits mehrere Vorfälle gebe, die den organisatorischen Wert und den Bedarf nach Schutz von Daten unterstreichen würden.
Da der Stand der Forschung im Bereich Sicherheit im E-Learning noch sehr oberflächlich und wenig ausgeprägt ist, strebt das hier vorgestellte Forschungsprojekt eine detaillierte Analyse, sowie die Entwicklung einer Sicherheitsarchitektur für E-Learning an. Die Forschung folgt hierbei der Forschungsmethodik wie in Abb. 1 dargestellt.
Während der Hauptteil der Untersuchungen in der mittleren Säule angesiedelt werden kann, sind die angeschlossenen Disziplinen Psychologie/Pädagogik und Informationssicherheit als seitliche Säulen mit ihren Beziehungen zur mittleren Säule angegeben. Die mittlere Säule besteht aus vier Phasen, wobei ein finaler Vorschlag für ein sicheres E-

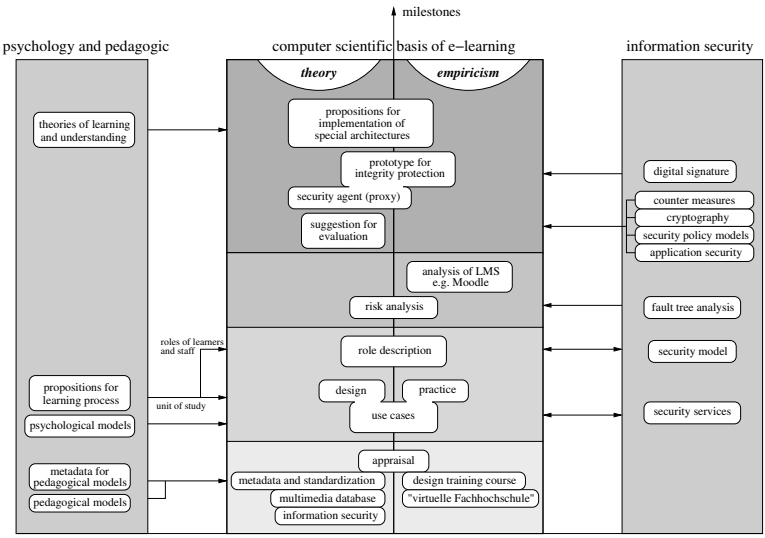

Abbildung 1: Forschungsmethodik mit Fokus auf Informatik und starken Beziehungen zu erziehungswissenschaftlichen Themen

Learning-System in der obersten Phase, d.h. Endphase, vorgestellt werden soll. Aus der linken Säule für Psychologie und Pädagogik kommen Implikationen für Funktionalitäten, die es gilt zu implementieren. Das kann grob zusammengefasst werden zu Fragen des kognitiven, sowie organisierten Lernprozesses, altersabhängige Unterschiede bei Lernenden und zu beachtende Kommunikationsbedürfnisse (vgl. Abschnitt 3.1). Die Disziplin der Informationssicherheit steuert zum Forschungsprojekt Klassifikationen von Sicherheitsdiensten bei, sowie Sicherheitsmodelle, z.B. das TFI-Modell (technical-formal-informal) von Åhlfeldt et al. [1], das die Notwendigkeit der Betrachtung formal- und informal-administrativer Sicherheit betont im Vergleich zu der meist singulär betrachteten technischen Sicherheit.

Bringt man beide Seitendisziplinen zusammen, so sind wir mit zwei sehr verschiedenen Ansichten und Ausrichtungen konfrontiert. Die Themen der linken Säule sind weit von einer technisch lösbaren und für weitere Analyse direkt verwendbaren Repräsentation entfernt, bilden jedoch eine gewisse Basis von Notwendigkeiten, die erfüllt sein müssen für eine akzeptable und das Lernen unterstützende E-Learning-Umgebung. Modelle und Methoden der Informationssicherheit auf der anderen Seite sind stark technisch orientiert, ihnen fehlt jedoch im Allgemeinen der Bezug zu E-Learning. Daraus folgt, dass eine wichtige Aufgabe dieses Forschungsprojektes darin besteht, die abstrakten, pädagogischen Anforderungen auf technisch nutzbare Themen zum Finden von passenden Sicherheitsmechanismen und Maßnahmen abzubilden, um eine Integration angepasster Verfahren in E-Learning zu ermöglichen.

Nachdem erste Risikoanalyseergebnisse basierend auf Rollenbeschreibungen (in Abstimmung mit dem genannten TFI-Sicherheitsmodell) und traditionellen Lernumgebungen in [6] präsentiert wurden, wird in diesem Artikel eine Analyse basierend auf erziehungswissenschaftlichen Forderungen verfolgt.

3 Anforderungsanalyse

3.1 Erziehungswissenschaftliche Betrachtung

Betrachten wir ein Informatiksystem, das durch angemessene Mechanismen geschützt werden soll, so scheint es das Einfachste zu sein, dieses System minimal zu gestalten. Je höher die Komplexität von Software, umso wahrscheinlicher existieren Sicherheitslücken und werden eines Tages aufgedeckt und ausgenutzt. Es stellt sich also die Frage, warum man nicht auf ein minimalistisches System setzt, das nicht viel mehr kann, als Material zur Verfügung zu stellen. Die Antwort hierauf ist leicht zu finden: Weil es nicht ausreicht für einen erfolgreichen und hinreichend gut unterstützten Lernprozess. Hamid fragte in [9] provokant, ob es bei E-Learning das „e“ (im Sinne von „elektronisch“) ist oder das „Lernen“ das zähle. Er stellte heraus, dass die Betonung in der Vergangenheit vor allem auf dem „e“ lag und Lernerfolg, sowie Akzeptanzsteigerung und -erhalt vernachlässigt wurden. Es bedürfe daher eines Wechsels, um das Lernen wieder stärker in den Vordergrund zu stellen. Die Verwendung von Informatiksystemen alleine reicht nicht aus, um „enhanced learning“, wie oben als Definition für E-Learning gegeben, zu erreichen. Es ist daher sinnvoll, Anforderungen und Erkenntnisse für den traditionellen Lernprozess und für Lernumgebungen auf ihr elektronisches Analogon zu übertragen.
Bei Betrachtung erziehungswissenschaftlicher und psychologischer Literatur ergeben sich Anforderungen, die sich zu den folgenden sechs Punkten zusammenfassen lassen:

P_1: Gleichbehandlung und gleiche Chancen
Gleichheit kann in verschiedenen Sichtweisen betrachtet werden und hat verschiedene Aspekte mit ähnlicher Relevanz, z.B. Geschlecht, Alter, Nationalität, Vorwissen oder technische Ausstattung. Bezüglich der Gleichbehandlung und Anpassung an die jeweilige Altersgruppe ist zu erwähnen, dass im letzten Jahrhundert viele Untersuchungen aus lernpsychologischer, sowie erziehungswissenschaftlicher Sicht angestrebt wurden, um den kognitiven Lernprozess und seine Beziehungen zu sozialen Verbindungen und mentaler Reife zu klären. Knowles et al. [11], zum Beispiel, untersuchten die Unterschiede und Gemeinsamkeiten zwischen Kindern und Erwachsenen und zeigten, dass Lerntheorien wie Behaviorismus oder Konstruktivismus mit ihren repräsentativen Modellen für Wissensaneignung nicht für alle Alterstufen bei Lernenden gleichermaßen verwendet werden können. Entsprechend dieser Untersuchungsergebnisse verändern Menschen ihr Lernverhalten von imitierenden Lernenden hin zu selbstbestimmten, kreativen Lernenden so signifikant, dass Aktivitätsanforderungen und Forderungen nach Möglichkeiten, den Lernprozess zu beeinflussen, enorm ansteigen. Gleichzeitig sinkt die Akzeptanz externer Kontrolle und Überwachung unabhängig vom (gut gemeinten) Ziel der besseren Betreuung durch Lehrende. Die psychologische Entwicklung von Lernenden bzgl. ihres Alters impliziert unterschiedliche Relevanz von Vorerfahrung und dem Drang nach Selbstbestimmung in ihrem Lernprozess (vgl. [4]). Anwendungsorientierung gewinnt mit steigender Erfahrung und abnehmender Lernleistung immer mehr an Bedeutung. All diese Aspekte sind im Sinne gleicher Chancen entsprechend der Zielgruppe zu berücksichtigen.
Weiterhin ergibt sich die Forderung nach Chancengleichheit bzgl. des erwarteten Vorwissens. Dies stellt sich bei E-Learning in zweierlei Hinsicht dar. Das Erwarten nicht

vorhandener Vorkenntnisse den Lerninhalt betreffend ist ein Problem das in allen Bildungseinrichtungen existiert und durch anfängliches „Abholen“ bei dem aktuellen Wissenstand in der Regel lösbar ist. Links zur Einführung und Hintergrundinformationen, sowie Terminologie für das jeweilige Themengebiet lassen sich leicht integrieren. Vorwissen bzgl. der Verwendung von Informatiksystemen hingegen ist schwieriger zu handhaben. Für Chancengleichheit darf von Lernenden nicht erwartet werden, dass sie ohne Hilfestellung wissen, wie benötigte Aufgaben mit dem System zu erledigen sind. Erkenntnisse aus Software-Ergonomie und Mensch-Computer-Interaktion können für eine angemessene Benutzungsschnittstelle übernommen werden. Weiterhin gilt auch hier der Grundsatz der ausführlichen Dokumentation und Hilfestellung.

P_2: Soziale Unterstützung durch Kooperation und Kommunikation
Für Kommunikation ergeben sich hauptsächlich zwei Gründe. Zum einen ist es ein psychologisches Bedürfnis, mit anderen soziale Kontakte aufzubauen und diese zu pflegen: „Whatever else we know or don't know about human beings, one thing is clear – we are essentially social beings.“ [14, S. 7]. Zum anderen bringt es aber auch signifikante Vorteile beim Lernen. Es ist wichtig und motivierend, Gedanken zu teilen und die eigene Sicht auf Lerninhalte anderen Lernenden mitzuteilen. Beal spricht hier von „broaden their viewpoints, gain understanding and crystallize their thinking“ [3, S. 182]. Lave und Wenger [13] prägten den Begriff des situierten Lernens, der die Relevanz der sozialen Umgebung eines Lernenden, sowie seiner Beziehungen zu anderen Lernenden hervorhebt. Kommunikation wird hierbei als ein Grundprinzip erfolgreichen Lernens verstanden. E-Learning-Systeme müssen solche Bedürfnisse ermutigen und bei der Kommunikation, sowie bei kooperativem Lernen unterstützen. Folglich ergibt sich aus diesem Ansatz die Notwendigkeit der ausreichenden Ausstattung an Kommunikationsmöglichkeiten, um Wissen auszutauschen und in Kontakt mit anderen Lernenden zu treten. Vor allem erwachsene Lernende brauchen das Gefühl der Selbstständigkeit, so dass ihnen die Gelegenheit gegeben werden sollte, über diesen Weg eigene Theorien zu verifizieren und zu verfeinern, sowie Bestätigungen oder Korrekturhinweise bzgl. ihrer Lernschritte zu erhalten (vgl. [10]).
Kommunikationstechnologien wie E-Mail, Chats und Diskussionsforen werden verwendet, um Lernende zu ermutigen, ihre Ideen mit anderen auszutauschen. Mittlerweile wird gelegentlich der Begriff „E-Learning 2.0“ in Anlehnung an „Web 2.0“ verwendet, um auf die steigende Verwendung kooperativer Software wie Blogs oder Wikis hinzuweisen, die in letzter Zeit sehr an Popularität gewonnen haben, und Publikationsmöglichkeiten für mehrere Nutzer bieten.

P_3: Aktivitäten von Lernenden als wichtiger Teil des Lernprozesses
Der kognitive Lernprozess wurde im letzten Jahrhundert sehr ausführlich und mit verschiedenen Ansätzen psychologisch untersucht, was in Lerntheorien wie Behaviorismus, Kognitivismus oder Konstruktivismus (vgl. [16, 19]) resultierte. Jede dieser Theorien beschreibt ein Modell, wie Wissen gewonnen wird, und folglich, wie Lernen stattfinden sollte, um möglichst effizient zu sein. Die momentan weitläufigste Akzeptanz findet der Ansatz des Konstruktivismus, bei dem davon ausgegangen wird, dass Lernen kein externes Einflößen von Wissen (vgl. „Nürnberger Trichter“), sondern ein aktiver Prozess der Wissenskonstruktion in jedem einzelnen Lernenden ist. Daraus folgt, dass Aktivität und Teilnahme am Lernprozess deutlich an Wert gewonnen haben und zur Beachtung dieser

Lerntheorie auch auf ein Informatiksystem übertragbar sein müssen. Betrachtet man die verschiedenen Lerntheorien, so wird deutlich, dass sich nicht alle Theorien mit vergleichbarem Aufwand implementieren lassen. Je komplexer sich eine Theorie zur Wissensaneignung Lernender darstellt, desto komplexer stellen sich auch die Methoden zur Interaktion mit Lernenden im E-Learning-System dar. Obwohl es deutlich einfacher wäre, ein System mit sehr geringem Grad an Interaktion zu implementieren (vgl. einfache Rückmeldung „richtig/gut“ bzw. „falsch/schlecht“ bei behavioristischer Ausrichtung), müssen E-Learning-Systeme in Hinblick auf komplexere Lerntheorien wie Konstruktivismus entsprechende Möglichkeiten eröffnen, aktiv zu werden, und die Lernenden teilhaben zu lassen bei der Steuerung ihres Lernprozesses. Dies impliziert einen deutlich höheren Grad an Interaktivität und erhöht damit die Komplexität der Implementierung signifikant.

P_4: Priorität liegt beim Lernen
E-Learning zielt primär auf die Unterstützung des Lernens, nicht auf die Verwendung von Informatiksystemen per se [9]. Es gilt folglich, die Aufmerksam auf die Lerninhalte zu bündeln und Ablenkungen zu vermeiden, die aufgrund der Universalität von Informatiksystemen entstehen können. Offensichtlich ist Lernen zu priorisieren gegenüber der Beschäftigung mit technischen Problemen. In Verbindung damit stehen Forderungen nach einer angenehmen Lernumgebung, was durch übermäßige externe Eingriffe und Grenzen aufgrund fehlender Funktionen verletzt sein könnte. Lernende in traditioneller Lehre können ihre Lernumgebung in gewissen Grenzen formen und kontrollieren, wohingegen dies überwiegend nicht möglich ist in Informatiksystemen, die von fremden Personen administriert werden. Folglich sollten Erscheinungsbild, transparentes Verhalten von Informatiksystemen und fortgeschrittene Benutzerfreundlichkeit mit geeignetem Grad an Personalisierbarkeit im Sinne der Anpassung an eigene Bedürfnisse näher in Betracht gezogen werden. Wenn Lernende sich auf Lernen konzentrieren sollen, dann muss das System hinter diesem Zweck verschwinden. Interaktion mit dem System selbst, d.h. ohne Lerninhalte zu betreffen, sollte für die Zeit des Lernens auf ein Minimum begrenzt werden können.

P_5: Flexibilität und Anpassbarkeit
Da Gruppen von Lernenden sehr unterschiedlich sein können, z.B. bezüglich Alter, Geschlecht, Motivation, Vorwissen oder Beruf, folgt, dass ein System an die jeweiligen Bedürfnisse und Anforderungen einer speziellen Zielgruppe flexibel und genau angepasst werden können muss. Aktuelle Modelle von Lernen propagieren zudem eine Verlagerung der Verantwortlichkeit von Lehrenden auf die Lernenden, d.h. lernerzentrierte Szenarien: „The design aims towards a usercentred, trainee-centred, interactive, collective, collaborative structure for the webbased learning environment that allows the individual to collect, organize and recontextualize knowledge.“[12, p. 1]. Dies hat zur Folge, dass flexibles Handeln im System für alle Beteiligten ermöglicht werden muss. Die Spanne zwischen tatsächlichem Vorwissen und den Erwartungen durch Lehrende in einem Kurs begründet zudem die Forderung nach Flexibilität im Sinne der Vernetzung unterschiedlichster interner und externer Ressourcen zum Zweck des individuellen Vor- und Nachbereitens von Lerninhalten.

P_6: Integration von E-Learning in die Lernumgebung
Lernen ist ein Prozess, der eine sorgfältig gestaltete Lernumgebung erfordert. Die Hauptbewegung geht hierbei zum sog. Blended Learning. Das bedeutet, dass traditionelle Lehre

und E-Learning kombiniert eingesetzt werden. Jedoch sollte nicht jede Form computerunterstützten Lernens als Blended Learning betitelt werden. Stacey und Gerbic haben mehrere Definitionsversuche analysiert und zu folgender Definition vereint: „In our application of the term blended learning, ICT may be used to either enhance the dominant mode of face-to-face on-campus interaction and or may provide a blend of synchronous and asynchronous media (that can also include face-to-face classes) to complement a dominant mode of distance education.“ [17, p. 3].
Die Integration von E-Learning in existierende Lernumgebungen sollte derart erfolgen, dass keine logischen Brüche entstehen, z.B. durch deutlich komplexere Arbeitsschritte im Vergleich zu vorher. Eine Verbindung verschiedener Teilsysteme zu einer Anwendung, die sich uniform nutzen lässt und konsistent aufgebaut ist, ist anzustreben.

3.2 Aspekte der Informationssicherheit

Es ist zu beachten, dass Sicherheit von E-Learning nicht auf technische Systeme beschränkt werden darf [20]. Es ist notwendig, die gesamte Umgebung einschließlich der organisatorischen Prozesse des Lehrens, der Administration und der Prüfungen abzudecken. Daraus folgt, dass in sinnvolle Sicherheitsbetrachtungen alle beteiligten Nutzer integriert werden müssen. Es ergibt sich hierfür eine Kombination aus Zielen, Personen, Abläufen und Werkzeugen (vgl. [15, S. 32]). Unter Verwendung dieser Erkenntnis führten Åhlfeldt et al. [1] ein erweitertes Sicherheitsmodell ein, das organisatorische Sicherheit hervorhebt. Das resultierende TFI-Modell (drei Hauptteile für Sicherheit: TFI=technical-formal-informal Security) betrachtet technische Sicherheit als lediglich ein Drittel der gesamten Sicherheitsuntersuchung. Zusätzlich dazu wird formal-administrative Sicherheit benötigt, d.h. externe Regelungen, z.B. durch Gesetze und übergestellte Reglementierungen, sowie interne Richtlinien mit lokalen Adaptionen und feine Abstimmungen, um exakt auf die jeweilige Situation zu passen. Diese Reglementierungen müssen erstellt und verifiziert werden, um die Umgebung sicher zu halten. Informal-administrative Sicherheit als dritter Teil des Modells zielt auf die Anwender im System. Sicherheitsrichtlinien sind nur von Wert, wenn alle beteiligten Personen sich deren Bedeutung und möglicher Konsequenzen der Nichteinhaltung bewusst sind, so dass sie gar nicht erst versuchen, Grenzen im System zu unterwandern. Daraus folgt, dass informal-administrative Sicherheit versucht, über die Relevanz von Sicherheitmaßnahmen aufzuklären. Weiterhin ist hierbei von Bedeutung, dass Benutzer des Systems relevante Arbeiten einfach und schnell erledigen können, so dass Schulungen zur Verwendung und der Effizienzsteigerung in diesen Bereich fallen.
Aufgrund der vielfältigen Ausprägungen von E-Learning-Systemen, z.B. Präsentationssystem vs. Prüfungssystem, wird die folgende (abstrakte) Definition für Sicherheit verwendet, die bzgl. des geforderten Sicherheitslevels innerhalb der Teilaspekte weitreichend Spielraum für situative Anpassungen lässt:

> *Ein E-Learning-System wird sicher genannt, wenn es Verfügbarkeit (S_1), Integrität (S_2) und Vertraulichkeit (S_3) für alle Benutzer garantiert in Kombination mit entsprechenden Zugriffskontrollmechanismen (S_4).*

Hierbei seien die Punkte S_1 bis S_4 wie folgt gegeben:

S_1 Verfügbarkeit:
Ein E-Learning-System wird verfügbar genannt, wenn es immer über das Netzwerk erreichbar ist, sobald es gebraucht wird, und die Anbindung ausreichend Ressourcen und Qualität bietet. Service-Zeiten müssen kurz gehalten und rechtzeitig angekündigt werden. Fehler sollten schnellstmöglich beseitigt werden, um Beeinträchtigungen zu begrenzen.

S_2 Integrität:
Modifikationen von übertragenen und gespeicherten Daten müssen erkennbar sein. Für technischen Defekt als Ursache können Fehlertoleranzen und Fehlererkennung angewandt werden. Falls es durch böswillige Angriffe begründet ist, so müssen Urheber und Kontext aufgedeckt werden können.

S_3 Vertraulichkeit:
Für die Sicherheit persönlicher Informationen (Datenschutz), z.B. Lernfortschritt, müssen Daten geheim gehalten werden. Es sollte der Entscheidung jedes einzelnen Benutzers überlassen sein, welche Daten, z.B. Lösungen und Probleme, an andere Personen weitergegeben oder verworfen werden.

S_4 Zugriffskontrolle:
Benutzer dürfen ihre Rechte nicht übertragen oder steigern können, selbst wenn mehrere Benutzer zusammenarbeiten.

4 Implikationen für Sicherheit im E-Learning

Um die Sicherheitsanforderungen im E-Learning zu untersuchen, werden die aufgestellten Kriterien aus der Erziehungswissenschaft mit den Aspekten der Informationssicherheit kombiniert. Als Basis für dieses Mapping dient das vorgestellte TFI-Modell, nach dem sich die folgenden drei Bereiche ergeben:

Technische Sicherheit: Es ist eine geeignete Infrastruktur aufzusetzen und sicherzustellen, dass diese der Menge an Daten auch in Zeiten von hohem Datenaufkommen gerecht wird. Um langen Verzögerungen bei der Kommunikation oder unzuverlässiger, angreifbarer Übertragung von Inhalten vorzubeugen, sollten das Filtern fehlerhafter Pakete, Load Balancing von eingehenden Anfragen und Quality-of-Service (QoS) für Netzverbindungen in Betracht gezogen werden. Dies ermöglicht effizienten Datenaustausch (vgl. P_2). Zusätzlich dazu sollte in Produktivumgebungen ein redundanter Aufbau mit Rückfallsystemen sichergestellt sein, so dass fehlerhafte Teile einfach und ohne Unterbrechung des Angebotes durch andere ersetzt werden können, d.h. „business continuity“ [20]. Dies stellt die Verfügbarkeit mit entsprechender Qualität sicher (vgl. S_1).
Um in Kontakt mit anderen Lernenden zu treten, muss das System entsprechende Funktionen bieten (vgl. P_2). Für kooperative Arbeit wird eine zuverlässige Ablage auf einem zentralen Server erwartet, sowie die Koordination von verschiedenen Versionen und gleichzeitigem Zugriff auf bestimmte Dateien. Regelmäßige Datensicherung ist obligat.

Um Privilegien und Identitäten für Zwecke der Zugriffskontrolle korrekt zuweisen zu können, sind Funktionalitäten für eine angemessene Authentifikation nötig. Es ist hierfür sinnvoll, bekannte und einfach anzuwendende Authentifikationssysteme (vgl. P_4) mit ausreichender Sicherheit zu verwenden. Fortgeschrittene Authentifikationsmethoden wie Biometrie oder Challenge-Response-Methoden, z.B. unter Verwendung von digitalen Signaturen, sind sinnvoll, aber nicht in allen Umgebungen anwendbar.
In Bezug auf kollaborative Arbeit ist die Datenintegrität essentiell. Das System muss garantieren, dass niemand böswillig Ergebnisse verändern kann, die zwischen teilnehmenden Personen ausgetauscht werden, zumindest nicht, ohne dass diese Änderungen zeitnah aufgedeckt werden. Datenintegrität ist ebenfalls wichtig bzgl. der Korrektheit von Lernmaterial sowie persönlichen Daten. Speziell Information für die Benotung von Lernenden und der Ausstellung von Zertifikaten darf nicht geändert worden sein. Digitale Signaturen können helfen, solche Manipulationen durch Dritte aufzudecken.
Wenn Prüfungen computergestützt durchgeführt werden sollen, müssen Routinen existieren, die dafür sorgen, dass Zeit-Fairness (vgl. P_1) sowie zuverlässige Verbindungen zwischen Client und Prüfungsserver sichergestellt werden [8]. Es ist darauf zu achten, dass allen Prüflingen nur die gleiche Menge an Hilfsmitteln zur Verfügung steht. Mit Hilfe kryptographischer Verfahren kann eine sichere Datenübertragung im Sinne der Vertraulichkeit und Integrität sichergestellt, sowie eine Fehlererkennung implementiert werden.
Für eine nahtlose Integration von E-Learning in existierende Lernumgebungen müssen E-Learning-Elemente so arbeiten, dass der Einsatz nicht störend wirkt. Eine Anbindung an relevante, weitere Systeme unter Berücksichtigung sicherheitstechnischer Kriterien kann hierbei unterstützen (vgl. P_6). Um technische Komponenten hinter den Lernzielen verschwinden zu lassen, ist die Menge systembezogener Interaktionen zu minimieren (vgl. P_4). Daraus folgt, dass, wenn mehrere Systeme zusammengeschlossen wurden, wobei jedes dieser Teilsysteme eine Authentifikation benötigt, eine Single-Sign-On-Lösung bevorzugt werden sollte. Mit Single-Sign-On, z.B. Shibboleth, Kerberos oder Verzeichnisdiensten, müssen sich Lernende nur noch einmal an einem zentralen Server anmelden und jedes Teilsystem kann anschließend den zentralen Server kontaktieren bevor im Fall von nicht ausreichender Berechtigung oder Authentifikation der Benutzer erneut gebeten wird, sich für dieses System zu authentifizieren.

Formal-administrative Sicherheit: Für diese Form der Sicherheit sind Richtlinien zu erstellen, wer in welcher Art und Weise und in welchem Umfang innerhalb des Systems agieren darf und wie bei bestimmten Ereignissen, z.B. bei Sicherheitsvorfällen, weiter verfahren wird. In der Umsetzung genießen vor allem Zugriffsrechte hohe Aufmerksamkeit, da mit einer ausreichend detaillierten und angemessenen Rechteverteilung ermöglicht wird, dass Lernende aktiv sein können ohne andere zu stören und selbst durch unautorisierte Aktionen abgelenkt zu sein (vgl. P_3,P_4). Mit Blick auf hierarchische Strukturen in traditioneller Lehre erscheinen rollenbasierte Zugriffskontrollen besonders geeignet. Da die Zahl der beteiligten Rollen sich stark unterscheiden kann in verschiedenen Kursen, folgt, dass rollenbasierte Zugriffsmechanismen flexibel erweiterbar sein sollten. Es wird hierfür ein Ansatz mit globalen und lokalen Rollen empfohlen. Globale Rollen können verwendet werden für allgemeine kursunabhängige Privilegien, die durch den Systemadministrator vergeben werden. Innerhalb von Kursen sollten Lehrende die Möglichkeit besitzen, eigene lokale Rollen zu erstellen und diese zu verwalten. Das ermöglicht eine feinere Einstel-

lung und Verteilung von Berechtigungen, da für alle beteiligten Personen und Gruppen in Kursen eigene Einstellungen erfolgen können. Hierdurch ergibt sich eine flexible Lernumgebung, die auch Anpassungen hinsichtlich der Zielgruppe erlaubt (vgl. P_5).
Um Bedenken bzgl. weitreichender Folgen von Aktivitäten im System zu vermeiden, sollte darauf geachtet werden, dass vor allem kritische Aktionen mit Warnhinweisen versehen werden. Wenn jede Aktion Schaden am System anrichten könnte und solche Aktionen nicht rückgängig gemacht werden können, kann das zu Unsicherheit und übermäßiger Vorsicht bis hin zu Inaktivität führen (vgl. P_3). Bezüglich der Vertraulichkeit ergeben sich verschiedene Sichten. Der Verlust von personenbezogenen Daten wie Name oder Adresse ist bereits problematisch, der Verlust noch privaterer und intimerer Daten über den Lernfortschritt, das Verständnis des Lernmaterials und der Inhalte privater Kommunikation ist jedoch noch schlimmer. Bedenken bzgl. der Vertraulichkeit solcher Daten können Lernende abschrecken, an Kommunikation und Kooperation teilzunehmen – gerade wenn langfristige Datenspeicherung zu erwarten ist, so dass aktuell geäußerte Meinungen noch weit in der Zukunft zu ihrem Nachteil gereichen könnten, obwohl diese Meinungen bis dahin schon überholt sind (vgl. P_2). Unterschiedliche Ansichten bzgl. der Betreuungsabsicht der Lehrenden gegenüber der Forderung nach Privatheit bei Lernenden wurden weiter im Detail in [6] erörtert. Für Richtlinien im System spielt diesbezüglich die Zielgruppe (vgl. P_1,P_5) und die Absprachen vor Beginn der Ausbildung eine große Rolle.
Für den Fall von Sicherheitsvorfällen sind entsprechende Maßnahmen zu überlegen und Pläne hierfür bereitzulegen, z.B. ein Team von Experten, das den Angriff analysiert und prüft, was ursächlich war für eine Sicherheitslücke. Ziel hierbei ist, Fehler in anderen Systemen zu vermeiden [7]. Weiterhin erlaubt dieses Vorgehen die strafrechtliche Verfolgung von Angreifern, um entstandene Schäden geltend zu machen.

Informal-administrative Sicherheit: Um die „Fehleranfälligkeit“ auf Benutzerseite zu minimieren, sollten E-Learning-Systeme möglichst einfach verwendbar sein und lernrelevante Elemente gegenüber kritischeren, technischen Elementen hervortreten (vgl. P_4). Da davon ausgegangen werden muss, dass nicht alle Lernenden Erfahrung in Bezug auf die Verwendung von Informatiksystemen mitbringen, ist eine kleine Einführung in die Benutzung der komplexen Software vor den eigentlichen Kursen sinnvoll. Mit einer solchen Einführung besteht die Möglichkeit, Überlegungen hinter gewissen Sicherheitseinstellungen und Konzepten zu erklären, um Lernenden ein Verständnis der Notwendigkeit und möglicher Konsequenzen von Fehlverhalten zu vermitteln. Ziel ist, die Bereitschaft zu steigern, solche Mechanismen zu akzeptieren statt Wege zu suchen, sie zu umgehen. Um im Fall von technischen Problemen schnell und einfach Hilfe zu erhalten, sind Kontaktmöglichkeiten vorzuhalten, z.B. über eine Hotline (vgl. P_4).
In Bezug auf die Benutzungsschnittstellen können sich signifikante Unterschiede ergeben (vgl. P_1,P_5,P_6), wenn man z.B. die Gruppe der Kinder, die eher spielerisch lernen mit vielen Anwendungen, um aktiv zu werden, und die Gruppe der Erwachsenen, die Fakten gegenüber Spielen bevorzugen und auch Teile überspringen wollen, wenn diese bereits bekannt sind, betrachtet. Es ist hierbei zu unterscheiden, wie komplex die Möglichkeiten für Anwender sein sollen oder dürfen, das System eigenen Vorstellungen anzupassen (vgl. P_1 im Sinne altergerechter Anpassbarkeit).
Eine Kombination verschiedener Systeme wie dem Verwaltungssystem einer Einrichtung, dem E-Learning-System und z.B. der Bibliothekskatalogsuche in eine Lernumgebung kann

zu einer Vereinfachung für Lernende führen. Ähnlich der Forderungen ungestörter Konzentration auf die Lernziele (P_4) ergibt sich die Forderung, dass Lernumgebungen mit integrierten E-Learning-Systemen möglichst einheitlich, ohne der regelmäßigen Notwendigkeit sich selbst an neue Erscheinungen und Bedienvarianten anzupassen, verwendet werden können (vgl. P_6). Die Verwendung eines Corporate Designs kann hierbei hilfreich sein.

5 Zusammenfassung und Ausblick

Wir haben sechs Kriterien vorgestellt für ein E-Learning-System, das aus erziehungswissenschaftlicher Sicht Lernen unterstützen kann. Da jedes Kriterium bei Anwendung und Einbringen in die Implementierung des Systems dessen Komplexität steigert, ergaben sich Implikationen für Informationssicherheit, um vor möglichen Problemen zu schützen. In diesem Artikel wurden dafür sicherheitsrelevante Themen in Verbindung mit den genannten Designkriterien gebracht und anhand der Zuordnung zu den Teilen des TFI-Sicherheitsmodells diskutiert.
Hauptziel der Überlegungen zur Informationssicherheit im E-Learning liegt auf der ungestörten Konzentration von Lernenden auf ihren Lernprozess, so dass Sicherheitsmechanismen möglichst transparent und ohne Ablenkung zu integrieren sind. In [5] wurde ein Proxy-Server als Proof-of-Concept implementiert, der alle genannten Kriterien erfüllt. Das Konzept betrachtet hierbei den Proxy-Server als eine Art persönlicher Sekretär mit Sicherheitsaufgaben, der alle technischen Angelegenheiten des Lernenden übernehmen kann, ohne auf übermäßige Interaktion mit Lernenden angewiesen zu sein. Als Beispielaufgabe wurde für den Prototyp die digitale Signierung von Lernmaterialien und Nachrichten an E-Learning-Systeme implementiert. Dieses Beispiel ermöglicht die Verifikation von empfangenen Daten und damit die Kontrolle auf Integrität. Von diesem Beispiel ausgehend lassen sich beliebige Erweiterungen des Proxy-Servers implementieren, z.B. der Authentifikation mit Challenge-Response-Verfahren, um, ohne die Lernenden zu stören, technische Sicherheitsvorgänge automatisieren zu lassen.
Da es sich bei dem Proxy-Server jedoch um ein Programm mit begrenzten semantischen Analysefähigkeiten handelt, ist davon auszugehen, dass mit Blick auf versierte Anwender, die Sicherheit nicht zwangsläufig erhöht wird. Bei Betrachtung wenig versierter Lernender, die sich nicht mit technischen Themen befassen möchten, kann die Verwendung einen deutlichen Sicherheitsvorteil bringen, da sich so trotzdem Sicherheitkonzepte integrieren lassen, ohne den Lernenden damit zu belasten und Fachkenntnisse zu verlangen. Es liegt noch im Bereich der Forschung inwiefern und unter welchen Bedingungen die Verwendung des Proxy-Servers Sicherheitsvorteile erwarten lässt.

Literatur

[1] Åhlfeldt, R.-M.; Spagnoletti, P.; Sindre, G.: Improving the Information Security Model by using TFI. In: [18], pp. 73-85, 2007.

[2] Anderson, A.: Effective Management of Information Security and Privacy. Educause Quarterly, Journal, no. 1/2006, pp. 15-20, 2006.

[3] Beal, G.M.; Bohlen, J.M.; Raudsbaugh, J.N.: Leadership and Dynamic Group Action. Iowa State University Press, Ames, Iowa, 1962.

[4] Biggs, J.B.; Moore, P.J.: The Process of Learning. Third edition, Prentice Hall, New York, 1993.

[5] Eibl, C.J.; von Solms, S.H.; Schubert, S.: Development and Application of a Proxy Server for Transparently, Digitally Signing E-Learning Content. In: [18], pp. 181-192, 2007.

[6] Eibl, C.J.: Information Security in E-Learning. In: Abbott, C.; Lustigova, Z. (Eds.): Information Technologies for Education and Training. Proc. of IFIP iTET, University of Prague, pp. 204-213, 2007.

[7] Geschonnek, A.: Computer-Forensik. 2. Auflage, iX Edition, dpunkt, Heidelberg, 2006.

[8] Graf, F.: Lernspezifische Sicherheitsmechanismen in Lernumgebungen mit modularem Lernmaterial. Dissertation, TU Darmstadt, 2002.

[9] Hamid, A.A.: e-Learning: Is it the "e" or the learning that matters? Internet and Higher Education, Vol. 4, No. 3, pp. 311-316, 2002.

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

[11] 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.

[12] Koulountzos, V.; Seroglou, F.: Designing a web-based learning environment. The case of ATLAS. In: Benzie, D.; Iding, M. (eds.): Proceedings of IFIP-Conference on „Informatics, Mathematics and ICT: A golden triangle", Boston, USA, 2007, ISBN-13: 978-0-615-14623-2.

[13] Lave, J.; Wenger, E.: Situated learning: Legitimate peripheral participation. New York: Cambridge University Press, 1991.

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

[15] McCarthy, M.P.; Campbell, S.: Security Transformation: Digital Defense Strategies to Protect Your Company's Reputation & Market Share. McGraw-Hill, New York, 2001.

[16] Skinner, B.F.: Science and Human Behavior. URL: `http://www.bfskinner.org/SHBtext.pdf`, 1953, online publiziert: 2005. [10.08.2007]

[17] Stacey, E.; Gerbic, P.: Teaching for blended learning. How is ICT impacting on distance and on campus education? In: Kumar, D.; Turner, J. (eds.): Education for the 21st Century-Impact of ICT and Digital Resources: Proceedings of the IFIP 19th World Computer Congress, TC-3, Education, Springer, Boston, 2006, pp. 225-234.

[18] Venter, H.; Eloff, M.; Labuschagne, L.; Eloff, J.; von Solms, R. (Eds.): New Approaches for Security, Privacy and Trust in Complex Environments. IFIP sec2007, Springer, New York, 2007.

[19] Vygotsky, L.: Mind in society. Cambridge, MA: Harvard University Press, 1978.

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