

Ereignisbasierte und konzeptuelle Schwachstellen in E-Learning-Systemen

Christian J. Eibl

Didaktik der Informatik und E-Learning
Universität Siegen

DeLFI 2009, Berlin
15. September 2009

1. Motivation
2. Einleitung
3. Identifikation von Assets
4. Fallbeispiel
5. Folgerungen für Konzept
6. Zusammenfassung und Ausblick

- ▶ häufiger Ansatz: Analogie zu Schulunterricht
- ▶ Problem: Ansatz greift zu kurz
 - ▶ stark unterschiedliche Teilnehmerzahlen
 - ▶ Anonymität von Teilnehmern
 - ▶ zentrale vs. dezentrale Datenablage
 - ▶ keine klare Rollenabbildung möglich
- ▶ tatsächliche Gefahrenlage für E-Learning muss betrachtet werden
- ▶ Identifikation zu schützender Daten
- ▶ Trennung von konzeptuellen und ereignisbasierten Problemen

- ▶ Forschungsprojekt für Sicherheit webbasierter E-Learning-Systeme
- ▶ allgemeine Sicherheitsliteratur nicht direkt übertragbar
- ▶ aus Common Criteria, Ver. 3.1, Overview, S. 10:
„The CC does not contain security evaluation criteria pertaining to administrative security measures not related directly to the IT security functionality. However, it is recognised that significant security can often be achieved through or supported by administrative measures such as organisational, personnel, physical, and procedural controls.“
- ▶ ... aber gerade organisatorische und administrative Aspekte unterscheiden E-Learning von rein technischen Systemen
- ▶ bisher keine systematische Untersuchung dieses Feldes

- ▶ Interessenskonflikte zwischen Rollen
 - ▶ Autonomie und selbstbestimmtes Lernen vs.
 - ▶ Verfolgen der Lernfortschritte und Eingreifen bei Problemen
- ⇒ Zielgruppe und Szenario haben starken Einfluss auf Sicherheitsanforderungen
- ▶ Lernen als primäres Ziel, Sicherheit sekundär
 - ▶ System muss weiterhin gut nutzbar sein
 - ▶ perfekte Sicherheit nicht erstrebenswert
 - ▶ technischen Interaktionsbedarf reduzieren
 - ▶ Privatsphäre schützen
- ▶ Identifikation möglicher Gefahren nötig für Abschätzung akzeptabler Risiken!
- ▶ Hinweis: keine quantitative Risikoanalyse, da Eintrittswahrscheinlichkeiten hier nachrangig

- ▶ Lernfortschritte
 - ▶ auftretende Probleme und kognitive Barrieren
 - ▶ peinlich und unangenehm bei Fremdzugriff
- ▶ Lerninhalte
 - ▶ Korrektheit von Material
 - ▶ ggf. urheberrechtliche Aspekte
- ▶ Daten von Kollaboration & Kommunikation
 - ▶ (private) Kommunikation
 - ▶ Lösungsansätze und unfertige Skizzen

- ▶ **Datenschutz**
 - ▶ personenbezogene Daten, z.B. Kontaktdaten
 - ▶ Fortschritte, absolvierte Kurse, ggf. Noten
- ▶ **Verbindlichkeit**
 - ▶ Status der Übermittlung kritischer Nachrichten
 - ▶ Bestätigungen in *beide* Richtungen
- ▶ **Transparenz/Mitbestimmung**
 - ▶ gegenseitiges Einverständnis einholen
 - ▶ Bestätigung von Statusänderungen, z.B. Kurseinschreibung
- ▶ **Zuverlässigkeit**
 - ▶ keine unzumutbaren Verzögerungen
 - ▶ Vermeidung von Datenverlust
 - ▶ möglichst durchgehende Erreichbarkeit

- ▶ ereignisbasierte und konzeptunabhängige Gefahren:
 - ▶ fehlende Eingabeüberprüfung
 - ▶ Injection-Angriffe, v.a. SQL-Injection
 - ▶ XSS und Session-Hijacking
- ▶ ereignisbasierte und konzeptabhängige Gefahren:
 - ▶ Protokollschwächen, z.B. bei HTTP
 - ▶ Management von synchron-kollaborativen Systemen (vgl. Race Conditions)
 - ▶ ungeeignete Versionierung, Löschen bisheriger Arbeiten
- ▶ konzeptuelle Gefahren:
 - ▶ Störung durch übermäßige/unerwünschte Moderation und Beobachtung von Prozessen
 - ▶ Rückfall in Passivität, statt Eigeninitiative zu zeigen
 - ▶ fehlende Integration von Verbindlichkeitsmechanismen in Einreichungssysteme

- ▶ **Vertraulichkeit**
 - ▶ Authentifikation und Benutzeraccounts
 - ▶ globale und lokale Rollen
 - ▶ klare Trennung der Zuständigkeiten
 - ▶ Pseudonymisierung/Anonymisierung
 - ▶ zeitliche Begrenzung der Speicherung
 - ▶ Transparenz
- ▶ **Integrität**
 - ▶ Korrektheit von Lerninhalten (inkl. Kommunikationsinhalte)
 - ▶ Simultanzugriffe kontrollieren
 - ▶ Zustimmung und Bestätigung
 - ▶ Konsistenzprüfung

- ▶ Verfügbarkeit
 - ▶ geeignete Infrastruktur
 - ▶ Datensicherung
 - ▶ verteilte Architektur
 - ▶ Rückfallsysteme
 - ▶ Lastausgleich
 - ▶ Plausibilitätskontrollen
- ▶ Verbindlichkeit
 - ▶ kritische Aktionen aufzeichnen
 - ▶ PKI und digitale Signaturen
 - ▶ Trusted Third Party

- ▶ Bedarf organisatorischer Sicherheitsbetrachtung von E-Learning-Systemen illustriert
- ▶ Assets im Rahmen einer Gefahrenanalyse eingeführt
- ▶ Gefahren allgemein und am Beispiel demonstriert
- ▶ Ergebnis: nicht alle Gefahren ohne Weiteres vermeidbar, z.B. Protokollunzulänglichkeiten

- ▶ Folgerungen als vereinfachte Tipps
- ▶ noch laufendes Forschungsprojekt, daher nur Auszüge präsentiert
- ▶ weitere Forschung v.a. im Bezug auf nicht behandelte Assets nötig