*HANS-ULRICH BIERHAHN*

# Sicherheit von IT-gestützten Lernsystemen

## 1 Aktuelle Situation der IT-Sicherheit

Das Internet ist nicht nur Medium für Kunst und Kultur, Information und Nachrichtenaustausch, in ihm wird auch spioniert, sabotiert, betrogen und gehehlt. In Deutschland entstehen jährlich riesige volkswirtschaftliche Schäden durch strafbare Handlungen mit Hilfe moderner Informationssysteme. Das baden-württembergische Landesamt für Verfassungsschutz schätzte diese Schäden auf jährlich 15 Milliarden Mark, die Gewerkschaft der Polizei auf 20 Milliarden Mark. Und diese Schätzungen sind noch als verhalten anzusehen, da bei Straftaten v. a. mit Hilfe des Internets die Dunkelziffer extrem hoch ist.

Diese Bedrohung betrifft aber nicht nur die Wirtschaft. Auch im privaten Bereich ist man mit Problemen der IT-Sicherheit konfrontiert. So waren z.B. bei einer Untersuchung der Stiftung Warentest die meisten privat genutzten E-Mail-Dienste nicht sicher. Traurige Berühmtheit erreichte auch der Wurm „Code Red“, der allein in einer Woche schätzungsweise 300.000 Computer weltweit befallen hat. Besonders pikant: Da „Code Red“ nur Server von Microsoft befiel, hatte Microsoft nach der Entdeckung von „Code Red“ innerhalb eines Wochenendes noch ein „Sicherheitspatch“ zu seiner Bekämpfung veröffentlicht. Trotz dieser Maßnahme hatte „Code Red“ aber zwei Tage später sogar den Server infiziert, auf dem Microsoft diesen „Sicherheitspatch“ veröffentlichte.

Einen Eindruck von der künftigen Entwicklung auf diesem Gebiet vermittelt eine CERT/CC-Statistik zur Anzahl der erfassten Systemschwachstellen und der erfassten IT-Sicherheitsvorfälle im Zeitraum 1988 bis 2001 (Abb. 1).

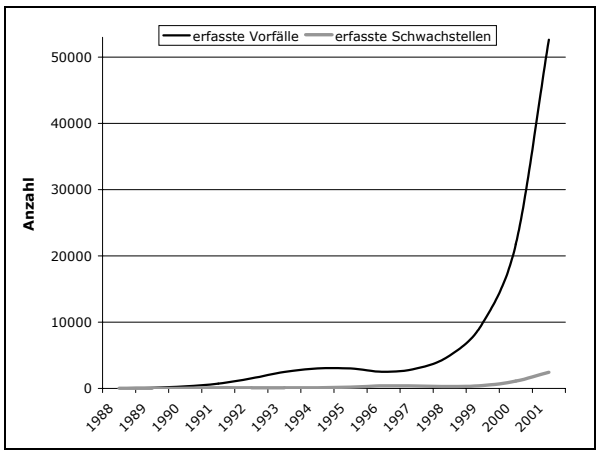


Abb. 1. *CERT/CC Statistik 1988-2001.*

Es zeichnet sich deutlich ab, dass die Anzahl der erfassten Systemschwachstellen ein immer stärkeres Wachstum aufweist. Noch interessanter ist aber das fast exponentielle Wachstum der Anzahl erfasster Sicherheitsvorfälle.

Es spricht alles dafür, dass sich die aufgezeigten Entwicklungen auch in der Zukunft in dieser Weise fortsetzen werden. Im Gegensatz dazu begegnet man aber in vielen Firmen, Institutionen und Einrichtungen immer wieder der Aussage, dass es keinerlei Probleme mit der IT-Sicherheit gäbe. Es sei durchaus möglich, dass solche Trends, wie die aufgezeigten, für andere Firmen zuträfen, aber in der eigenen Firma wären alle IT-Systeme sicher.

Diese Aussage ist bereits ein Widerspruch in sich selbst, da es keine hundertprozentige IT-Sicherheit geben kann. Ausnahmslos jedes IT-System ist unsicher, und alle Bemühungen um Sicherheit können lediglich dazu dienen, das Restrisiko zu vermindern und in ein vertretbares Verhältnis zum Aufwand zu setzen. Woraus resultiert die häufige Aussage, keinerlei Probleme mit der IT-Sicherheit zu haben? Hier sind vor allem drei Ursachen zu nennen:

Erstens aus einer Angst vor Image-Verlust, die ihre Wurzeln in einem falschen Sicherheitsverständnis hat. Anstatt davon auszugehen, dass es immer Sicherheitslücken gibt und es darauf ankommt, diese sinnvoll zu minimieren, wird jede Sicherheitslücke als Makel angesehen, den man am besten ignoriert und totschweigt.

Zweitens werden oft persönliche Konsequenzen gefürchtet, wenn Vorgesetzte, ebenfalls aus einem falschen Sicherheitsverständnis heraus, IT-Sicherheitslücken grundsätzlich als Fehlleistungen der verantwortlichen Mitarbeiter ansehen.

Und drittens werden die Erfolgskriterien für den Einsatz der begrenzten Mittel oft falsch priorisiert. Es liegt nahe, dass die Mittel z.B. für ein eLearning-Projekt vorrangig auf die Realisierung pädagogisch-didaktischer Prozesse mit Hilfe der IT konzentriert werden. Auch der Erfolg des Projektes wird verständlicherweise z.B. am Lernerfolg der Studierenden gemessen. Andere Aspekte wie die IT-Sicherheit werden dabei oft unterbewertet oder gar ganz außer acht gelassen.

Diesen Aspekt spiegeln die Ergebnisse einer Umfrage deutlich wider, bei der 500 Unternehmen und Institutionen befragt wurden, wie hoch ihr Anteil des Budgets für die IT-Sicherheit am Gesamt-IT-Budget ist. Ein Drittel aller Unternehmen und Institutionen gibt weniger als 5 Prozent des IT-Budgets für die IT-Sicherheit aus! Und bei über zwei Drittel der Unternehmen und Institutionen liegt dieser Anteil bei maximal 10 Prozent! Dieses Ergebnis ist alarmierend, wenn man es vor dem Hintergrund der immensen volkswirtschaftlichen Schäden durch mangelnde IT-Sicherheit sieht.

**Security of IT-based learning systems**

IT security incidents are increasing nearly exponentially. With this increase, the importance of data accessibility, confidentiality, integrity, and authenticity grows. IT-based learning systems are especially endangered through intentional destructive actions. A basic condition to guarantee the security of personal data is the compliance with national laws and international regulations, especially the data protection laws. Furthermore, the complex standards of the BSI baseline protection manual must be fulfilled to avoid intentional destructive actions against the IT systems.

Die Folgen dieses zunehmenden Missverhältnisses sind auch an Bildungseinrichtungen zu spüren. So wurde der Autor beispielsweise bei seinen seltenen Kontakten mit deutschen Universitäten in den letzten zwei Jahren zufälliger Zeuge folgender Sicherheitsvorfälle:

- E-Mails verschwanden spurlos
- Absenderangaben von E-Mails wurden gefälscht
- personenbezogene Daten von Mitarbeitern wurden weltweit verbreitet
- Anwendungssysteme standen wochenlang nicht zur Verfügung
- Server wurden für Angriffe auf andere Systeme missbraucht
- Hacker brachten an einer Universität die Passworte aller Nutzer in Erfahrung.

Einige Bemerkungen zum letzten Punkt, welche die Probleme hinter diesen Vorfällen verdeutlichen:

Als die IT-Administration einer deutschen Universität zufällig bemerkte, dass sich Hacker Zugriff auf die Passwortdateien verschafft hatten, bestand die hauptsächliche Reaktion in einer Empfehlung an alle eingetragenen Nutzer, sich neue Passwörter zu wählen. Das Hauptproblem besteht doch aber vielmehr darin, dass es Unbefugten überhaupt möglich war, auf diese vertraulichen Dateien zuzugreifen! Mehr noch: Es stellt sich doch die Frage, wie viel Hacker-Angriffe es bisher gab, die nicht – wie dieser – zufällig bemerkt wurden! Ein solcher schwerwiegender Sicherheitsvorfall müsste Anlass zu einer sofortigen, tiefgreifenden Analyse und grundsätzlichen Änderung des gesamten IT-Sicherheitssystems sein. Dies erfolgte in der betreffenden Universität aber nicht.

## 2 Bestandteile der IT-Sicherheit

Daten sind der Ausgangspunkt und das Ziel jeder IT-Lösung. Die Sicherheit einer IT-Lösung ist daher immer gleichbedeutend mit der Sicherheit ihrer Daten, mit deren Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität.

*Verfügbarkeit* von Daten bedeutet, dass sie zum erforderlichen Zeitpunkt im erforderlichen Umfang zur Verfügung stehen. Ist die Verfügbarkeit von Daten bei IT-gestützten Lernsystemen nicht oder nicht im erforderlichen Umfang vorhanden, kann das z.B. zur Folge haben, dass

- Prüfungsergebnisse von Studenten verloren gehen,
- hohe Kosten für die Wiederherstellung verloren gegangener Datenbestände entstehen,
- Lern- und Testprogramme nicht zum erforderlichen Zeitpunkt genutzt werden können.

*Vertraulichkeit* von Daten ist dann gegeben, wenn nur die dazu befugten Personen bzw. Personengruppen Zugriff auf die Daten haben. Mangelnde Vertraulichkeit von Daten kann z.B. bewirken, dass

- Prüfungsaufgaben vorzeitig bekannt werden,
- personenbezogene Daten incl. Testergebnisse zur Veröffentlichung kommen,
- durch Diebstahl geistigen Eigentums wie z.B. Forschungsergebnissen Schäden entstehen.

*Integrität* von Daten beinhaltet, dass diese nur in der zugelassenen Weise verändert werden und keine unberechtigten Löschungen, Ergänzungen oder Modifizierungen vorliegen. Ist die Datenintegrität nicht gesichert, kann das z.B. zur Folge haben, dass Prüfungsaufgaben, Prüfungsergebnisse, Studiennachweise, Pläne und andere Festlegungen gefälscht werden.

*Authentizität* von Daten bedeutet, dass die Herkunft der Daten eindeutig ersichtlich und belegbar ist. Ist das nicht gegeben, könnte das z.B. bewirken, dass

- der Ruf der Universität oder von einzelnen Personen durch zweifelhafte Veröffentlichungen in deren Namen geschädigt wird,
- Testergebnisse nicht eindeutig Studierenden zugeordnet werden können und damit unbrauchbar sind, oder
- eine Diskriminierung oder andere Schädigung von Personen durch zweifelhafte Emails mit deren Absender erfolgt.

## 3 Gefährdungsanalyse

Die Sicherheit von Daten wird durch höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen oder vorsätzliche Handlungen gefährdet. Für jeden dieser Bereiche müssen angemessene IT-Sicherheitsmaßnahmen konzipiert und realisiert werden. Dafür ist es – ebenfalls für jeden dieser Bereiche – erforderlich, die Gefährdungen anhand der Wahrscheinlichkeit von Schadensereignissen und deren Auswirkungen (Schadenshöhe) zu analysieren.

Einige der dabei zu berücksichtigenden Aspekte sollen im Weiteren beispielhaft an der Gefährdung IT-gestützter Lernsysteme durch vorsätzliche Handlungen skizziert werden:

*Anzahl der Nutzer:* Je höher die Anzahl der Nutzer eines eLearning-Systems ist, umso höher ist auch die Wahrscheinlichkeit vorsätzlicher Handlungen gegen dieses System.

*Alter der Nutzer:* Erfahrungsgemäß ist z.B. davon auszugehen, dass es in einer Nutzergruppe im Alter von 20 bis 30 Jahren deutlich mehr vorsätzliche Handlungen gegen ein System geben wird als etwa in einer Nutzergruppe im Alter von 50 bis 60 Jahren.

*Motivation:* Je höher die Motivation für vorsätzliche Handlungen gegen das eLearning-System ist, umso höher ist auch die Wahrscheinlichkeit solcher Handlungen. Werden mit einem eLearning-System z.B. relevante Prüfungen durchgeführt und Noten vergeben, ist die Motivation für Betrugshandlungen wesentlich höher als bei einem System, das keinerlei Tests oder Prüfungen durchführt.

Weitere Aspekte in Bezug auf die Nutzer sind z.B. auch ihr Bildungsstand, ihre verfügbare Freizeit, ihr Freizeitverhalten, die Gruppendynamik usw.

Aspekte in Bezug auf die IT-Umgebung sind z.B. die Anzahl der angeschlossenen Workstations und Server, die Homogenität der IT-Komponenten, die Größe und Komplexität des Netzes, die Dynamik der Netzstruktur, die Administration usw. Darüber hinaus wären weitere Aspekte zu untersuchen, die sich aus anderen Bereichen wie z.B. den baulichen Gegebenheiten, der Zutrittskontrolle, der technischen Infrastruktur usw. ergeben.

Insgesamt wird aber bereits an diesen wenigen beispielhaft genannten Aspekten deutlich, dass bei eLearning-Systemen an Universitäten, Hoch- und Fachschulen sowie allgemein- und berufsbildenden Schulen insgesamt von einer hohen Wahrscheinlichkeit vorsätzlicher

Handlungen gegen diese Systeme ausgegangen werden kann. Für die Abschätzung der Schäden, die durch erfolgreiche Angriffe zu erwarten sind, muss ebenfalls eine Vielzahl von Aspekten berücksichtigt werden.

Die Vertraulichkeit besitzt eine besonders hohe Wertigkeit bei der Beurteilung von Gefährdungen und Konzeption von IT-Sicherheitsmaßnahmen, da für sie in einer Vielzahl von Fällen konkrete rechtliche Regelungen und Pflichten bestehen, die zwingend eingehalten werden müssen.

## 4 Gesetzliche Bestimmungen

Gesetze, in denen Festlegungen zur IT-Sicherheit getroffen werden, sind z.B. das Gesetz zur Kontrolle und Transparenz (KonTraG), das Telekommunikationsgesetz (TKG), das Signaturgesetz (SigG), die Landesdatenschutzgesetze (LDSG) und das Bundesdatenschutzgesetz (BDSG). Von besonderer Bedeutung für IT-gestützte Lernsysteme sind dabei die Datenschutzgesetze, da diese Systeme meistens personenbezogene Daten verarbeiten und somit dem Datenschutzrecht unterliegen.

Personenbezogene Daten sind zum Beispiel: Namen, Geburtsdaten, Adressen, Angaben zu Schulbesuchen, Qualifikationen, Beschäftigungsverhältnissen usw. Darüber hinaus fallen noch weitere personenbezogene Daten an wie z.B. Angaben über den Studienverlauf, Leistungen, Prüfungsergebnisse und Einschätzungen, Persönlichkeitsprofile und -merkmale. Gerade diese Daten sind für die Gewährleistung der Persönlichkeitsrechte des Einzelnen besonders kritisch!

Beispielhaft sollen hier nur einige Probleme skizziert werden, die sich aus datenschutzrechtlicher Sicht für die Verarbeitung personenbezogener Daten ergeben:

*Personenbezogene Daten dürfen nicht ohne gesetzliche Ermächtigung oder Zustimmung der Betreffenden erhoben, verarbeitet und gespeichert werden.*

Das heißt, dass für jede Erhebung, Verarbeitung und Speicherung von personenbezogenen Daten eines Lernenden in einem eLearning-System dessen schriftliche Zustimmung erforderlich ist. Pauschale Einverständniserklärungen reichen nicht aus. Vielmehr muss aus der Erklärung hervorgehen, welche konkreten Daten (z.B. auch Daten zum Lernverlauf, Daten zu Ergebnissen psychologischer oder psychosomatischer Tests usw.) erhoben, gespeichert und weiterverarbeitet werden.

*Personenbezogene Daten dürfen nicht für andere Zwecke als den Erhebungszweck genutzt werden.*

Diese Rechtspflicht könnte an Universitäten und Hochschulen problematisch werden, wo es verständliches Interesse daran gibt, empirische Daten z.B. aus Lernprogrammen auch für Forschungszwecke weiterzunutzen. Ist dies vorgesehen oder wird es perspektivisch nicht ausgeschlossen, muss die Einverständniserklärung der Lernenden auch diese Verwendung der Daten einschließen, damit eine solche Nutzung zulässig ist.

Personenbezogene Daten dürfen nicht über den erforderlichen Zeitraum hinaus gespeichert werden.

Das Problem bei der Erfüllung dieser Rechtspflicht liegt bei eLearning-Systemen zum einen in einer exakten Begründung des erforderlichen Zeitraums. Das trifft insbesondere auf Daten zu, die ausdrücklich auch zum Zwecke späterer Forschungszwecke erhoben und gespeichert werden. Zum anderen ist es an Universitäten meist schwer, die Löschung der Daten nach Ablauf des erforderlichen Zeitraums organisatorisch sicherzustellen, da oft nicht einmal bekannt ist, wo welche Daten gespeichert sind und wann sie gelöscht werden müssen.

Personenbezogene Daten dürfen nicht Dritten zugänglich gemacht werden.

Auch dieses Problem dürfte von besonderer Relevanz für IT-gestützte Lernsysteme sein, mit denen auch Daten für Forschungszwecke – so z.B. zur Evaluation des Systems – gewonnen werden sollen. Die Weitergabe dieser Daten z.B. an Forschungsprojekte anderer Einrichtungen ist nur zulässig, wenn der Lernende dieser Weitergabe seiner Daten ausdrücklich zugestimmt hat.

Festlegungen zur IT-Sicherheit sind aber nicht nur in gesetzlichen Bestimmungen enthalten. Darüber hinaus gibt es eine Vielzahl allgemeiner Normen für die IT-Sicherheit, die bei der Konzeption und Anwendung IT-gestützter Lernsysteme berücksichtigt werden müssen.

## 5 Allgemeine Normen

Hierunter werden alle die Normen für die IT-Sicherheit gefasst, die nicht unmittelbar rechtsverbindlich, aber allgemein anerkannt sind. Solche Normen sind z.B.

- das BSI-Grundschutzhandbuch,
- die Europäische Bildschirmrichtlinie (90/270/EU),
- die ISO 9241 (Ergonomische Anforderungen für Bürotätigkeiten mit Bildschirmgeräten) – 17 Teile,
- die ISO 13407 (Benutzerorientierte Gestaltung interaktiver Systeme),
- Arbeitsschutzvorschriften.

Weitere allgemeine Normen für die verschiedensten IT-Gebiete werden ständig erarbeitet. Für IT-gestützte Lernsysteme besonders interessant ist z.Zt. die Arbeit des Normungsausschusses Lerntechnologien NI-36 beim DIN e.V., der allgemeine Normen für IT-gestützte Lerntechnologien erarbeitet.

Wenn diese Normen auch nicht direkt rechtsverbindlich sind, ist eine indirekte Verbindlichkeit in den meisten Fällen aber dadurch gegeben, dass andere rechtsverbindliche Festlegungen eine Einhaltung dieser Normen fordern. So ist z.B. die Einhaltung der ISO-Normen für die Ergonomie von Bildschirmarbeitsplätzen selbst keine Rechtspflicht, wird aber beispielsweise für den öffentlichen Bereich durch Verordnungen, Rahmenvereinbarungen usw. zwingend gefordert. Als Beispiel für allgemeine Normen soll im weiteren das BSI-Grundschutzhandbuch kurz näher betrachtet werden.

Die Standards des BSI sind in seinem „Grundschutzhandbuch“ zusammengefasst, einem äußerst umfangreichen Werk, das inzwischen zur einer Art „Bibel der IT-Sicherheit“ in Deutschland geworden ist.

Das umfangreiche Grundschutzhandbuch des BSI regelt ausschließlich Anwendungen mit niedrigem und mittlerem Schutzbedarf. Für IT-gestützte Lernsysteme, die personenbezogene Daten verarbeiten, gilt, dass sie aus datenschutzrechtlicher Sicht mindestens hohen Schutzbedarf haben. Das heißt, dass sie in jedem Fall die umfangreichen Standards des BSI-Grundschutzhandbuches erfüllen müssen. So anspruchsvoll und

aufwendig das auch zu realisieren ist, reicht es dennoch nicht aus. Darüber hinaus müssen weitergehende, aufwendige IT-Sicherheitsmaßnahmen konzipiert und umgesetzt werden, um dem hohen Schutzbedarf der verarbeiteten Daten gerecht zu werden.

## 6 Angriffsmethoden

Die Sicherheitsmaßnahmen müssen u.a. auch destruktive vorsätzliche Handlungen ausschließen bzw. deren Auswirkungen verringern. Zur Illustration, wie Gefährdungen durch vorsätzliche Handlungen konkret aussehen können, werden einige häufige Angriffsmethoden genannt, die speziell für IT-gestützte Lernsysteme von Bedeutung sind (ausführlich Bierhahn, 2002):

- Angriffe auf Passworte (durch Raten, Erfragen, durch entspechende Programme),
- Provozieren von Programmabstürzen,
- Sniffing (Abfangen und Analysieren von IP-Paketen durch Unbefugte, insbesondere bei Wireless Lans),
- Spoofing (Vortäuschen einer falschen Identität; Varianten: IP-Spoofing, DNS-Spoofing, Mail-Spoofing),
- Spamming (massenhaftes Versenden von Emails),
- Denial Of Service Attacken (Ziel: IT Komponenten durch Überlassung außer Betrieb setzen),
- Einsatz destruktiver Programme (Viren, Würmer, Trojaner sowie Mischformen),
- Social Engineering (systematisches Aushorchen durch Beobachten oder Ausfragen).

## 7 Schutzmaßnahmen

Noch vielfältiger als die Gefährdungen sind die möglichen IT-Sicherheitsmaßnahmen. Da gibt es Maßnahmen für physischen, logischen oder zeitlichen Zugriffsschutz, Maßnahmen für den Virenschutz, Firewalls, Verschlüsselungen, Virtual Private Networks, digitale Signaturen, Maßnahmen zur korrekten Konfiguration von Servern, Intrusion Detection Systeme, Backupkonzepte, Desaster Recovery und vieles mehr. Diese Maßnahmen, können aber im Rahmen dieses Beitrags nicht dargestellt werden und müssen für jede Lösung IT-gestützter Lernsysteme spezifisch erarbeitet werden.

## Literatur

Bierhahn, H.-U. (2002, i.D.). Security in IT-based learning systems. *International Journal of Computer Science in Sport, 1* (www.iacss.org/ijcss/iacss_ijcss.html)

Carpenter, J.J. (2002). *CERT/CC: Overview Incident and Vulnerability Trends.* Zugriff am 23. August 2002 unter http://www.cert.org/present/cert-overview-trends/module-1.pdf

Hans-Ulrich BIERHAHN
TÜV-Nord SecurITy
Kieler Str. 303
22525 Hamburg
eMail: u.bierhahn@web.de