Gesellschaft für Informatik e.V. (GI)

IT-Sicherheit in der Ausbildung

Empfehlung zur Berücksichtigung der IT-Sicherheit in der schulischen und akademischen Ausbildung

Inhalt

Empfehlung der Gesellschaft für Informatik e.V. (GI), verabschiedet vom GI-Präsidium auf seiner Sitzung am 3. Oktober 2006 in Dresden

KURZFASSUNG

Die vorliegende Empfehlung enthält Vorschläge zur Berücksichtigung der IT-Sicherheit in der schulischen und akademischen Ausbildung und richtet sich sowohl an die in der IT-Sicherheit tätigen Lehrkräfte bzw. Professorinnen und Professoren als auch an Personen, die für Konzeption und Planung von Ausbildungsprogrammen an Schulen und Hochschulen verantwortlich sind.

In der Schule soll fächerübergreifend ein grundlegendes Verständnis für Sicherheitsbelange im Umgang mit dem Computer geweckt werden. Dabei soll – je nach Schultyp und -ausrichtung – die IT-Sicherheit nicht nur im Rahmen des Informatikunterrichtes gelehrt, sondern auch in andere Fächer einbezogen werden. Alle Jugendlichen müssen bis zum Ende ihrer schulischen Ausbildung grundlegende Kenntnisse erwerben.

Darauf aufbauend sollen Grundlagen der IT-Sicherheit für alle Studierenden unabhängig von ihrer Fachrichtung Bestandteil der akademischen Ausbildung sein. Besonders in Informatik- bzw. informatiknahen Bachelor- und Master-Studiengängen (auch Lehramt Informatik und Informatik als Nebenfach) muss Sicherheit ein Bestandteil des Curriculums sein und je nach individuellem Interessensschwerpunkt in Wahlpflichtveranstaltungen vertieft werden können. Diese Spezialisierung soll bis hin zu eigenständigen Studiengängen in IT-Sicherheit führen, die vom Umfang her einem Informatik- oder informatiknahen Master-Studiengang entsprechen.

Die inhaltliche Tiefe, die genaue Ausgestaltung, sowie die Art der Vermittlung des Themas IT-Sicherheit werden abhängig vom Typ der Hochschule und dem jeweiligen Studiengang stark variieren. Auch das Profil der jeweiligen Hochschule und der dort Lehrenden wird die genaue inhaltliche Ausgestaltung weiter beeinflussen. Die folgenden Vorschläge dienen als Rahmenempfehlung und Hilfestellung für die Integration sicherheitsrelevanter Inhalte in die Ausbildung an Schulen und Hochschulen.

1 EINLEITUNG UND MOTIVATION

Die Informationstechnik hat unsere Gesellschaft verändert und wird sie weiter verändern. Durch die Verlagerung von Prozessen aller Art auf IT-Systeme wird die Abhängigkeit der gesamten Gesellschaft von einer sicher funktionierenden Informationstechnik deutlich; und diese Abhängigkeit wird sich weiter verstärken. Computer werden immer kleiner, schneller, allgegenwärtig und 'unsichtbar'; sie werden in nahezu allen Bereichen der modernen Gesellschaft eingesetzt.

In dem Maße, in dem Wirtschaft und Verwaltung und zunehmend auch unsere Privatsphäre vom ordnungsgemäßen, das heißt vom verlässlichen und beherrschbaren Funktionieren der Systeme und Verfahren abhängen, kommt der Sicherheit – sowohl gegen ungeplant auftretende Systemstörungen als auch gegen planvoll initiierte böswillige Aktionen – eine immer größere Bedeutung zu. Sicherheit muss immer die Systeme als Ganzes berücksichtigen und dabei unter zwei Aspekten gesehen werden: Sicherheit der Systeme selbst und Sicherheit der durch die Systeme Betroffenen.

Ziel jeder Art von Hochschulausbildung muss es sein, die Ausgebildeten in ihren späteren Rollen (beispielsweise in der Nutzung, Entscheidung oder Entwicklung der Systeme) zu unterstützen. Mit dem Thema Sicherheit als unverzichtbarem Bestandteil der Ausbildung sollen Lernende in die Lage versetzt werden, die Informationstechnik sicher zu nutzen, einzusetzen, zu betreiben, zu entwerfen oder zu entwickeln.

In den letzten Jahrzehnten ist in der Informatik zu diesem Thema ein selbständiges Lehr- und Forschungsgebiet entstanden. Ziel dieser Aktivitäten ist, Vertraulichkeit, Integrität und Verbindlichkeit sowie Verfügbarkeit und Zuverlässigkeit im Betrieb von Computern und Netzen zu erreichen. Nutzende erwarten den Schutz ihrer Daten und die Sicherheit ihrer PCs, Handys, etc. Mangelnde Ausbildung und fehlendes Wissen machen oft die Nutzenden selbst zu einem erheblichen Sicherheitsrisiko. Unternehmen erwarten den Schutz ihrer Unternehmensdaten; gleiches verlangt der Gesetzgeber auch bei der Verarbeitung personenbezogener Daten. Finanzdienstleister und Rating-Agenturen fordern dies für sich und ihre Geschäftspartner in hohem Maße, weil sie gesetzlich dazu verpflichtet sind und weil überdies viele Unternehmen von der Informationstechnik betriebswirtschaftlich und volkswirtschaftlich stark abhängig sind. Die heute in Wirtschaft, Verwaltung und Militär genutzten IT-Systeme bieten erhebliche Angriffsmöglichkeiten, die weltweit immer wieder zu hohen materiellen und immateriellen Schäden führen.

Wegen der großen Bedeutung der Informationstechnik für die Gesellschaft muss eine Ausbildung in IT-Sicherheit so früh wie möglich beginnen. Deshalb ist es sinnvoll, IT-Sicherheit bereits in die schulische Ausbildung zu integrieren und dies in Studiengängen aller Fachrichtungen fortzusetzen. Besonders in die Konzeption von informatikbezogenen Studiengängen ist die IT-Sicherheit unbedingt einzubeziehen. Sowohl in Bachelor- wie in Master-Studiengängen soll IT-Sicherheit fester Bestandteil des allgemeinen Curriculums sein und in Studienschwerpunkten vertieft werden können. Ergänzend dazu wird die Einrichtung von speziellen Studiengängen in IT-Sicherheit empfohlen.

Für Schülerinnen und Schüler sollten Themen altersgerecht und für eine akademische Ausbildung dem jeweiligen Ausbildungsgang entsprechend ausgewählt werden. Allgemein gilt, dass sich die Inhalte nicht nur auf ein einzelnes Fachgebiet innerhalb der IT-Sicherheit beschränken dürfen. Die Ausbildung muss breit ausgerichtet sein und die Behandlung von Sicherheit fächerübergreifend berücksichtigen.

Im Folgenden werden Inhalte einer Ausbildung in IT-Sicherheit sowohl auf akademischer als auch auf schulischer Ebene (Kapitel 2 und Kapitel 3) aufgeführt. Für die Ausbildung an Hochschulen wird zwischen Bachelor- und Master-Studiengängen, Informatik als Nebenfach und Lehramt Informatik unterschieden.

2 AUSBILDUNG AN HOCHSCHULEN

IT-Sicherheit muss unabhängig von der Fachrichtung in alle Studiengänge an allen Hochschulen so früh wie möglich einbezogen und ihrer zunehmenden Bedeutung entsprechend gelehrt werden. Die nachfolgende Empfehlung macht Vorschläge zur Berücksichtigung der IT-Sicherheit in Studiengängen an Hochschulen. Die Vorschläge sollen als Rahmenempfehlung interpretiert werden, die die Hochschulen auf ihre jeweilige Situation und Ausrichtung anpassen können. Die inhaltliche Tiefe, die genaue Ausgestaltung, sowie die Art der Vermittlung können abhängig vom Typ der Hochschule und dem jeweiligen Studiengang stark variieren.

In Informatik- und informatiknahen Studiengängen müssen die Studierenden in die Lage versetzt werden, neue Konzepte, Methoden und Werkzeuge der IT-Sicherheit zu entwickeln und zu bewerten, aber auch einzuführen und in der Praxis einzusetzen. Inhaltlich muss die Ausbildung nicht nur die wissenschaftliche und technische Entwicklung berücksichtigen, sondern auch Kenntnisse in Analyse, Entwurf, Qualitätssicherung und Projektmanagement der IT-Sicherheit vermitteln. Dazu müssen Strategien zur Methodenentwicklung, Methodenauswahl, Modellierung und Problemlösung gelehrt werden. In Projekten, auch gemeinsam mit der Wirtschaft, müssen die Studierenden lernen, im Team fächerübergreifend Sicherheitskonzepte und -lösungen zu erarbeiten.

Ziel der Ausbildung in allen Studiengängen, auch in jenen ohne direkten Informatikbezug, muss die Bewusstseinsbildung um die möglichen Risiken und Gefahren der IT-Nutzung und die Vermittlung von Wissen über entsprechende Schutzmechanismen sein. IT-Sicherheit muss in allen Studiengängen als Querschnittsthema mit Anwendungsbezug Berücksichtigung finden.

Bereits in einer frühen Phase der Bachelor-Studiengänge soll ein Basiswissen in IT-Sicherheit vermittelt werden. Ganz allgemein soll der Abschluss eines Bachelorstudiums den Absolventinnen und Absolventen den Berufszugang bzw. den Zugang zu einem Masterstudium eröffnen. Dies bedeutet, dass die inhaltliche Struktur der Studiengänge von Hochschule zu Hochschule verschieden ausfallen kann, je nachdem ob bei der Ausbildung der unmittelbare Einstieg in den Arbeitsmarkt stärker im Vordergrund steht oder ein weitergehendes vertiefendes Studium im Sinne des konsekutiven Studienmodells Bachelor/Master.

Der curriculare Aufbau eines Bachelor-Studiengangs kann daher je nach Gewichtung dieser Ausbildungsziele mehr anwendungs- oder auch mehr grundlagenorientiert erfolgen. Für Master-Studiengänge gilt die in den ländergemeinsamen Strukturvorgaben der KMK enthaltene Verpflichtung zur Differenzierung mit Hilfe der Profiltypen „stärker anwendungsorientiert" bzw. „stärker forschungsorientiert". Die Zuordnung zu einer der beiden Profiltypen kann anhand der vom Akkreditierungsrat beschlossenen Deskriptoren geschehen. Das jeweilige Profil ist bei Auswahl der Inhalte, Form, Ziele und Didaktik der vorgeschlagenen Veranstaltungen entsprechend zu berücksichtigen. (Siehe hierzu auch die Empfehlungen der Gesellschaft für Informatik e.V. für Bachelor- und Masterprogramme im Studienfach Informatik an Hochschulen vom Dezember 2005 und die Standards zur Akkreditierung von Studiengängen der Informatik und interdisziplinären Informatik-Studiengängen an deutschen Hochschulen vom Juni 2000.)

Im Folgenden werden Bachelor- und Master-Studiengänge sowie Informatik als Nebenfach und Lehramt Informatik betrachtet. Weiterhin werden informatikbezogene Studiengänge und nicht-informatikbezogene Studiengänge voneinander abgegrenzt. Die Empfehlung stellt Mindestanforderungen (z.B. Pflichtveranstaltungen) und ggf. vertiefende Inhalte (z.B. Wahlpflichtveranstaltungen, Studienschwerpunkte) dar.

2.1 Bachelor-Studiengänge

2.1.1 Informatikbezogene Bachelor-Studiengänge

Die Vermittlung von Grundkenntnissen in IT-Sicherheit ist in jedem Informatik- oder informatiknahen Studiengang (d.h. Typ 1-3 gemäß den oben genannten GI-Empfehlungen) unerlässlich. In Übereinstimmung mit dem Vorschlag des Fakultätentags Informatik vom 19.11.2004 und den Empfehlungen der GI vom Dezember 2005 wird gefordert, ein verpflichtendes Modul *Einführung in die IT-Sicherheit* in das Curriculum aller Bachelor-Studiengänge aufzunehmen. In dem Modul sollte auf Bezüge zu anderen Basisvorlesungen aus der Informatik geachtet werden und diese entsprechend ergänzen.

Abhängig vom Profil und der Schwerpunktsetzung im Studiengang sollten folgende Inhalte behandelt werden:

- Beispiele von Schadensfällen (Auswirkungen, Ausfälle, Missbrauch)
- Begriffe und Ziele der IT-Sicherheit
- Grundfunktionen sicherer IT-Systeme
- Datenschutz und seine Verknüpfung mit IT-Sicherheit
- Methoden zur Beschreibung sicherer Systeme
- Diagnosemethoden für Software, Hardware und Angriffe; Fehlermodelle, Teststrategien
- Grundlegende Redundanztechniken, Zuverlässigkeitstechniken
- Fehlertoleranz für Hard- und Software
- Mechanismen für Angriffsschutz
- Sicherheitsmanagement

- Risikoanalyse (Bedrohungs- und Schwachstellenanalyse)
- Bewertung von Hard- und Software, Evaluierung, Zertifizierung, Bewertungskriterien
- Rechtliche Aspekte der IT-Sicherheit
- Entwicklung sicherer Systeme

Die Reihenfolge der angeführten Themen, ihre Gewichtung und inhaltliche Ausgestaltung kann je nach Erfahrung und Neigung des Dozenten abgewandelt werden. Eine Aufteilung auf zwei Veranstaltungen ist möglich.

Ist im Bachelor-Studiengang bereits eine Schwerpunktbildung in IT-Sicherheit angestrebt, müssen die Inhalte des einführenden Moduls ergänzt und auf zwei Veranstaltungen verteilt und/oder weiterführende Wahlpflicht-Module angeboten werden. Weiterführende Module sollten sinnvollerweise nicht vor dem vierten Studiensemester in Frage kommen. Abschnitt 2.2.1 enthält Anregungen für mögliche weiterführende Module.

2.1.2 Nicht-informatikbezogene Bachelor-Studiengänge

Die Vermittlung eines grundlegenden Verständnisses für IT-Sicherheit sollte auch in Bachelor-Studiengänge ohne direkten Informatikbezug einfließen. Absolventinnen und Absolventen von Fächern wie Medizin, Betriebswirtschaftslehre, Jura oder Germanistik werden IT-Systeme in ihrem beruflichen Alltag intensiv nutzen, so dass das Wissen über deren Sicherheit auch für diesen Personenkreis von großer Bedeutung ist.

Die IT-Sicherheit ist Querschnitts- bzw. Anwendungsthema, wobei einzelne Aspekte von anderen Bereichen der Informatik, Mathematik, Wirtschaftswissenschaften, aber auch Ingenieurdisziplinen detailliert untersucht und genutzt werden. Abhängig von der Ausrichtung des Studiengangs muss dies bei der Ausgestaltung der Inhalte entsprechend berücksichtigt werden.

Für alle Studiengänge mit intensiver Computernutzung muss ebenfalls ein grundlegendes Lehrangebot für IT-Sicherheit vorhanden sein. Die von Rechenzentren und anderen entsprechenden Institutionen angebotenen Veranstaltungen zur Ausbildung in der Rechner- und Anwendungsnutzung müssen auch auf IT-Sicherheit eingehen. Im Speziellen werden Inhalte aus den einführenden Veranstaltungen aus der Empfehlung für informatikbezogene Bachelor-Studiengänge vorgeschlagen (siehe Abschnitt 2.1.1).

2.2 Master-Studiengänge

2.2.1 Informatikbezogene Master-Studiengänge

In jedem Informatik- oder informatiknahen Master-Studiengang sollte mindestens ein weiterführendes Modul zu IT-Sicherheit im Curriculum verankert werden. Die Vorlesung sollte auf dem bereits im Bachelor-Studium gelehrten Modul *Einführung in die IT-Sicherheit* aufbauen. Es sollen sowohl dort behandelte Themengebiete vertieft als auch zusätzliche Aspekte der IT-

Sicherheit behandelt werden. Vorschläge für weitere Themen und Veranstaltungen finden sich am Ende dieses Abschnittes.

Darüber hinaus wird empfohlen, im Rahmen von informatikbezogenen Master-Studiengängen einen Studienschwerpunkt für IT-Sicherheit anzubieten. Die Ausgestaltung des Studienschwerpunktes wird das Profil des Master-Studiengangs entscheidend prägen und vom Arbeitsschwerpunkt der beteiligten Lehrstühle bestimmt sein. Weiter unten findet sich eine Auflistung über mögliche Module eines Schwerpunkts IT-Sicherheit. Es ist darauf zu achten, dass die angebotenen Veranstaltungen ein ausreichend breites Feld an Themen abdecken, damit je nach Interessenslage der Studierenden ein individueller Fokus im Rahmen des Schwerpunktes möglich ist. Weiterhin ist darauf zu achten, dass Modul-Kombinationen fachlich sinnvoll sind und aufeinander aufbauen, gleichzeitig aber Überschneidungen möglichst vermieden werden. Die Inhalte der aufgeführten Module können – je nach gewünschter Tiefe der Thematik – auf zwei Veranstaltungen verteilt oder in einer Veranstaltung zusammengefasst werden. Ein Studienschwerpunkt in IT-Sicherheit muss um einschlägige Praktika, Seminare und Projekte ergänzt und mit einer Masterarbeit in IT-Sicherheit abgeschlossen werden. Mögliche weiterführende Module sind:

- Kryptologie und ihre Anwendungen
- Fallstudien zur IT-Sicherheit
- Systemsicherheit
- Datenbanksicherheit
- Netz- und Kommunikationssicherheit
- Middleware-Sicherheit
- Sicherheit mobiler Systeme
- Sicherheit im E-Business
- Entwicklung sicherer Systeme
- Formale Spezifikation und Verifikation
- Fehlersimulation
- Diagnoseverfahren
- Fehlertoleranzverfahren
- Rechtliche Aspekte der IT-Sicherheit
- Datenschutzorientierte Technologien
- Sicherheitsstrategie und -management
- Zertifizierung und Evaluation
- Ethische und soziale Aspekte

2.3 Informatik als Nebenfach

Die IT-Sicherheit muss auch im Nebenfach Informatik berücksichtigt werden. Gerade auch Personen, die Informatik und ihre Methoden vorwiegend als Mittel zur Bearbeitung ihrer Aufgaben betrachten, benötigen Kenntnisse der IT-Sicherheit.

2.4 Lehramt Informatik

Da mit der Sensibilisierung für Fragen der IT-Sicherheit bereits in der schulischen Ausbildung begonnen werden muss (siehe Kapitel 3), muss sich die Konzeption des Lehramt-Studiengangs Informatik an den Mindestanforderungen der informatikbezogenen Bachelor-Studiengänge orientieren (siehe Abschnitt 2.1.1). Neben dem Modul *Einführung in die IT-Sicherheit* sollten im Wahlpflichtbereich wenigstens ein bis zwei weiterführende Module angeboten werden.

Für Lehrkräfte, die kein Informatikstudium absolviert haben, ist eine qualifizierte Fortbildung erforderlich, in der die notwendigen Fähigkeiten für die Vermittlung von sicherheitsrelevanten Aspekten in der Schule erworben werden. Im Dienst stehende Lehrerinnen und Lehrer müssen in geeigneten Kursen eine grundlegende Einführung in die IT-Sicherheit erhalten.

3 AUSBILDUNG AN SCHULEN

Die Sensibilisierung für Sicherheitsaspekte in der Informationsgesellschaft sollte bereits in der schulischen Ausbildung verankert werden. Hierzu gehört ein Überblick

- über mehr Chancen durch bessere Sicherheit und über Risiken durch ungenügende Sicherheit,
- über mehr oder weniger zufrieden stellende oder aber nur mit hohem Aufwand zu betreibenden Schutzmöglichkeiten vor Missbrauch oder Versagen.

Die Vor- bzw. Nachteile, die ein (in-)kompetenter Umgang mit Sicherheitsanforderungen mit sich bringt, müssen klar benannt und diskutiert werden. Damit die Schülerinnen und Schüler in diesem Bereich ihre Erfahrungen aufarbeiten können, ist es nötig, motivierende Unterrichtsmaterialien zu entwickeln, die einen hohen Identifizierungsgrad besitzen. Erst durch die direkte Betroffenheit kann eine ernsthafte Auseinandersetzung mit dem Thema Sicherheit erreicht werden. Für interessierte Schülerinnen und Schüler sollten darüber hinaus vertiefende Kursabschnitte im Informatikunterricht der weiterführenden Schulen angeboten werden, in denen überzeugende Themen und Aspekte herausgegriffen und in Projektphasen, z.B. durch Kleingruppen, bearbeitet werden.

3.1 Unterrichtsinhalte für die Schülerinnen und Schüler

In der Schule kann nur ein grundlegendes Verständnis für Sicherheitsbelange geweckt werden. Aktuelle Entwicklungen und weiter gehende Zusammenhänge können erst in einer beruflichen Ausbildung bzw. einem Studium aufgegriffen werden oder bleiben Veranstaltungen vorbehalten, die sich detaillierter und gründlicher mit IT beschäftigen. Dementsprechend sollten im IT-Curriculum der Schule die einzelnen Aspekte der Sicherheit in den verschiedenen Schultypen und Fächern nach Alter und Verständnis der Jugendlichen mit unterschiedlichem Gewicht behandelt werden. Dabei sollen Probleme und deren Lösungsmöglichkeiten möglichst selbstständig erarbeitet werden. Neben dem eigentlichen Informatikunterricht kommt dabei auch den Sozialwissenschaften eine besondere Rolle zu. Sie sind besonders geeignet, gesellschaftliche Bezüge zum Thema Sicherheit herzustellen und seine Auswirkungen auf die Gesellschaft aufzuzeigen.

Beispielhaft könnte behandelt werden:

- Sichere E-Mail-Kommunikation
- Sicherheit bei Online-Auktionen
- Schutz der Privatsphäre im Internet (Regeln in Chaträumen usw.)
- Schadsoftware: Viren, Würmer, Trojanische Pferde
- Wie sichere ich meinen PC?
- Sicherheit technischer Systeme (z. B. spektakuläre Systemausfälle, einfache Redundanztechniken, Zuverlässigkeit von Netzen: Warum kommen Mails manchmal nicht an?)
- Nachverfolgung des individuellen Verhaltens: Kundenkarten, Überwachungskameras, Biometrie, RFID-Technologie, etc.

Dabei sollen im Besonderen Themen angesprochen werden, die die Jugendlichen im täglichen Umgang mit dem Internet und den Informations- und Kommunikationsmöglichkeiten der Neuen Medien wie selbstverständlich einsetzen.

3.1.1 Schwerpunktbildung im Informatikunterricht

Das Fach Informatik wird in den Bundesländern in höchst unterschiedlichem Maß angeboten, sowohl was die Klassenstufen als auch was die Inhalte betrifft. Typischerweise wird Informatikunterricht in allgemeinbildenden Schulformen (Haupt-, Real- und Gesamtschulen und Gymnasien) im Wahlpflichtbereich (8. bis 10. Klasse) und in Grundkursen der gymnasialen Oberstufe, selten auch in Leistungskursen, angeboten - in einigen Bundesländern wie Bayern als Pflichtfach in bestimmten Klassenstufen. An die Forderung der GI nach einem verpflichtenden Informatikunterricht bereits in der Sekundarstufe I wird in diesem Zusammenhang erinnert.

Damit Sicherheit im Informatikunterricht mit Erfolg behandelt und in der Schülerschaft Interesse geweckt werden kann, ist es sinnvoll, mehrere beispielhafte Unterrichtsprojekte, die exemplarisch Schwachstellen aufzeigen, für Informatikkurse vorzubereiten. Themengebiete könnten neben den bereits für die allgemeine Sensibilisierung für Sicherheit genannten Aspekten folgende sein, aus denen exemplarisch ausgewählt werden sollte:

- Ziele der Sicherheit
- technische Grundlagen der Sicherheit
- theoretische Grundlagen (u.a. Kryptographie, Authentisierung z. B. über Passwörter)
- Anwendungen und spezielle Techniken (z.B. eCommerce und elektronisches Geld, biometrische Authentisierungs- und Identifikationssysteme, Chipkarten, Firewalls, Virenscanner, Datensicherung)

Einzelne Themen könnten beispielsweise als Softwareprojekt bearbeitet, als Referat vergeben oder in Gruppen mit unterschiedlichen Rollen diskutiert werden. Praktische, konkret im Unterricht umsetzbare Beispiele sind dabei wichtig.

3.1.2 Einbeziehung in alle anderen Fächer

Ein Grundkonzept zur IT-Sicherheit umfasst typischerweise folgende Themen:

- Aktuelle Themen mit Bezug zur Sicherheit (z. B. Manipulation der Schul-Webseiten, elektronische Wahlen, Missbrauch von E-Mails; Schülerfotos im Internet oder im Schul-Intranet und deren Auswirkungen; Datenflüsse, d.h. die Frage nach den Informationen, die über einzelne Mitglieder der Schulgemeinde (Kinder, Jugendliche, Eltern, Lehrkräfte) im Internet zu finden sind und wie präventiv Missbrauch vorgebeugt werden kann.
- Gesetzliche Regelungen zu Datenschutz und IT-Sicherheit, Urheberrecht (Kopieren von Musiktiteln, korrektes Zitieren, Übernahme von fremden Texten für Referate, etc.). Gerade das unberechtigte Kopieren von Musiktiteln ist z.B. ein Thema, bei dem nur geringes Unrechtsempfinden besteht und das nahezu alle Jugendlichen betrifft.
- Praxisbeispiele: Umgang mit elektronischem Geld, Mobiltelefone, Internet-Auktionen, Vertrauen in Computerergebnisse, Authentizität und Aussagekraft von E-Mails.

Dabei müssen die Themen an die Erfahrungswelt der Schülerinnen und Schüler anknüpfen. Sie könnten beispielsweise folgende Fragen aufgreifen:

- Welche Daten werden während der Internetnutzung von wem gespeichert und warum?
- Warum muss oder darf (während normaler Internetnutzung) ein anderer Rechner (Anbieter, Provider) Zugriff auf meinen Rechner haben – zum Lesen / zum Schreiben / zum Ändern von Daten?
- Was sind Cookies? Wie können sie meinen Rechner gefährden?
- Werden Passwörter, Dateien etc. auch temporär auf der Festplatte gespeichert?
- Was bedeuten Zertifikate?
- Was sind Viren und wie gehe ich damit um?

Inwieweit solch ein Grundkonzept Eingang in die Schule finden kann und wird und die vorgeschlagenen Themen in das Curriculum aufgenommen werden, wird abzuwarten sein. Alle Jugendlichen müssen während ihrer schulischen Ausbildung für das Thema IT-Sicherheit sensibilisiert werden.

3.2 Unterstützung der Lehrkräfte / Materialien

Bedingt durch die fehlende Tradition in Informatik und die hohe Innovationsgeschwindigkeit in der Entwicklung des Fachgebiets sind nur wenige geeignete Unterrichtsmaterialien verfügbar. Erschwerend kommt hinzu, dass wegen der Kulturhoheit der Bundesländer, der Informatikunterricht nicht in allen Ländern den gleichen Stellenwert hat. Umso wichtiger ist ein allgemein verfügbares Internet-Portal, auf dem geeignete Materialien verfügbar sind.

Mit www.lehrer-online.de existiert ein Internet-Forum für Lehrende mit Unterrichtsmaterialien für alle Fächer, Linklisten, etc. In dieses Forum sollten Unterrichtsmaterialien zur IT-Sicherheit eingestellt werden, die didaktisch so aufbereitet werden, dass sie von Lehrkräften einfach übernommen werden können – vorausgesetzt, sie haben eine Basisqualifikation erhalten. Wichtig ist dabei eine fortwährende Pflege, da veraltetes Material von Schülerinnen und Schülern nicht angenommen wird. Eine weitere Bezugsquelle für aktuelle Informationen bietet das Bundesamt für Informationssicherheit mit der Webseite www.bsi-fuer-buerger.de an.

Bezugnahmen:

- Standards zur Akkreditierung von Studiengängen der Informatik und interdisziplinären Informatik- Studiengängen an deutschen Hochschulen (Juni 2000)
  http://www.gi-ev.de/fileadmin/redaktion/empfehlungen/akkreditierung.pdf
- Gesamtkonzept zur informatischen Bildung an Schulen (Juni 2001)
  http://www.gi-ev.de/fileadmin/redaktion/empfehlungen/gesamtkonzept_26_9_2000.pdf
- Memorandum der Gesellschaft für Informatik: Digitale Spaltung verhindern - Schulinformatik stärken! (September 2004)
  http://www.gi-ev.de/fileadmin/redaktion/Presse/gi_memorandum_schulinformatik2004.pdf
- Pressemitteilung: Gesellschaft für Informatik warnt vor digitaler Spaltung - Informatik muss in jeder Schule gelehrt werden! (November 2004)
  http://www.gi-ev.de/presse/pressemitteilungen-thematisch/pressemitteilung-vom-22-november-2004/
- Empfehlungen der Gesellschaft für Informatik e.V. (GI) zu Bachelor- und Masterprogramme im Studienfach Informatik an Hochschulen (Dezember 2005)
  http://www.gi-ev.de/fileadmin/redaktion/empfehlungen/GI-Empfehlung_BaMa2005.pdf

Mitglieder des GI AK Sicherheit in der Ausbildung:
Rüdiger Dierstein, Jana Dittmann, Felix Freiling, Karl Großpietsch, Anja Hartmann, Michael Höllen, Jan Jürjens, Peter Löhr, Isabel Münch (stv. Sprecherin), Jens Nedon, Günther Pernul (Sprecher), Hartmut Pohl, Daniel Scheibler, Monika Schulte, Gerhard Weck, Hiltrud Westram, Cornelia Winter

Ansprechpartner:
Prof. Dr. Günther Pernul
Universität Regensburg
Lehrstuhl für Wirtschaftsinformatik I - Informationssysteme
guenther.pernul@wiwi.uni-regensburg.de

Kontakt:
Gesellschaft für Informatik e.V. (GI)
Ahrstraße 45
53175 Bonn
gs@gi-ev.de
www.gi-ev.de