FAKULTÄT FÜR !NFORMATIK

Informationssicherheit in Schulen mit besonderem Augenmerk auf die Anwenderschulung

MAGISTERARBEIT

zur Erlangung des akademischen Grades

Magister der Naturwissenschaften

im Rahmen des Studiums

Lehramt Informatik und Informatikmanagement

eingereicht von

Martin Gruber
Matrikelnummer 0325487

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung:
Betreuer: Ao. Univ. Prof. Dipl.-Ing. Dr. techn. Gerald Futschek

Wien, 08.05.2009

(Unterschrift Verfasser) (Unterschrift Betreuer)

Danksagungen

Das Verfassen meiner Diplomarbeit ist mir durch die Unterstützung einer Vielzahl von Menschen ermöglicht worden. Ganz besonders möchte ich mich bei folgenden Personen bedanken:

Für die Übernahme dieses Themas und die Betreuung bei der Abfassung meiner Arbeit bedanke ich mich recht herzlich bei Ao. Univ. Prof. Dipl.-Ing. Dr. techn. Gerald Futschek.

Ebenso waren die Diskussionen im Diplomandenseminar immer wieder sehr anregend.

Auch meinen Interviepartnern sei an dieser Stelle gedankt.

Bedanken möchte ich mich bei meiner ganzen Familie für die ständige Unterstützung ihrerseits. Allen voran meinen Eltern, Berta und Gerhard Gruber, zu denen ich immer mit allen Problemen kommen konnte, und die mir nicht nur durch finanzielle Unterstützung den Abschluss meines Studiums ermöglicht haben.

Dank gilt auch meinen Studienkollegen, allen voran Rudolf Langer, Martin Schedlbauer und Philipp Prinzinger. Ohne sie wäre das Studium nur der halbe Spaß gewesen.

Ganz besonders möchte ich mich auch bei meiner Lebensgefährtin Stefanie Kauer bedanken. Ihrer Motivationskunst ist es zu verdanken, dass ich diese Arbeit doch noch rechtzeitig fertigstellen konnte.

Martin Gruber
Alser Straße 16/7
1090 Wien

„Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe."
Wien, den 12. Mai 2009

Martin Gruber

Kurzfassung

Computersicherheit und Informationssicherheit sind Themen, die über die letzten Jahre immer mehr an Bedeutung gewonnen haben. Meine Arbeit beschäftigt sich mit der Informationssicherheit in österreichischen Schulen.
Ausgehend von der Frage der Notwendigkeit von Informationssicherheit für das Funktionieren der IT untersuche ich, durch qualitative empirische Interviews mit IT-Administratoren an Schulen, die Bedeutung von Informationssicherheit in österreichischen Schulen. Im Rahmen der Analyse der Interviews nach der „grounded-theory“ von Strauss wird erarbeitet, dass die klassischen Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit durch ein umfassendes und vollständiges Informationssicherheitsmanagementsystem (ISMS) sichergestellt werden können. Teil eines solchen Systems sind die Anwenderschulung und -sensibilisierung. Dabei kommt es in Schulen zum Problem der Heterogenität der Anwendergruppen Schüler und Lehrer. Dies wird durch eine differenzierte Schulung gelöst und fließt auch in die Ausarbeitung der Curricula zur Schulung von Lehrern und Schülern ein.

Abstract

Computer security and information security have gained importance over the last several years. My thesis engages with information security in Austrian schools.
The initial question of my study is the need of information security for the successful operation of IT-systems. Based on this question, I investigate the importance of information security in Austrian schools, using qualitative empiric interviews with people responsible for IT in schools. Within the analysis of the interviews, following the grounded theory by Strauss, it is acquired, that the classical security targets availability, integrity and confidentiality can be reached by applying a broad and complete information security management system (ISMS). An important part of an ISMS is raising the awareness of users and training them towards security interests. Within the training of users the problem of heterogeneous groups arises. It is solved by distinguishing different methods and contents for training teachers and pupils. It also influences the development of curricula for pupils and teachers.

Inhaltsverzeichnis

Danksagungen **iii**

Kurzfassung **v**

Abstract **v**

Abbildungsverzeichnis **ix**

1 Einführung **1**
1.1 Motivation 1
1.2 Zielsetzung und Forschungsfragen 3
1.3 Aufbau und Kapitelübersicht 3

2 Grundlagen **5**
2.1 Grundlagen der Informationssicherheit 5
2.1.1 Grundbegriffe der Informationssicherheit 5
2.1.2 Anforderungen an IT-Sicherheit 7
2.1.3 Bedrohungen 8
2.2 Methodische Grundlagen 10
2.2.1 Qualitative Forschungsmethoden 10
2.2.2 Durchführung 10
2.2.3 Auswertung 11

3 Analyse **13**
3.1 Vorbereitungen 13
3.1.1 Problemanalyse 13
3.1.2 Leitfadenkonstruktion 14
3.1.3 Pilotphase 16
3.2 Durchführung 17
3.2.1 Zeitraum und Auswahl der Interviewpartner 17
3.2.2 Anmerkungen 18
3.3 Auswertung 18
3.3.1 Transkription 18
3.3.2 Kodierung 19
3.3.3 Interpretation 22

3.3.4 Hypothesen . . . 24
3.3.5 Zusammenfassung . . . 25

4 Informationssicherheitsmanagement 27
4.1 Vorüberlegungen . . . 27
4.1.1 Ziele und Aufgaben eines ISMS . . . 28
4.2 Durchführung . . . 28
4.2.1 Informationssicherheitspolitik . . . 28
4.2.2 Risikoanalyse . . . 31
4.2.3 Sicherheitskonzept . . . 33
4.2.4 Umsetzung . . . 34
4.2.5 Laufender Betrieb . . . 36

5 Anwendersensibilisierung und -schulung 39
5.1 Vorüberlegungen zur Curriculumsentwicklung . . . 39
5.1.1 Lehrer . . . 39
5.1.2 Schüler . . . 40
5.2 Curriculum Schüler . . . 40
5.2.1 Lernorganisation . . . 40
5.2.2 Lerninhalte . . . 41
5.2.3 Lernziele . . . 42
5.3 Curriculum Lehrer . . . 43
5.3.1 Lernorganisation . . . 43
5.3.2 Lerninhalte . . . 43
5.3.3 Lernziele . . . 44
5.4 Beispiel: Passwortsicherheit . . . 45
5.4.1 Didaktische Vorüberlegungen . . . 45
5.4.2 Wahl einer Methode . . . 46
5.4.3 Schulung für Lehrer . . . 47
5.4.4 Schulung für Schüler . . . 50
5.4.5 Unterschiede . . . 51

6 Schlussbetrachtungen 53
6.1 Ergebnisse der Arbeit . . . 53
6.2 Diskussion und Ausblick . . . 54

A Leitfaden zur Durchführung der Interviews 57

B Transkription 59

Literatur 76

Abbildungsverzeichnis

2.1 Abfolge der nötigen Schritte bei der Durchführung eines Leitfaden-Interviews 11

3.1 Ergebnis eines ersten Brainstormings zum Thema Informationssicherheit 14
3.2 Einteilung des Ergebnisses des Brainstormings und Zuordnung der einzelnen Begriffe zu den Themenblöcken 15
3.3 Beziehung der Kategorien untereinander 16
3.4 Zusammenhänge der Kategorien 20

4.1 Abfolge der notwendigen Schritte zur Implementierung eines ISMS in zeitlicher Reihenfolge nach [OeSiH] 29
4.2 Schichten des IT-Grundschutzmodells nach [GSHB] 32
4.3 Auffindung des Optimalpunkts hinsichtlich der Kosten-Nutzen Relation bei der Wahl von Sicherheitsmaßnahmen 33

5.1 Startbildschirm beim Einloggen in die Schulung für Lehrer 48
5.2 Überprüfung des Lernerfolgs für Lehrer 49
5.3 Startbildschirm beim Einloggen in die Schulung für Schüler 51

„An allem Unfug, der passiert, sind nicht etwa nur die schuld, die ihn tun, sondern auch die, die ihn nicht verhindern.“ - Erich Kästner[1]

[1]Erich Kästner, deutscher Schriftsteller, in: „Das fliegende Klassenzimmer“

Kapitel 1

Einführung

1.1 Motivation

Über die letzten Jahrzehnte hinweg ist die Abhängigkeit der Menschen von der Informationstechnologie immer größer geworden. Dabei hat die Zahl der Attacken auf Computersysteme in den letzten Jahren stets zugenommen. Täglich werden zig Angriffe auf PCs gestartet. Wird ein ungeschützter PC nur wenige Minuten lang mit dem Internet verbunden, so kann dieser bereits mit Schadcode infiziert sein[1]. Dabei muss es sich nicht einmal um ein System einer großen Firma handeln, es müssen nicht einmal irgendwelche lohnenden Informationen auf dem Rechner gespeichert sein. Oft reicht es den Angreifern[2] bereits, den „eroberten“ Computer für weitere Zwecke zu nutzen. Je wertvoller die verarbeiteten Informationen jedoch sind, umso interessanter wird deren Inhalt für Angreifer.

Trotz der steigenden Anzahl der Angriffe wird der Informationssicherheit, vor allem in kleinen und mittleren Unternehmen (KMU)[3], und dazu gehört meiner Meinung nach auch ein Großteil der österreichischen Schulen, immer noch zu wenig Aufmerksamkeit zugemessen.

Für die meisten Menschen ist es mittlerweilen selbstverständlich geworden, im alltäglichen Leben Risiken zu minimieren. So sperrt man etwa seine Wohnungstür nach dem Verlassen ab, um Einbrüche zu verhindern oder man benützt beim Autofahren den Sicherheitsgurt, um seine Gesundheit im Falle eines Unfalls zu schützen. Umso erstaunlicher ist es oft, wie leichtfertig viele Menschen mit Informationen, seien es nun

[1] Vgl. derStandard.at, „Ein ungepatchter Windows-PC überlebt vier Minuten im Netz“, 15. 7. 2008. Online erhältlich via URL: <http://derstandard.at/?id=3414847&sap=2&_pid=10071314> (16. April 2009).

[2] Aus Gründen der Lesbarkeit soll in dieser Arbeit auf die Verwendung einer geschlechterspezifischen Form verzichtet werden. Wird im Folgenden von Angreifern, Administratoren, Anwendern usw. gesprochen, so soll immer das grammatikalische, nicht das natürliche Geschlecht gelesen werden.

[3] Vgl. pressetext.austria, „IT-Security: Situation bei KMUs 'desaströs'“, 3. 4. 2008. Online erhältlich via URL: <http://pressetext.at/news/080403037/it-security-situation-bei-kmus-desastroes/> (16. April 2009).

persönliche Daten oder Daten die im Zuge ihrer Arbeitstätigkeit verarbeitet werden, umgehen. Beispielsweise gibt es in Unternehmen immer noch viele Benutzer die ihr Passwort auf einem kleinen gelben Zettel am Monitor kleben haben oder Jugendliche die allzu sorglos mit ihren privaten Informationen auf Social Networking Plattformen im Internet umgehen.

Aus diesen Gründen erhält das Thema Informationssicherheit für viele Menschen eine immer größere Bedeutung.

Dass die Informationssicherheit auch im Bildungsbereich ein nicht unwichtiges Thema ist, sollen die beiden folgenden Zitate belegen. Das erste der beiden wurde dem im April 2009 veröffentlichten Symantec Global Internet Security Threat Report [ISTR] für das Jahr 2008 entnommen:

> „Identity theft continues to be a high-profile security issue, particularly for organizations that store and manage large amounts of personal information. Based on the most recent information available from 2007, roughly 8.4 million U.S. residents were victims of identity theft, which represents approximately 3 percent of the adult population. Not only can compromises that result in the loss of personal data undermine customer and institutional confidence, result in costly damage to an organization's reputation, and be costly for individuals to recover from the resulting identity theft, they can also be financially costly to organizations. In 2008, the average cost per incident of a data breach in the United States was $6.7 million, an increase of 5 percent from 2007, and lost business amounted to an average of $4.6 million. Also, organizations can be held liable for breaches and losses, which may result in fines or litigation. [...]In 2008, the education sector represented the highest number of known data breaches that could lead to identity theft, accounting for 27 percent of the total“[4]

Im Jahr 2007 fielen also viele US-Bürger dem Datendiebstahl personenbezogener Daten zum Opfer. Davon passierten mehr als ein Viertel im Bereich des Erziehungssektors. Doch die USA sind dabei nicht die Ausnahme. In Österreich sind die Verwaltungsnetze von Schulen ebenso das Ziel von Hackern, was folgender Auszug aus dem IT Weblog des Landesschulrats für Niederösterreich belegt:

> „Auf Grund von aktuellen Hackerangriffen an Schulen, weisen wir nochmals auf Erlass Präs.-4114/26-2006 hin, in dem darauf hingewiesen wird, dass das Verwaltungsnetz aus sicheheitstechnischen [sic!] Gründen vom Pädagogischen Netz zu trennen ist! (Firewall etc.)[...] Aktuelle Hackerprogramme ermöglichen u.a. das ausspionieren von Passwörtern auf Windows-Rechnern, daher möchten wir auf die Hilfe und Supportseite von Microsoft verweisen, auf der beschrieben wird, wie dieses Auslesen von Passwörtern erschwert bzw. unmöglich gemacht wird.“[5]

[4] Vgl. Symantec Corporation, „Symantec Global Internet Security Threat Report“, 2009, S. 19f.

[5] Vgl. IT Weblog des LSRNOE, "Hackerangriffe und Sicherheitshinweise", 4. 4. 2008. Online erhältlich via URL: `<http://itblog.lsr-noe.gv.at/?p=36>` (16. April 2009).

Im Rahmen dieser Arbeit möchte ich mich deshalb speziell mit der Informationssicherheit an österreichischen Schulen beschäftigen. Aufgrund der Vielzahl unterschiedlicher Schultypen muss hierbei allerdings eine Einschränkung auf allgemeinbildende (AHS) sowie berufsbildende (BHS) höhere Schulen vorgenommen werden.

1.2 Zielsetzung und Forschungsfragen

Durch qualitative Interviews mit IT-Administratoren an österreichischen Schulen möchte ich herausfinden, welche Bedeutung der Informationssicherheit an den heimischen Schulen derzeit zugemessen wird. Was wird unternommen bzw. welche Punkte werden bei der Planung der IT-Sicherheit berücksichtigt? Gibt es überhaupt eine Art Informationssicherheitsmanagement an den Schulen? Sind schon sicherheitsrelevante Ereignisse geschehen?
Aufbauend auf den Ergebnissen der Befragung möchte ich mir die Frage stellen, wie ein Informationssicherheitsmanagementsystem in Schulen umgesetzt werden kann. Weiters interessiert mich in diesem Zusammenhang auch die Bedeutung der Anwenderschulung bei der Umsetzung von IT-Sicherheit. Gibt es dabei Unterschiede bei der Schulung von Lehrern und Schülern und wie können diese überhaupt hinsichtlich IT-Sicherheit sensibilisiert werden?

Meine Überlegungen und Ausführungen bei dieser Arbeit werden also von folgenden Forschungsfragen geleitet:

- Welche Bedeutung wird der Informationssicherheit an österreichischen Schulen zugemessen?
- Wie kann die Herstellung von Informationssicherheit an österreichischen Schulen gewährleistet und systematisiert werden?
- Was muss getan werden, damit die Anwender (also Schüler und Lehrer) hinsichtlich der Informationssicherheit geschult und sensibilisiert werden?
- Welche Inhalte müssen Lehrern und Schülern hinsichtlich der Informationssicherheit vermittelt werden und was ist ein geeigneter Rahmen dafür?

1.3 Aufbau und Kapitelübersicht

Ohne Grundlagen über Informationssicherheit zu sprechen, erscheint mir nicht als sinnvoll. Daher werden in Kapitel 2 zunächst die Grundlagen für das Folgende gelegt. Zuerst werden wichtige Begriffe der Informationssicherheit definiert. Danach wird auf die unterschiedlichen aktuellen Anforderungen, seien sie nun informationstechnisch oder rechtlich, und auf aktuelle Bedrohungen der IT-Sicherheit eingegangen.
Es werden auch Grundlagen der von mir angewandten Methodik, dem qualitativen Interview, dargelegt.

In Kapitel 3 wird die Analyse der Bedeutung von Informationssicherheit an österreichischen Schulen durchgeführt. Dazu wird zuerst ein Leitfaden für die folgenden Interviews entwickelt. Danach soll kurz über die Durchführung der Interviews berichtet werden.
Schlussendlich wird eine Auswertung und Interpretation der geführten Interviews nach dem „grounded-theory“-Ansatz von A. L. Strauss durchgeführt.

In Kapitel 4 wird, aufbauend auf dem Österreichischen Informationssicherheits-Handbuch [OeSiH] und den Ergebnissen der durchgeführten Interviews, die Implementierung eines Informationssicherheitsmanagementsystems in Schulen beschrieben. Zuerst werden die Ziele eines solchen Systems angeführt, danach werden die dazu notwendigen Schritte beschrieben. Dabei soll auch die Wichtigkeit der Anwenderschulung und -sensibilisierung im Rahmen des Informationssicherheitmanagementsystems dargelegt werden.

In Kapitel 5 werden zuerst Vorüberlegungen zur Erstellung eines Curriculums zur Anwenderschulung hinsichtlich der Informationssicherheit in Schulen durchgeführt. Danach soll sowohl für die Schulung der Schüler als auch für die Schulung der Lehrer ein eigenes Curriculum entwickelt werden.
Die Unterschiede bei der Schulung von Lehrern und Schülern sollen danach am Beispiel Passwortsicherheit verdeutlicht werden. Dazu werden zunächst didaktische Überlegungen zum Einsatz einer eLearning Plattform durchgeführt. Danach werden die Inhalte zum Thema Passwortsicherheit dargelegt.

Kapitel 6 fasst schlussendlich die erzielten Ergebnisse zusammen. Außerdem wird meine Arbeit diskutiert und ein möglicher weiterer Forschungsverlauf in Ausblick gestellt.

Kapitel 2

Grundlagen

Ziel dieses Kapitels ist es sowohl Grundlagen der Informationssicherheit als auch methodische Grundlagen darzulegen. Zunächst sollen wichtige Begriffe der Informationssicherheit definiert und erklärt werden und Anforderungen an die IT-Sicherheit dargestellt werden. Danach soll auf die in der Arbeit verwendete Methodik eingegangen werden.

2.1 Grundlagen der Informationssicherheit

2.1.1 Grundbegriffe der Informationssicherheit

Um über Informationssicherheit zu sprechen, muss zunächst einmal der Begriff der Sicherheit definiert werden. Jeder Mensch hat eine Idee über den Begriff Sicherheit: Im Straßenverkehr meint man mit Sicherheit die Vermeidung von Unfällen, im Zusammenhang mit Kriminalität etwa die Verhinderung bzw. die Minimierung der Wahrscheinlichkeit eines Einbruchs und im Hinblick auf die finanzielle Sicherheit wird auf Wahrung der Liquidität geachtet.

Egal in welchem Kontext man Sicherheit betrachtet, der gemeinsame Nenner ist immer die Vermeidung bzw. die Minimierung von Risiken. Daraus folgt

Definition 2.1 *Sicherheit ist die Minimierung der Risiken.*

Dabei versteht man unter Risiko den Erwartungswert des Schadens. Also

Definition 2.2 *Risiko = Schaden * Eintrittswahrscheinlichkeit.*

Wir haben nun also Sicherheit im Allgemeinen definiert. Bevor wir nun den Zusammenhang mit Informationstechnologie (IT) herstellen, muss noch der Begriff der „Information“ präzisiert werden.

In der Informationstechnik werden Daten verarbeitet. Daten sind prinzipiell bloß eine Aneinanderreihung von Zeichen. Erst die Interpretation durch Menschen in einem Kontext gibt ihnen einen Sinn. Daher lässt sich Information folgendermaßen definieren:

Definition 2.3 *Informationen sind durch Menschen in einen Kontext gebrachte Daten.*

Im Zusammenhang mit Informationstechnologie gilt es, viele unterschiedliche Risiken zu minimieren. So sind zum Beispiel der Verlust von Daten, der Ausfall von Hardware, ein im System befindlicher Virus als auch ein Stromausfall Risiken für den Betrieb eines IT-Systems. Die Art dieser Bedrohungen ist dabei recht unterschiedlich.

Welche spezifischen Bedürfnisse an die Sicherheit haben nun IT-Systeme? Grundsätzlich werden von IT-Systemen die Verlässlichkeit und die Beherrschbarkeit gefordert. Dies lässt sich durch Erfüllen von Schutzzielen sicherstellen.
In der Literatur finden sich zur Gewährleistung der Verlässlichkeit folgende Schutzziele:

- Vertraulichkeit (confidentiality)
- Integrität (integrity)
- Verfügbarkeit (availability)

Unter den Begriff der Beherrschbarkeit fallen folgende Schutzziele:

- Authentizität (authenticity)
- Nichtabstreitbarkeit (non-repudiation)

Um ein besseres Verständnis dieser Begriffe zu gewährleisten sollen sie im Folgenden genauer erklärt werden.
Unter *Vertraulichkeit* wird im Allgemeinen verstanden, dass die Daten eines IT-Systems nicht an Unbefugte gelangen dürfen. Insbesondere gilt dies für vertrauliche Informationen wie personenbezogene Daten, Betriebsgeheimnisse usw. Im Zusammenhang mit der Vertraulichkeit von Daten spielen Verschlüsslungen und Zugriffsschutz eine große Rolle.
Daten werden dann als integer bezeichnet, wenn sie vollständig und unversehrt sind. Durch die *Integrität* von Daten soll also gewährleistet werden, dass die Daten unverfälscht vorliegen und nur von befugten Personen verändert werden dürfen. Um dies zu gewährleisten ist eine gute Backup-Strategie von Bedeutung. Weiters erfordert die Erfüllung dieses Schutzziels Zugriffsschutz um die Daten vor Manipulation zu schützen. Dies wird etwa durch eine restriktive Rechtevergabe erreicht.
Ein IT-System ist dann *verfügbar*, wenn sichergestellt ist, dass es für die Anwender ordnungsgemäß funktioniert. Dies lässt sich prozentuell darstellen. Dazu betrachtet man den Anteil der Up-Time, also jene Zeit, in der eine Komponente korrekt läuft, an der Gesamtlaufzeit der Komponente. Also

$$Verfügbarkeit\ einer\ Komponente = \frac{Up - Time}{Gesamtlaufzeit}\%$$

Die Verfügbarkeit des gesamten IT-Systems ist dann einfach das Produkt der Verfügbarkeiten der einzelnen Komponenten:

$$Verfügbarkeit\ eines\ IT-Systems = \prod Verfügbarkeit\ der\ einzelnen\ Komponenten$$

Durch die *Authentizität* und die *Nichtabstreitbarkeit* soll einerseits die Echtheit und andererseits der Ursprung von Daten gewährleistet werden.

2.1.2 Anforderungen an IT-Sicherheit

Wir kennen nun die Schutzziele im Hinblick auf IT-Sicherheit. Nun sollen die verschiedenen Anforderungen an die Sicherheit näher betrachtet werden. Zuerst sollen allgemeine informationstechnische und rechtliche Anforderungen angesprochen werden. Danach wird auf schulspezifische Anforderungen eingegangen.

Informationstechnische Anforderungen
Ein großes Problem hinsichtlich der informationstechnischen Anforderungen ist die rasche Fortentwicklung in der IT.
Nach dem Moorschen Gesetz verdoppelt sich die Anzahl der Transistoren auf einem Chip alle zwei Jahre. Damit steigern sich die Rechengeschwindigkeit, die Speicherkapazität und die Miniaturisierung von Chips. Gleichzeitig werden IT-Komponenten preislich immer günstiger. Durch diese rasche Entwicklung fällt es den Benutzern von IT-Systemen nicht immer leicht auf dem neuesten Stand der Technik zu sein.
Doch auch im Bereich der Software steigt die Komplexität immer weiter an. Programmierer sind dazu angehalten, neue Produkte bzw. neue Versionen von Produkten so schnell als möglich zu veröffentlichen. Dies resultiert einerseits in zahlreichen Updates und Patches und andererseits in der Gefahr, dass ein Programm unbeabsichtigt Sicherheitslücken öffnet.

Die daraus folgenden informationstechnischen Bedrohungen sind breit gestreut. Unbeabsichtigte Gefahren (Fehler bei der Übertragung von Daten, Bedienungsfehler, höhere Gewalt, ...) sind ebenso möglich wie informationstechnische Angriffe. Diese lassen sich in zwei Kategorien einteilen: aktiv und passiv.
Bei passiven Angriffen werden vom Angreifer keine Änderungen an einem System vorgenommen. Schaden entsteht dabei z.B. durch Abhören oder Mitlesen von Verbindungen. Aktive Angriffe erfordern jedoch Eingriffe oder Änderungen in einem System. Dabei kommt oft schädliche Software (Malware) wie Viren, Würmer, Trojaner oder Spyware zum Einsatz.

Rechtliche Anforderungen
Neben den informationstechnischen Anforderungen sind vor allem auch rechtliche Anforderungen zu erfüllen. Der Unternehmensleiter ist verantwortlich für die Einhaltung

der Sorgfaltspflicht. Werden in einem Unternehmen oder einer Behörde personenbezogene Daten verarbeitet, so kommt auch das „Bundesgesetz über den Schutz personenbezogener Daten“ (DSG2000)[1] zum tragen. Eng verbunden mit dem Datenschutz ist auch die Wahrung des Fernmeldegeheimnisses, welche im Telekommunikationsgesetz (TKG 2003)[2] geregelt ist. Sollte ein Zuwiderhandeln gegen diese Anforderungen festgestellt werden, so kommen auch, je nach Vergehen, Haftungs-, Zivil- und Strafrecht zur Geltung.

Schulspezifische Anforderungen
In Schulen werden im Bereich der Verwaltung personenbezogene Daten verarbeitet. Diese sind, laut Angaben von Sicherheitsverantwortlichen in Schulen, besonders schützenswert.
Sowohl Lehrer als auch Schüler nutzen im Schulalltag beinahe täglich Arbeitsstationen von immer größer und komplexer werdenden Schulnetzwerken. Die dabei eingesetzten Geräte reichen von klassischen PCs über Notebooks und Projektoren bis hin zu für den Schulbetrieb wichtigen Servern. Diese IT-Infrastruktur gilt es zu Verwalten und aktuell zu halten.
Wichtig dabei ist allerdings auch die Mitarbeit der Schüler und Lehrer und damit eine auf deren Bedürfnisse abgestimmte Sensibilisierung im Hinblick auf IT-Sicherheit.

Standards in der IT-Sicherheit
Aufgrund der unterschiedlichen Anforderungen an die IT-Sicherheit ist ein Kriterienkatalog zur Umsetzung in Betrieben bzw. Behörden von großer Bedeutung. Aus diesem und anderen Gründen wird seit Jahren mit unterschiedlichen Ansätzen versucht, Standards zur Implementierung von IT-Sicherheit zu entwickeln.
International anerkannt sind dabei die Bestrebungen des bereits 1990 gegründeten Bundesamts für Sicherheit in der Informationstechnik (BSI) in Deutschland. 1995 wurde vom BSI zum ersten Mal eine Sammlung von Erfahrungen unter dem Titel „IT-Grundschutzhandbuch“ (GSHB) veröffentlicht. Seit 2005 heißt diese Sammlung „IT-Grundschutzkataloge“. Darin wird eine Methode zur Einführung eines Informationssicherheitsmanagements beschrieben. Dazu wird vom BSI eine umfassende Sammlung von Bausteinen und Maßnahmen zur Einrichtung und Aufrechterhaltung zur Verfügung gestellt.
Aufbauend auf den IT-Grundschutzkatalogen des BSI wurde in Österreich im Auftrag des Bundeskanzleramts ein „Österreichisches Informationssicherheits-Handbuch“ [OeSiH] entwickelt, auf das ich mich im Weiteren auch beziehen werde.

2.1.3 Bedrohungen

Nachdem nun der Begriff der Sicherheit definiert wurde und die unterschiedlichen Anforderungen an die IT-Sicherheit bekannt sind, soll nun auf die für die für IT-Systeme

[1] Vgl. http://www.dsk.gv.at/site/6229/default.aspx
[2] Vgl. http://www.bmvit.gv.at/telekommunikation/recht/aut/gesetze/tkg.html

relevanten Bedrohungen eingegangen werden. Bei der Vielzahl an informationstechnischen Bedrohungen sollten aber nicht elementare Gefahren vergessen werden. Durch Feuer, Wassereinbruch (Wasserrohrbruch, Hochwasser, usw.), Erdbeben, Blitzschlag, Sturm und andere Katastrophen ist die Sicherheit der IT ebenso gefährdet wie etwa durch Hackerangriffe.

Technische Bedrohungen können sowohl von internen als auch von externen Personengruppen ausgehen. Bei internen Personen müssen dabei nicht einmal vorsätzliche Handlungen vorliegen. Alleine durch Fehlbedienung und das Ignorieren der Sicherheitsrichtlinien kann beträchtlicher Schaden entstehen.

Das Spektrum der Angriffsarten von externen Personen ist groß. Dabei sind die Ziele der Angreifer unterschiedlich. Das Ziel einer *Denial of Service* (DoS) Attacke ist es, ein gewisses System oder ein gewisses Service stillzulegen. Die Lahmlegung eines Servers etwa kann für ein Unternehmen weitreichende Folgen haben. Ziel einer *Code Injection* ist es, eigenen Code in ein System einzuschleusen, um dort beliebige Befehle ausführen zu können. Dies ist für Angreifer sehr attraktiv. Erreicht werden kann Code Injection etwa durch Buffer Overflows oder Command Injection (etwa SQL Injection in Websites). Weitere Angriffsarten sind Man in the Middle Attacken, Spoofing, Session Hijacking, Poisoning, Flooding usw.

In den Medien wird hauptsächlich über die Bedrohung durch *Malicious Content* berichtet. Unter diesen Begriff fallen sowohl Viren, Würmer, Trojaner und Rootkits als auch SPAM und Phishing. Würmer verbreiten sich mittlerweilen mit sehr hoher Geschwindigkeit auf ungepatchten Rechnern. Seit Oktober 2008 verbreitet sich etwa der „Conficker"-Wurm rasant auf Windows-Systemen:

> „Nach Angaben der Antiviren-Spezialisten F-Secure sind bisher neun Millionen Windows-Rechner vom Conficker-Wurm befallen. Extrem bedenklich erscheint die rasante Verbreitung: innerhalb von vier Tagen stieg die Zahl der infizierten PCs von 2,4 Millionen auf 8,9 Millionen an. Der Wurm ist auch unter dem Namen Downadup bekannt und nistet sich über eine Sicherheitslücke in Windows-Betriebssystemen ein. Microsoft hat dieses Leck zwar bereits geschlossen, dennoch breitet sich Conficker rasant aus."[3]

Durch Kevin Mitnick[4] wurden *Social Engineering* Angriffe bekannt. Darunter versteht man Methoden um Menschen derart zu beeinflussen, sodass sie für den Angreifer handeln. Meist werden dabei Eigenschaften wie Hilfsbereitschaft, Vertrauen oder Autorität ausgenutzt. Unter den Begriff des Social Engineerings fallen auch Dumpster Diving (Durchsuchen des Abfalls nach Informationen) und Shoulder Surfing (Ausspähen von Daten durch „über die Schulter schauen").

[3] DiePresse.com, "Conficker-Wurm wütet: Neun Millionen Computer infiziert", 23. 1. 2009. Online erhältlich via URL: `<http://diepresse.com/home/techscience/internet/sicherheit/446338>` (24. März 2009).

[4] Kevin Mitnick, ehemaliger US-amerikanischer Hacker, heute Geschäftsführer einer Sicherheitsfirma

2.2 Methodische Grundlagen

2.2.1 Qualitative Forschungsmethoden

Um das Verhalten bzw. die Erfahrungen von Menschen in bestimmten Handlungsfeldern (z.B.: Arbeitsplatz) zu erforschen, bieten sich qualitative Methoden an. Im Gegensatz zur quantitativen Forschung zählt nicht die Zahl der befragten Personen, vielmehr ist es wichtig, typische Fälle auszuwählen. Bei der qualitativen Forschung stehen dabei die Prinzipien von Offenheit und Flexibilität im Vordergrund. Die dafür eingesetzten Verfahren reichen von Interviews über Gruppendiskussionen bis hin zu teilnehmender Beobachtung.
Für die Befragung von IT-Sicherheitsverantwortlichen an Schulen habe ich mich in diesem Zusammenhang für ein sogenanntes Leitfaden-Interview entschieden. Dabei handelt es sich um eine Befragungstechnik, bei der im Vorhinein festgelegte Fragen gestellt werden. Diese können vollkommen offen beantwortet werden, es werden also keine Antwortmöglichkeiten vorgegeben. Dies sollte dazu führen, dass die interviewten Personen völlig frei berichten, kommentieren und erklären können. Der Interviewer hat in diesem Fall also nur die Aufgabe, das Interview durch den Leitfaden zu steuern und wenn es sich anbietet Ad-hoc-Fragen zu stellen.
Der große Vorteil dieser Art von Interviews ist, dass die durch den Fragenkatalog vorgegeben Fragen beantwortet werden und möglicherweise zusätzlich, durch die offene Art der Fragestellung begünstigt, noch neue Aspekte auftreten, die der Forscher im Vorhinein vielleicht noch gar nicht bedacht hat.

2.2.2 Durchführung

Beim Leitfadeninterview geht man wie in Abbildung 2.1 dargestellt vor.
In der Phase der Problemanalyse muss man sich der Fragestellung seines Projektes bewusst werden. Um einen ersten Überblick über das Thema zu gewinnen bietet sich ein Brainstorming an. Dabei ist die Erstellung einer Mindmap überaus hilfreich. Mit Hilfe dieser gilt es nun geeignete Leitfragen für das Interview zu erstellen.
Bei der Leitfadenkonstruktion sollte darauf geachtet werden, dass Fragen möglichst kurz und verständlich formuliert sind. Damit will man etwaige Nachfragen des Interviewten unterbinden. Auch Suggestivfragen sollten vermieden werden.
In der Pilotphase wird der Leitfaden auf die Tauglichkeit geprüft. Dazu führt man einen Pretest des Interviews mit einer geeigneten Person durch. Werden Mängel in der Fragestellung festgestellt, so muss diese nochmals überarbeitet werden. Ansonsten kann das eigentliche Interview durchgeführt werden.
Mit Einverständnis des Befragten sollte das Interview auf Tonband aufgezeichnet werden. Das Interview wird mit sogenannten Sondierungsfragen begonnen. Dabei handelt es sich um Einstiegsfragen. Man will dadurch eine angenehme Atmosphäre schaffen und herausfinden, welche Bedeutung das Thema für den Interviewten hat. Danach kann mit den Leitfadenfragen begonnen werden. An einigen Stellen des Interviews wird es sich

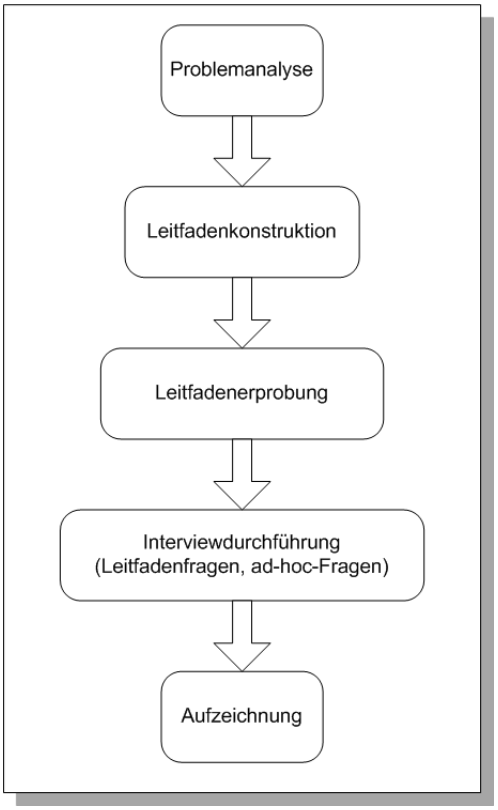

Abbildung 2.1: Abfolge der nötigen Schritte bei der Durchführung eines Leitfaden-Interviews

anbieten, ad-hoc Fragen zu stellen, um Askpekte, die im Leitfaden nicht vorkommen, dennoch abzudecken.

2.2.3 Auswertung

Für den Prozess der Auswertung und Analyse bei der qualitativen Forschung gibt es unterschiedliche Ansätze. Bei der Auswertung der von mir durchgeführten Leitfadeninterviews habe ich mich dabei an den „grounded-theory"-Ansatz von A. L. Strauss [Strauss] gehalten, bei der besonders der Kodiervorgang sehr wichtig ist.

Der erste Schritt bei der Auswertung eines Leitfadeninterviews ist die Transkription. Anhand dieser wird das Interview dann ausgewertet. Durch den sogenannten Kodiervorgang werden die Daten nun aufgebrochen. Ziel dieses Vorganges ist es, Schlüsselkategorien zu entdecken und Zusammenhänge zu erkennen. Einige dieser Kategorien hatte man natürlich schon bei der Fragengenerierung im Hinterkopf. Es ergeben sich jedoch meist auch neue. Nach Strauss können drei verschiedene Kodierungsprozesse unterschieden werden, die zirkulär ablaufen.
Durch das offene Kodieren werden die Daten aufgebrochen, indem sie in Kategorien und Subkategorien eingeteilt werden. Beim axialen Kodieren werden die Daten danach auf eine einzelne Kategorie durchsucht. Dabei handelt es sich meist um eine potenzielle

Schlüsselkategorie. Wurde festgelegt, welche Kategorie für die Forschung als zentral anzusehen ist, kann zum selektiven Kodieren übergegangen werden. Dabei werden gezielt Verbindungen der Schlüsselkategorie zu anderen Kategorien gesucht.

Nach Auffinden der Schlüsselkategorien ordnet man diesen Stellen in der Transkription zu. Dies erleichtert die Interpretation des Interviews, bei der schlussendlich versucht wird, die Kernaussagen des Interviews herauszufiltern. Ziel ist es, danach aus den Interpretationen der Interviews und dem für die Interviews verwendeten Leitfaden Hypothesen zu entwickeln.

Kapitel 3

Analyse

Ziel dieses Kapitels ist es, anhand der Durchführung qualitativer Forschung in Form von Leitfadeninterviews mit IT-Administratoren an österreichischen Schulen, herauszufinden, inwieweit Informationssicherheit an Schulen ein Thema ist. Zuerst soll ein Leitfaden für die Interviews entwickelt werden. Danach soll eine Analyse und Interpretation der durchgeführten Interviews dargestellt werden.

3.1 Vorbereitungen

3.1.1 Problemanalyse

Wie in Kapitel 2.2 beschrieben, ist der erste Schritt bei der Erstellung eines Leitfadens ein Brainstorming Prozess. Ich habe dabei versucht, alle Begriffe, die mir zum Thema IT-Sicherheit unmittelbar einfielen, festzuhalten.
Das Ergebnis ist in Abbildung 3.1 zu sehen.
Mein nächster Schritt bestand darin, Begriffe in Themenblöcke zu sammeln, vgl. dazu Abbildung 3.2.

Es ergaben sich folgende vier Kategorien, die anschließend für die Generierung der Fragen relevant waren:

- Infrastruktur
- Anforderungen
- Bedrohungen
- Maßnahmen

Dadurch wurde eine Klassifizierung für die nun entstehenden Fragen erarbeitet. Anhand dieser Klassifizierung sollen die Fragen dann auch geordnet werden. Dies erleichtert dem Interviewer sowie dem Befragten ein geordnetes Gespräch. Um diese Ordnung zu finden

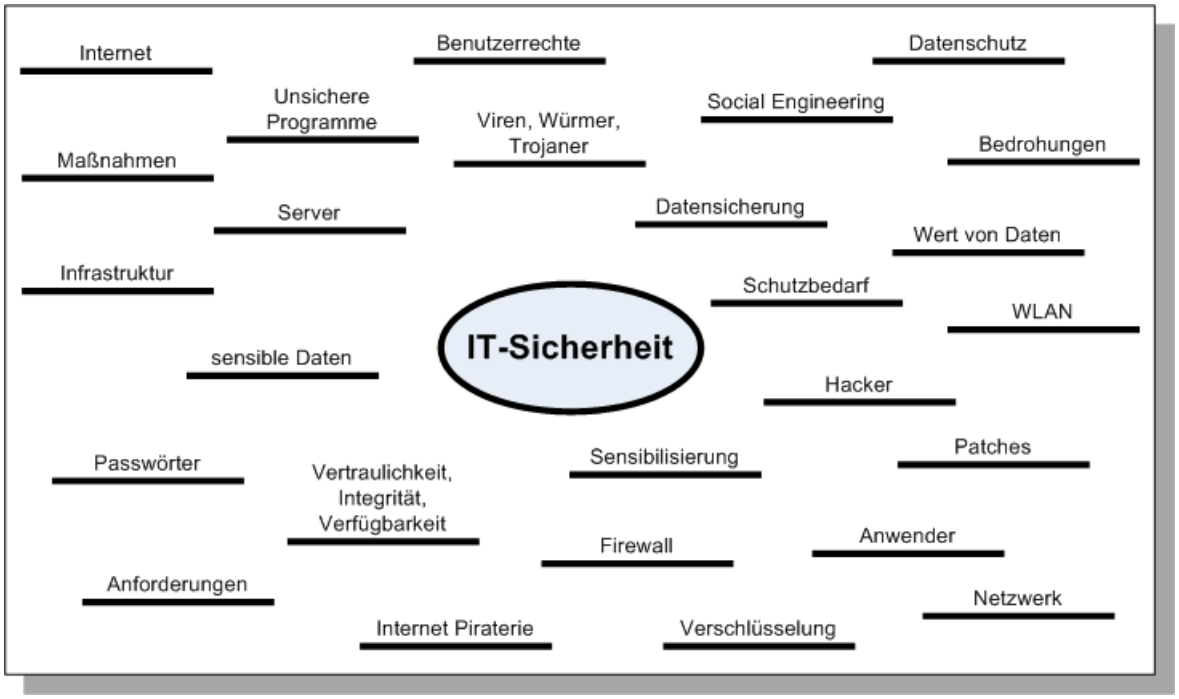

Abbildung 3.1: Ergebnis eines ersten Brainstormings zum Thema Informationssicherheit

habe ich die Kategorien in Beziehung zueinander gesetzt. Diese Beziehungen können Abbildung 3.3 entnommen werden.

Es hat sich also angeboten, das Interview mit Fragen zur IT-Infrastruktur der Schule zu beginnen und dann sukzessive zu den anderen Kategorien überzugehen.

3.1.2 Leitfadenkonstruktion

Bei der Erstellung des Leitfadens hatte ich die zuvor im Brainstorming gefundenen Begriffe im Hinterkopf. Ich möchte hier nun die von mir erstellten Leifadenfragen anführen, und welche Gedanken mich zu den einzelnen Fragen geführt haben. Durch ad-hoc Fragen während des Interviews kann ich den Befragten noch in eine gewisse, von mir gewünschte, Richtung lenken.

Bevor ich mit dem eigentlichen Interview beginne, möchte ich einige allgemeine Fragen stellen, um dem Befragten sowie mir selbst einen angenehmen Einstieg in das Interview zu ermöglichen.

- Welche Fächer unterrichten Sie?
- Wie lange sind Sie bereits an dieser Schule?
- Wie lange betreuen Sie bereits die IT an dieser Schule?

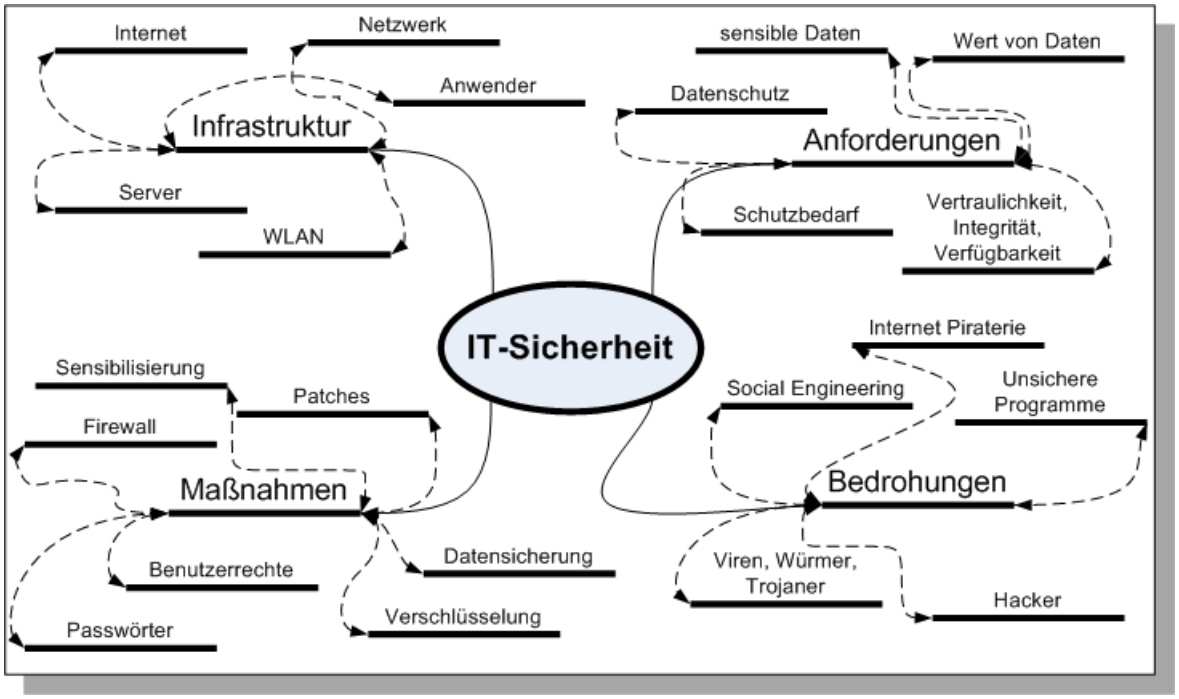

Abbildung 3.2: Einteilung des Ergebnisses des Brainstormings und Zuordnung der einzelnen Begriffe zu den Themenblöcken

Um danach auf das eigentliche Thema des Interviews überzuleiten, folgt nun eine Sondierungsfrage, aus deren Beantwortung ich mir eine persönliche Stellungnahme des Befragten zum Thema “IT-Sicherheit“ erwarte.

- Was fällt Ihnen spontan zum Thema „IT-Sicherheit“ ein? Haben Sie sich schon näher mit dem Thema auseinandergesetzt?

Nun folgen die Hauptfragen des Interviews, mit denen ich alle für mich relevanten Aspekte abdecken möchte.

1. Wie sieht die IT-Infrastruktur an Ihrer Schule aus?
   Diese Frage zielt offensichtlich auf die Kategorie *Infrastruktur* ab. Ich möchte dadurch einen Überblick über die an der Schule vorhandenen Geräte sowie deren Einsatz gewinnen. Des Weiteren soll hier auch beantwortet werden, wer an der Schule Zugriff auf die IT hat und welche Rechte den einzelnen Benutzern eingeräumt werden.

2. Wie hoch schätzen Sie den Schutzbedarf der IT an Ihrer Schule ein?
   Diese Frage ist der Kategorie *Anforderungen* zuzuordnen. Neben einer Einschätzung des Schutzbedarfs erwarte ich mir hier auch Hinweise auf mögliche sensible Daten oder Systeme.

3. Welche sensiblen Daten gibt es?
   Ziel dieser Frage ist es herauszufinden, welche Arten von Daten in der Schule verarbeitet werden und welche davon der Befragte als sensibel einstufen würde.

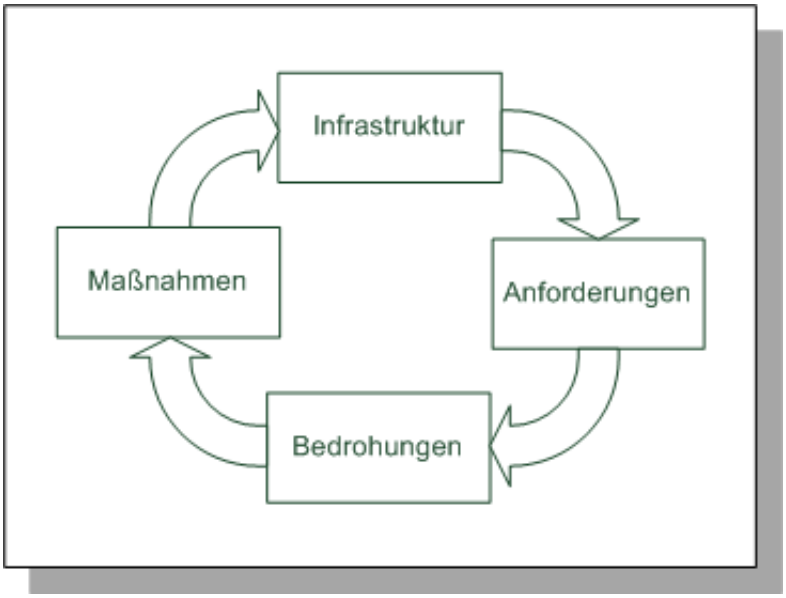

Abbildung 3.3: Beziehung der Kategorien untereinander

4. Welche Bedrohungen sind Ihnen bereits begegnet?
   Von dieser in die Kategorie *Bedrohungen* fallenden Frage erwarte ich mir Hinweise auf vergangene Sicherheitsvorfälle. Von wem wurden diese ausgelöst und wie wurde mit ihnen umgegangen?
5. Welche Maßnahmen zur IT-Sicherheit werden gefordert?
6. Inwiefern werden die Benutzer sensibilisiert?
   Diese beiden Fragen fallen unter die Kategorie *Maßnahmen*. Hier möchte ich wissen, ob und welche Sicherheitsmaßnahmen gefordert wurden bzw. welche bereits umgesetzt wurden.
7. Nehmen Sie an, Sie hätten die Möglichkeit, alle Benutzer an Ihrer Schule zum Thema IT-Sicherheit zu schulen. Was würde Sie sich wünschen, dass Schüler, Lehrer, Direktor usw. nach dieser Schulung wissen?
   Mit dieser Beschreibung einer Situation möchte ich eine Vorstellung davon bekommen, welches sicherheitsrelevante Wissen dem Sicherheitsverantwortlichen bei den einzelnen Benutzergruppen als wichtig erscheint. Dies soll schlussendlich Einfluss auf die von mir erstellte Schulung haben.

3.1.3 Pilotphase

Zur Erprobung des Leitfadens führte ich einen Pretest durch. Dadurch sollte die Qualität der Fragen getestet werden. Bei der Durchführung des Pretests merkte ich rasch, dass einige Fragen noch zu suggestiv bzw. zu ungenau formuliert waren. Der Leitfaden wurde dahingehend nochmals überarbeitet.

Frage 1 erwies sich nicht als spezifisch genug. Der Interviewte erzählte zwar manche

Dinge aus seinem Erfahrungsschatz doch leider nicht ausreichend viele. Es wurde zum Beispiel zwar erwähnt, welche Geräte vorhanden sind, leider aber nicht von wem und wie diese eingesetzt werden. Da ich bei dieser Frage allerdings auch nicht den Erzählfluss einschränken möchte habe ich zusätzliche Fragen vorbereitet, die sich während des Interviews als ad-hoc Fragen stellen lassen.
Frage 4 ist zu suggestiv verfasst. Es wird durch die Formulierung bereits vermutet, dass sensible Daten vorhanden sind. Um diese Frage zu vermeiden wurde sie, aufgrund der Themenverwandtschaft zu Frage 2, bei dieser als mögliche ad-hoc Frage eingegliedert.
Frage 5 erschien mir während des Pretests ebenfalls als zu suggestiv und auch nicht präzise genug formuliert. Der Befragte gab nur eine kurze für eine tiefergehende Analyse nicht brauchbare Antwort. Die Frage wurde deshalb umformuliert.
Frage 6 war ebenfalls zu suggestiv verfasst. Es wurde bereits vermutet, dass die Anwender sensibilisiert werden.

Der überarbeitete Leitfaden ist Anhang A zu entnehmen.

3.2 Durchführung

3.2.1 Zeitraum und Auswahl der Interviewpartner

Die Interviews wurden im Zeitraum zwischen 1. März 2009 und 31. März 2009 durchgeführt. Durch die große Vielfalt an unterschiedlichen Schultypen in Österreich war es mir leider nicht möglich, alle abzudecken. Ich habe mich allerdings bemüht, Interviewpartner sowohl in allgemeinbildenden höheren Schulen als auch in berufsbildenden höheren Schulen zu finden.

Im Rahmen meiner Diplomarbeit zum Thema „Informationssicherheit in Schulen mit besonderem Augenmerk auf die Anwenderschulung“ habe ich vier qualitative Interviews an Schulen durchgeführt. Meine Interviewpartner waren dabei IT-Sicherheitsverantwortliche in Schulen. Dabei handelte es sich durchgehend um die IT-Administratoren der jeweiligen Schule.

Interviewpartner 1: Herbert K.[1], IT-Administrator an einer allgemeinbildenden höheren Schule in Wien, unterrichtet die Fächer Informatik und Informatikmanagement und Mathematik.

Interviewpartner 2: Walter M., IT-Administrator an einer allgemeinbildenden höheren Schule in Oberösterreich, unterrichtet die Fächer Geschichte, Sozialkunde und Politische Bildung, Informatik und Informatikmanagement und Mathematik.

Interviewpartner 3: Rudolf S., IT-Administrator an einer allgemeinbildenden höheren Schule in Niederösterreich, unterrichtet die Fächer Geografie und Wirtschaftskunde, Geschichte, Sozialkunde und Politische Bildung und Informatik und Informatikmanagement.

[1]Die Namen aller Interviewpartner wurden zwecks Anonymisierung geändert.

Interviewpartner 4: Markus H., IT-Administrator an einer berufsbildenden höheren Schule in Niederösterreich, unterrichtet die Fächer Informatik und Informatikmanagement, Mathematik und Physik.

3.2.2 Anmerkungen

Exemplarisch möchte ich hier über das letzte von mir durchgeführte Interview berichten, welches auch im weiteren Verlauf der Arbeit für die Anführung der Auswertungsschritte angeführt wird. Grund dafür ist, dass sich aus meiner Sicht dieses Interview besonders gut eignet um die nötigen Schritte darzustellen.

Das Interview mit Markus H. (Name zwecks Anonymisierung geändert) wurde am 31. März 2009 an einer berufsbildenden höheren Schule in Niederösterreich durchgeführt. Dankenswerter Weise hat Markus H. sich genug Zeit genommen alle meine Fragen zu beantworten, und war mit einer Aufzeichnung des Gespräches auf Tonband einverstanden. Bevor das eigentliche Gespräch zum Thema IT-Sicherheit in Schulen begonnen wurde, stellte ich mich und den Kontext des Interviews vor. Das Interview folgte danach weitgehend meinem Leitfaden. Durch die bereits in den davor geführten Interviews gesammelte Erfahrung, war es mir möglich, bei mir wichtigen Themen einzuhaken und ad-hoc Fragen unterzubringen. Das Gespräch entwickelte sich äußerst positiv. Markus H. nutzte die Gelegenheit, vieles aus dem Alltag eines IT-Administrators an einer Schule einzubringen.

3.3 Auswertung

3.3.1 Transkription

Ziel einer Transkription ist es, den gesamten Verlauf eines Interviews zu Papier zu bringen. Für die spätere Kodierung und Inhaltsanalyse würde eine Auswahl der Daten eine Einschränkung bedeuten. Deshalb ist es besser, das Interview vollständig zu transkribieren. Die Schriftform sollte also einen hohen Genauigkeitsgrad besitzen weshalb auch Füllwörter wie „ahm“ oder Gefühle wie das Lachen einer Person zu Papier gebracht werden sollten.

Das größte Problem bei der Transkription der von mir durchgeführten Interviews, war die Qualität der Tonaufnahmen. Da mir leider kein professionelles Equipment zum Aufzeichnen der Interviews zur Verfügung stand, ist die Qualität der Aufnahmen teilweise mangelhaft. Nichtsdestotrotz habe ich mich bemüht, die Interviews so exakt wie möglich zu transkribieren.
Beispielhaft findet sich die Transkription des Interviews mit Markus H. im Anhang B. In der ersten Spalte der Transkription findet sich die Zeitleiste bezogen auf die Sprachaufnahme des Interviews. Dadurch ist eine schnelle Orientierung möglich, falls man bei der Auswertung einer Stelle nochmals das Gespräch anhören will. In der zweiten Spalte

folgt eine Nummerierung der einzelnen Aussagen. Dabei habe ich den Ansatz verfolgt, bei jedem Sprecherwechsel die Nummerierung um eins zu erhöhen. In der dritten Spalte ist festgehalten, wer am Wort ist. In der vierten Spalte folgen schlussendlich die Aussagen.

3.3.2 Kodierung

Der erste Schritt beim Kodieren der Interviews war das offene Kodieren. Bei der Erstellung des Leitfadens für das Interview hatte ich bereits einige Kategorien im Hinterkopf. Ich habe versucht diese bzw. neue Kategorien im Interview zu entdecken. Dabei ging ich Zeile für Zeile vor. Um das Generieren der Kategorien darzustellen, beziehe ich mich im Folgenden wieder auf das Interview mit Markus H.[2].

Zeile 10 (L): (...) nur fünf unterrichten; damit wird ein Zustand der *personellen Infrastruktur* beschrieben.
Zeile 20,22 (L): Die Kollegin (...) war überfordert; damit wird ein *personelles Problem* beschrieben.
Zeile 36 (L): Das beginnt bei (...) Datenschutz bis hin zu Web-Security; hier findet man Schlagworte zum Bereich Informationssicherheit. Damit wird versucht eine *Definition* des Themas zu finden.
Zeile 42,44 (L): (...) Backup (...) in der Verwaltung; hierbei handelt es sich um eine *Anforderung* an die Informationssicherheit.
Zeile 58 (L): (...) es passen da die Schnittstellen nicht ganz; es ist also ein *infrastrukturelles Problem* aufgetreten.
Zeile 68 (L): (...) Ich habe ein pädagogisches und ein (...) Verwaltungsnetzwerk; damit wird ein Zustand der *technischen Infrastruktur* beschrieben.
Zeile 70 (L): ...die physikalisch komplett getrennt sind ...; es wurde also eine *Maßnahme* gesetzt.
Zeile 212 (L): (...) die fladern ihnen RAM raus; damit wir eine *Bedrohung* der IT dargestellt.
Zeile 340 (L): (...) Wie sensibel gehe ich mit meinen Daten im Internet um; damit wird eine *Sensibilisierung* der Benutzer beschrieben.

Damit haben sich nach dem ersten Kodierdurchgang folgende Kategorien ergeben:

- Definition von Informationssicherheit
- Anforderungen an die Informationssicherheit
- Technische Infrastruktur
- Personelle Infrastruktur
- Infrastrukturelle Probleme
- Personelle Probleme

[2]Vgl. Anhang B

- Bedrohungen der IT
- Maßnahmen
- Sensibilisierung

Bevor nun zum axialen Kodieren übergegangen wurde versuchte ich, aufgrund der großen Zahl an gefundenen Kategorien, ähnliche Kodes unter einem Oberbegriff zusammenzufassen und diese dann untereinander in Beziehung zu setzen. Damit reduzierten sich die Kategorien auf:

- Anforderungen an die IT-Sicherheit
- Infrastruktur
- Probleme
- Gefahren
- Maßnahmen

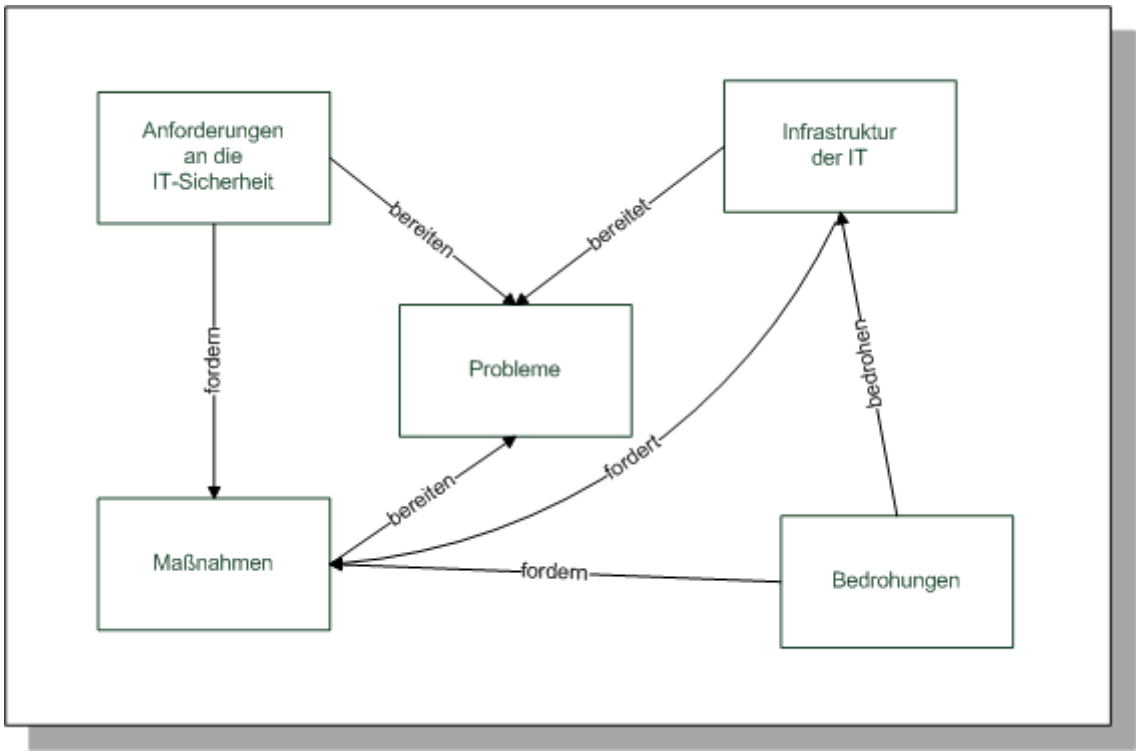

Abbildung 3.4: Zusammenhänge der Kategorien

Bedrohungen der IT-Sicherheit beeinflussen die Infrastruktur eines IT-Systems. Dadurch, und aufgrund anderer Anforderungen, müssen Maßnahmen zur Herstellung bzw. zur Wahrung der Sicherheit eines IT-Systems gesetzt werden.
Allerdings kommt es hierbei sehr oft zu Problemen. Sei es nun in personeller Hinsicht oder in infrastruktureller. Diese Zusammenhänge lassen sich am Besten aus Abbildung 3.4 entnehmen. Dadurch lässt sich auch bereits „Probleme“ als potentielle

Schlüsselkategorie erahnen.

Beim axialen Kodieren wird nun der Text intensiv auf die Kategorie „Probleme“ hin analysiert. Welche Probleme treten im Zusammenhang mit den an die IT-Sicherheit gestellten Anforderungen auf? Welche Probleme gibt es bei der Infrastruktur der IT? Welche Probleme gibt es bei der Umsetzung der Maßnahmen zur Wahrung bzw. Herstellung von IT-Sicherheit?

Bei der Herstellung und Wahrung von IT-Sicherheit in Schulen kommt es für den Administrator immer wieder zu unterschiedlichsten Problemen.
Nicht gut genug geschulte Administratoren, die diese Aufgabe vielleicht nur erledigen, weil sonst niemand da ist, der dies machen kann, sind oft schon mit anderen Aufgaben überfordert und haben dann keine Zeit bzw. auch nicht mehr die Kraft, sich um die IT-Sicherheit zu kümmern[3]. Auch durch die unterschiedlichsten Anforderungen an die IT-Sicherheit kommt es immer wieder zu Problemen. Einerseits wird die Wahrung der Sicherheit von höher geordneten Stellen wie dem Landes-/Stadtschulrat gefordert[4], andererseits gibt es auch viel näherliegende Anforderungen, wie Sicherheitslücken in Betriebssystemen oder Angriffe auf das Netzwerk. Bei der Umsetzung der Maßnahmen kommt es ebenfalls immer wieder zu Problemen. Nicht getestete Patches für Sicherheitslücken können die Leistung der IT-Komponenten beeinträchtigen oder sogar schlimmere Schäden an der Netzwerkstruktur anrichten[5].

Durch diese und weitere Zusammenhänge der Kategorie „Probleme“ entstand ein dichtes Beziehungsnetz um die „Achse“ der Kategorie und die Beziehungen zu anderen Kategorien nahmen immer mehr zu. Damit kristallisierte sich für mich die Kategorie „Probleme“ als Schlüsselkategorie heraus und ich ging zum selektiven Kodieren über.

Beim selektiven Kodieren wurde die Schlüsselkategorie „Probleme“ dann weiter in Verbindung mit den anderen Kategorien gesetzt. Dazu habe ich mich gefragt, welche Arten von Problemen im Zusammenhang mit Informationssicherheit auftreten.
Infrastrukturelle Probleme bereiten in mehrerlei Hinsicht Probleme. Einerseits sind dies personelle Probleme, z.B. zu wenig Zeit um Aufgaben zu erledigen oder zu schlecht geschulte Kollegen, andererseits treten technische Probleme auf. So kann etwa Hardware fehlerhaft sein oder es können Probleme in der Struktur des Netzwerkes auftreten.
Hinsichtlich der möglichen Maßnahmen kommt es ebenfalls zu Problemen. So kann zum Beispiel die geforderte Passwortkomplexität nicht allzu hoch sein, da viele User ansonsten ihr Passwort leichter vergessen, was zu einem sehr hohen administrativen Aufwand führt[6].
Die unterschiedlichen Anforderungen an die IT-Sicherheit können ebenfalls zu Problemen werden, da, wieder aufgrund der infrastrukturellen Probleme, nicht all das umgesetzt werden kann, was eigentlich umgesetzt werden sollte.

Nach dem Schritt des selektiven Kodierens beginnt der Kodiervorgang wieder von vor-

[3]Vgl. Anhang B, Zeile 21-22
[4]Vgl. Anhang B, Zeile 63-64
[5]Vgl. Anhang B, Zeile 242
[6]Vgl. Anhang B, Zeile 300, 302

ne, also beim offenen Kodieren. Dies habe ich so oft wiederholt, bis der Forschungstext, in meinem Fall die Transkription, gänzlich aufgebrochen war. Danach ging ich zur Interpretation der Texte über.

3.3.3 Interpretation

Zur Interpretation der Interviews möchte ich zuerst einige, mir als wichtig erscheinende, Aussagen aus den Interviews herausgreifen und näher dazu Stellung nehmen. Danach möchte ich meine Gedanken weiter ausführen und zu einem Lösungsansatz kommen.

Ich möchte zunächst versuchen mit Hilfe des Interviews meine erste Forschungsfrage nach der Bedeutung der Informationssicherheit an österreichischen Schulen zu beantworten.

> Interviewer: „Hast du dich damit [mit IT-Sicherheit] schon auseinandergesetzt irgendwie?“
> Markus H.: „Ja sicher [...] ich meine das muss man in Schulen unbedingt.“[7]

> Markus H.: „[Im Verwaltungsnetz] sind wirklich Daten, die wirklich sensibel sind.“[8]

Wie in allen Bereichen, in denen Informationen verarbeitet und Computer dazu eingesetzt werden, ist auch in der Schule die Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit der Informationen unumgänglich.
Besonders im Zuge der Schulverwaltung werden sensible, personenbezogene Daten verarbeitet, die es zu schützen gilt. Dabei werden in Schulen einzelne Maßnahmen, wie die Implementierung von Firewalls oder die Implementierung eines Virenschutzkonzepts, durchgeführt. Allerdings sind dies nur Teilaspekte, die es zu systematisieren gilt. Zu diesem Zweck bedarf es aus meiner Sicht der Implementierung eines Informationssicherheitsmanagementsystems.

Da sich in den Interviews für mich die Kategorie „Probleme“ zur Schlüsselkategorie entwickelte, möchte ich nun auf die Probleme, die im Zusammenhang mit Informationssicherheit an Schulen auftreten, eingehen.

> Markus H.: „Die Kollegin [...] war überfordert“[9]

> Interviewer: „[...] Gibt es vom Landesschulrat keine Weisungen in Richtung IT-[...]Sicherheit?“
> Markus H.: „Gibt es prinzipiell schon, wobei man andererseits sagen muss, es gibt keinen Verantwortlichen der es [...] ausführen sollte [...]“[10]

Diese beiden Aussagen stellen für mich offensichtliche Probleme bei der Umsetzung von Informationssicherheit an Schulen dar. Besonders in kleineren Schulen gibt es leider des

[7] Vgl. Anhang B, Zeile 31-34
[8] Vgl. Anhang B, Zeile 260
[9] Vgl. Anhang B, Zeile 21,22
[10] Vgl. Anhang B, Zeile 63-66

Öfteren noch ungeschulte Kollegen, die sich um das Funktionieren der IT-Systeme und damit auch um die Sicherheit dieser kümmern sollten. Da diese allerdings schon mit den „eigentlichen“ Aufgaben als Administrator eines Netzwerkes überfordert sind, bleibt ihnen oft keine Zeit mehr, sich auch noch um sicherheitstechnische Angelegenheiten zu kümmern.
Aber auch in größeren Schulen gibt es ähnliche Probleme. Es gibt zwar offensichtlich Weisungen des Stadt-/Landesschulrats, die in Richtung IT-Sicherheit gehen, doch wird dafür kein Verantwortlicher bestimmt. Damit wird die Aufgabe meist an den IT-Administrator übergeben, der allerdings mit seinen Routineaufgaben bereits mehr als ausgelastet ist. Markus H. etwa betreut ein Netzwerk mit mehr als 500 Benutzern[11], wofür er aber eigentlich nur 10 Werteinheiten an Arbeitszeit pro Woche verrechnet bekommt[12]. In dieser Zeit ist er allerdings bereits mit Dingen wie Aufrechterhaltung des Netzwerks, Benutzeranfragen usw. beschäftigt. Es bleibt also kaum Zeit sich intensiv mit der Sicherheit der eingesetzten IT-Systeme zu beschäftigen.

Probleme mit denen sich die Administratoren auch beschäftigen müssen, sind die unterschiedlichen Bedrohungen, die IT-Systeme gefährden.

> Markus H.: „[...] Einmal, das war diese Sasser-Zeit, [...] die war einfach ein wenig ein Problem. [...] Sicherheitslücken, das ist halt immer so ein bisschen ein heikles [...] Problem. [...]“[13]

> Markus H.: „Ich muss keine Mäuse anhängen, ich muss keine Computer zusperren. In HTLs kommt es vor, wenn ich mit anderen Administratoren rede, die fladern ihnen RAM raus.“[14]

Die Palette der Bedrohungen an die Informationssicherheit in Schulen ist also groß. Einerseits müssen die Systeme gegen Angriffe von außen, wie Viren, Würmer, Trojaner, ... geschützt sein, andererseits kann es auch zu Angriffen innerhalb der Schule kommen. Leider kommt es z.B. vor, dass Peripheriegeräte oder anderes Inventar abhanden kommen. Aber auch andere Bedrohungen wie Software-Piraterie sind mitunter ein Thema, da in Schulen teilweise Spezialsoftware für gewisse Aufgaben eingesetzt wird, die sich Schüler für den Eigengebrauch allerdings nicht leisten können[15].

Hinsichtlich der Sensibilisierung zum Thema IT-Sicherheit bedarf es auch noch einiger Arbeit.

> Markus H.: „Ich habe letztes Jahr einen Herren da gehabt, der ist Internet Broker gewesen. [...] Ich glaube, dass [...] das ein Thema für die Schüler [ist] [...] Datensicherheit. [...] Was gebe ich im Internet von mir Preis? Wie sensibel gehe ich mit meinen Daten im Internet um? [...] Also mit so Dingen, ahm, dass sie im Internet im Prinzip gläsern sind, das ist ihnen

[11] Vgl. Anhang B, Zeile 258
[12] Vgl. Anhang B, Zeile 260
[13] Vgl. Anhang B, Zeile 236-240
[14] Vgl. Anhang B, Zeile 212
[15] Vgl. Anhang B, Zeile 132-140

nicht bewusst.“[16]

Markus H.: „[. . .] Ich würde mir manches mal eine höhere IT-Fitness wünschen [. . .]“[17]

Markus H.: „[. . .] und dann ist das Problem, wenn dann im Prinzip jemand in den EDV-Raum geht und das Netzwerk gar nicht einmal versteht [. . .] dann wird es schon schwer [. . .]“[18]

Das mangelnde Sicherheitsbewusstsein der Benutzer, beziehungsweise generell das mangelnde Verständnis für die dahinterstehende Technik, sind oft genug ein Problem, nicht nur für die Sicherheit der IT-Systeme. Eine Schulung oder Sensibilisierung ist also notwendig und wünschenswert.

Dabei ist es bei der Schulung der Schüler aus meiner Sicht nicht so wichtig, sie nur im Hinblick auf die Informationssicherheit an der Schule selbst zu schulen. Viel wichtiger wäre es, den Jugendlichen bereits im Rahmen ihrer Schulausbildung ein grundlegendes Verständnis der Informationssicherheit zu vermitteln. Für Lehrer hingegen muss es ausreichend sein, schulspezifische Schulungen durchzuführen. Eine weitere Beschäftigung mit dem Thema Informationssicherheit, beispielsweise im Hinblick auf die Sicherheit bei der Verwendung von Online Banking usw. im privaten Bereich, muss der Eigenverantwortung der Lehrer überlassen werden.

3.3.4 Hypothesen

Anhand der Interpretation der Interviews und dem für die Gespräche entwickelten Leitfaden lassen sich nun Hypothesen zu den einzelnen Fragen entwickeln. Diese wurden dann mit den Aussagen der übrigen Interviews verglichen. Dabei musste keine der Hypothesen verworfen werden.

FF1: Was fällt Ihnen spontan zum Thema „IT-Sicherheit“ ein? Haben Sie sich schon näher mit dem Thema auseinandergesetzt?
H_0: Der Befragte hat sich bereits mit dem Thema auseinandergesetzt und ihm fallen zuerst als Maßnahmen zu kategorisierende Schlagworte ein.

FF2: Wie sieht die IT-Infrastruktur an Ihrer Schule aus?
H_0: Das Netzwerk ist in ein Pädagogisches- und ein Verwaltungsnetzwerk getrennt. In diesen sind sowohl Workstations als auch Server vorhanden.

FF3: Wie hoch schätzen Sie den Schutzbedarf der IT an Ihrer Schule?
H_0: Der Befragte kategorisiert den Schutzbedarf im Verwaltungsbereich als „hoch“ und im pädagogischen Bereich als „niedrig“.

FF4: Sind Ihnen in Ihrer Laufbahn als IT-Administrator an einer Schule schon Bedrohungen für die IT begegnet? Wenn ja, welche?

[16] Vgl. Anhang B, Zeile 338-364
[17] Vgl. Anhang B, Zeile 404
[18] Vgl. Anhang B, Zeile 408-410

H_0: Der Befragte musste sich zumindest schon mit kleineren Angriffen (Virenangriffe, Skripte, ...) auseinander setzen.

FF5: Werden, etwa von der Direktion, Sicherheitsmaßnahmen gefordert?
H_0: Es werden keine Sicherheitsmaßnahmen von der Schulleitung gefordert, jedoch gibt es Weisungen des Stadt-/Landesschulrats.

FF6: Gibt es Sicherheitsrichtlinien für die Benutzer?
H_0: Es gibt keine Sicherheitsrichtlinien für die Benutzer.

3.3.5 Zusammenfassung

In allen von mir durchgeführten Interviews erhielt ich sehr ähnliche Antworten zum Thema Informationssicherheit in Schulen.

Die unter anderem für die Sicherheit zuständigen Administratoren setzen sich sehr wohl mit dem Thema Informationssicherheit auseinander. Sie versuchen so viele Maßnahmen wie nur möglich zur Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Informationen umzusetzen. Dabei wird jedoch ohne ein ganzheitliches Konzept gearbeitet. Ohne ein solches ist es nahezu unmöglich, alle Bereiche des IT-Systems abzusichern. Es können bestenfalls Teilaspekte umgesetzt werden.

Dass der Schutzbedarf an sich teilweise als „hoch“ einzustufen ist, wurde mir ebenfalls von allen Befragten bestätigt. Zumindest in den Schulen der Befragten gibt es eine Trennung der Infrastruktur in ein pädagogisches Netzwerk und ein Verwaltungsnetzwerk. Dabei kategorisieren die Befragten den Schutzbedarf des Verwaltungsnetzwerkes als hoch. Grund dafür sind die darin verarbeiteten Daten wie personenbezogene Daten der Schüler, Kontodaten der Schule oder Schularbeits- und Maturaaufgaben.

Die Befragten sind in ihrer Laufbahn als IT-Administratoren schon vielen Bedrohungen der Informationssicherheit begegnet. Einige der Befragten etwa benennen Skript-Angriffe auf Webserver bereits als Standard. Auch mit Viren im Netzwerk gibt es hin und wieder Probleme.

Opfer eines Hackerangriffs wurde bisher keiner der Befragten, jedoch kann auch dies in Schulen vorkommen[19].

Bei der Etablierung von Informationssicherheit in Schulen kommt es auch zu bürokratischen Problemen. Von höhergeordneten Stellen, wie dem Stadt- und den Landesschulräten, gibt es zwar Weisungen in Richtung Informationssicherheit, dabei wird allerdings kein Verantwortlicher bestimmt. Dies ist die Aufgabe der Schulleitung, die sich aber oft den Bedrohungen an die Informationssicherheit nichteinmal bewusst ist. Damit bleibt die Aufgabe an den Administratoren der IT-Systeme an Schulen hängen. Da diese aber oft genug schon mit anderen Aufgaben ausgelastet sind, haben sie nur

[19]Vgl. IT Weblog des LSRNOE, "Hackerangriffe und Sicherheitshinweise", 4. 4. 2008. Online erhältlich via URL: `<http://itblog.lsr-noe.gv.at/?p=36>` (16. April 2009).

wenig Zeit, sich mit dem doch beträchtlichen Gebiet der Informationssicherheit auseinanderzusetzen. Teilweise fehlt den IT-Administratoren auch das nötige Fachwissen, um sich mit dem Thema zu beschäftigen.

Dass dies dabei kein rein österreichisches Problem ist, belegt auch der Artikel von M. Dark [Dark]. Darin wird über die Notwendigkeit von Informationssicherheit in K12-Schulen, einer speziellen Schulform in den Vereinigten Staaten von Amerika, und die Probleme bei der Umsetzung berichtet. Laut Dark ist ein Großteil der IT-Administratoren an K12-Schulen im Vergleich zu IT-Administratoren in der Wirtschaft/Industrie unterbezahlt. Auch die Wissensunterschiede der vielen Administratoren sind groß. Somit kann die Sicherheit der IT-Systeme nicht gewährleistet werden.

Aus der Sicht der Benutzer muss auch noch vieles getan werden. Schüler sind sich zum Beispiel oft ihrer Offenheit im Internet nicht bewusst. Hier wäre beispielsweise eine Sensibilisierung in Richtung Datenschutz und Datensicherheit von Nöten, um den Schülern die Gefahren, die damit verbunden sind, klar zu machen. Auch auf der Seite der Lehrer gibt es noch Aufholbedarf. Wer in einem Netzwerk arbeitet, sollte zumindest grundlegende Kenntnisse darüber besitzen, auch hinsichtlich der Sicherheit.

Aus diesen Gründen möchte ich mich in den Kapiteln 4 und 5 zuerst mit der Etablierung eines Informationssicherheitsmanagementsystems, aufbauend auf dem Österreichischen Informationssicherheits-Handbuch [OeSiH], beschäftigen. Danach soll der Schulung bzw. Sensibilisierung der Anwender besondere Aufmerksamkeit geschenkt werden.

Kapitel 4

Informationssicherheitsmanagement

Ziel dieses Kapitels ist es, aufbauend auf dem Österreichischen Informationssicherheits-Handbuch [OeSiH]s, die Etablierung eines Informationssicherheitsmanagementsystems (ISMS) in Schulen zu beschreiben. Zuerst soll auf die Ziele und Aufgaben eines solchen Managements eingegangen werden. Danach sollen die zur Durchführung notwendigen Schritte beschrieben werden.

4.1 Vorüberlegungen

Bei der Durchführung der Interviews (vgl. Kapitel 3) wurde mir bewusst, dass von den IT-Administratoren zwar vieles zur Herstellung bzw. Wahrung von IT-Sicherheit unternommen wird, dass dabei allerdings in den meisten Fällen kein System dahintersteckt. Durch die Installation eines Virenschutzes oder der Implementierung von Firewalls können bestenfalls Teilaspekte abgedeckt werden. Viele Sicherheitslücken werden jedoch ohne eine systematische Überprüfung übersehen werden. Aus diesem Grund gibt es eine Vielzahl von Ansätzen, die sich mit der Implementierung eines Informationssicherheitsmanagementsystems (ISMS) beschäftigen.
In Deutschland wurde zu diesem Zweck vom Bundesamt für Sicherheit in der Informationstechnik das Vorgehen nach dem Grundschutzhandbuch entwickelt [GSHB]. In Österreich wurde, aufbauend auf ebendiesem, Österreichisches Informationssicherheits-Handbuch [OeSiH] entwickelt, das für den Einsatz in österreichischen Behörden und Institutionen bestimmt ist.
Aufbauend auf diesem sollen nun im Folgenden alle notwendigen Schritte zur Implementierung eines Informationssicherheitsmanagementsystems in Schulen beschrieben werden.

4.1.1 Ziele und Aufgaben eines ISMS

Grundsätzliches Ziel bei der Implementierung eines Informationssicherheitsmanagementsystems (ISMS) ist es, die klassischen IT-Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit sicher zu stellen. Die Bedeutung dieser Ziele wurde bereits in Kapitel 2 erläutert. Durch die Wahrung dieser Ziele sollen beispielsweise die vertraulichen Schülerdaten aber auch die gesamte IT-Infrastruktur geschützt werden.

Die Aufgaben eines Sicherheitsmanagementsystems sind demnach folgende[1]:

- Festlegung der Sicherheitsziele und -strategien
- Auffinden und Bewerten von Sicherheitsrisiken
- Festlegung von Maßnahmen
- Überwachung des laufenden Betriebs
- Sensibilisierung der Anwender

Dabei ist zu beachten, dass die Aufgabe der Implementierung eines Informationssicherheitsmanagements nicht alleine die Aufgabe des IT-Administrators an einer Schule ist. Wird der Administrator dabei nicht von der Schulleitung unterstützt, so kann das System nicht erfolgreich umgesetzt werden.

4.2 Durchführung

Informationssicherheitsmanagement ist kein Prozess den man einmal durchführt und der danach abgeschlossen ist, sondern es ist als kontinuierlicher Prozess zu verstehen. Dabei bedarf es einer ständigen Überprüfung zur Aufrechterhaltung der gesetzten Maßnahmen.

In Abbildung 4.1 ist ein systematischer Ablauf eines ISMS abgebildet. Auf die einzelnen Punkte wird im Folgenden näher eingegangen.

4.2.1 Informationssicherheitspolitik

Als Informationssicherheitspolitik wird ein schriftliches Dokument bezeichnet, das die Basis für das ISMS bildet. Die darin enthaltenen Informationen sind möglichst allgemein verfasst und werden dann in den einzelnen Sicherheitsrichtlinien umgesetzt. Ziel ist es, dadurch die allgemeinen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit der Informationen in einer Schule sicherzustellen. Dabei sollen allerdings noch keine systemspezifischen Umsetzungen formuliert werden, sondern allgemeine Leitlinien angegeben werden. Die Informationssicherheitspolitik sollte dabei nicht nur vom IT-Administrator oder einer anderen Person in Eigenregie erstellt werden sondern im Zuge

[1] Vgl. [OeSiH]

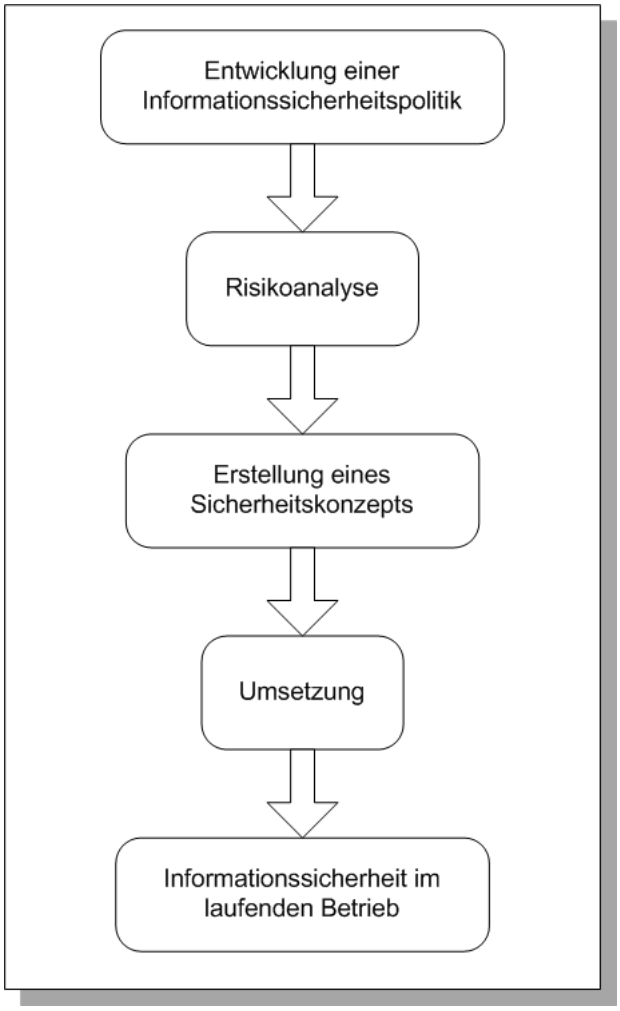

Abbildung 4.1: Abfolge der notwendigen Schritte zur Implementierung eines ISMS in zeitlicher Reihenfolge nach [OeSiH]

einer Arbeitsgemeinschaft. Darin sollten je nach Anforderungsprofil etwa die Schulleitung, der IT-Administrator, ein Lehrer- sowie, im Optimalfall, auch ein Schülervertreter mitwirken.
Die Informationssicherheitspolitik sollte in regelmäßigen Abständen aktualisiert werden.

Inhalte
Im Folgenden sollen die notwendigen Inhalte einer Informationssicherheitspolitik in einer Schule beschrieben werden.

- Informationssicherheitsziele und -strategien
  Unter diesen Punkt fallen alle allgemein zu erfüllenden Sicherheitsziele und -strategien. Dazu gehören die Einhaltung aller Gesetze, wie zum Beispiel dem Datenschutzgesetz in Zusammenhang mit der Verwertung personenbezogener Daten im Zuge der Schulverwaltung, und die Wahrung der Verfügbarkeit, Integrität und

Vertraulichkeit aller Daten und Systeme.
Weiters sollte das angestrebte Sicherheitsniveau, wobei hier aus meiner Sicht für fast alle österreichischen Schulen das Sicherheitsniveau „normal“ völlig ausreichend ist, angeführt werden.
Auf diese Punkte sollte, auf das Schulprofil angepasst, eingegangen werden.

- Bekenntnis der Schulleitung
  Hier sollte die Schulleitung eine kurze Stellungnahme über die Bedeutung von Informationssicherheit für die Schule abgeben. Es soll daraus ersichtlich sein, dass die Schulleitung voll und ganz hinter der Erfüllung der Sicherheitsziele steht.

- Organisation und Verantwortlichkeit
  Für Schulen sind eigene Teams für das Informationssicherheitsmanagement unnötig. Es ist aus meiner Sicht völlig ausreichend einen Sicherheitsbeauftragten zu bestimmen. In den allermeisten Fällen wird es sich anbieten, diese Aufgabe dem IT-Administrator zu übertragen. Dabei sollte allerdings der erhöhte Aufwand berücksichtigt werden. In einigen Fällen wird es sich daher anbieten, neben dem IT-Administrator eine zweite Peron, etwa einen Informatik-Lehrer, mit dieser Aufgabe zu betrauen.

- Risikoanalysestrategie
  Ohne eine Risikoanalyse ist ein vollständiges Informationssicherheitsmanagement undenkbar. Deshalb ist festzuhalten, welche Strategie zur Ermittlung des Gesamtrisikos verfolgt wird. Dieses ist zu minimieren und es ist festzulegen, wie hoch das akzeptable Restrisiko sein darf.

- Klassifizierung von Informationen
  Um später angemessene Maßnahmen umsetzen zu können muss eine Einteilung in Klassen bezüglich der Vertraulichkeit und bezüglich auf des Datenschutz von Informationen getroffen werden.
  Für die Klassifizierung im Bezug auf die Vertraulichkeit bietet sich eine Einteilung in drei Klassen, etwa „geheim“, „vertraulich“ und „normal“, an.
  Bezogen auf den Datenschutz wird gemäß DSG 2000 eine Einteilung in „nur indirekt personenbezogen“, „personenbezogen“ und „sensibel“ vorgeschrieben.
  Weiters ist festzuhalten, wie mit Daten, je nach Klasse, umgegangen werden soll.

- Klassifizierung von Anwendungen und Systemen
  Analog zur Einteilung in Klassen von Informationen soll eine Klassifizierung von Anwendungen und Systemen bezüglich der Verfügbarkeit erstellt werden.

- Überprüfung
  Schlussendlich soll in der Informationssicherheitspolitik eine Methode zur Überprüfung der laufenden Maßnahmen hinsichtlich der Informationssicherheit angegeben werden.

4.2.2 Risikoanalyse

Es gibt unterschiedliche Möglichkeiten eine Risikoanalyse durchzuführen. Eine detaillierte Risikoanalyse führt zu einem sehr hohen Maß an Sicherheit, kostet dabei allerdings viel Zeit, Aufwand und Geld. Beim Grundschutzansatz wird recht rasch ein vernünftiges Maß an Sicherheit erreicht. Der kombinierte Ansatz verbindet die Vorteile von beiden Methoden. Aus meiner Sicht empfiehlt sich im Hinblick auf Schulen der kombinierte Ansatz, da in Schulen das Verwaltungssystem einen höheren Schutzbedarf als die übrige IT hat.

Beim kombinierten Ansatz werden zuerst mögliche Schutzbedarfskategorien festgelegt. Für die meisten Schulen bietet sich eine Einteilung in „niedrig“, „mittel“ und „hoch“ an. Diejenigen Systeme, die für die Verwaltung der Schülerdaten eingesetzt werden, fallen dabei unter den Schutzbedarf „hoch“. Die Gründe dafür liegen auf der Hand. Ein Ausfall für längere Zeit ist im „Verwaltungsbereich eine Katastrophe“[2] und es werden im Verwaltungsbereich personenbezogene Daten der Schüler und Lehrer verarbeitet. Sollte eine Gefährdung der Vertraulichkeit dieser Daten bekannt werden, ist mit einem enormen Imageverlust der Schule zu rechnen.
Für die übrigen IT-Systeme, also diejenigen, die nichts mit der Verwaltung zu tun haben, wird eine Schutzbedarfsfeststellung durchgeführt. Dabei werden zuerst alle vorhandenen IT-Systeme erfasst und ähnliche Geräte gruppiert. Zum Beispiel bietet sich eine Gliederung in „Geräte ohne Netzwerkanbindung“, wie Laptops, „Arbeitsstationen“ und „Server“ an.

Danach werden alle verwendeten Anwendungen erfasst und den einzelnen Systemen zugeordnet, da auf unterschiedlichen Systemen unterschiedliche Anwendungen zum Einsatz kommen. Als letzter Schritt wird schlussendlich der Schutzbedarf für die so definierten Systeme festgestellt.

Ist der Schutzbedarf der Systeme festgestellt, folgt die eigentliche Risikoanalyse. Für die Schutzbedarfskategorie „hoch“ kann der Einsatz einer detaillierten Risikoanalyse überlegt werden. Aus meiner Sicht ist jedoch ein verstärkter Grundschutzansatz ausreichend. Bei den Systemen mit Schutzbedarf „niedrig“ und „mittel“ reicht jedenfalls der Grundschutzansatz. Die Reihung der während der Durchführung der Risikoanalyse untersuchten Systeme richtet sich dabei nach der Schutzbedarfskategorie.

Das Vorgehen bei der Grundschutzanalyse orientiert sich hier an den Vorgaben zum IT-Grundschutz des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI), dem BSI Standard 100-2 [BSI 100-2].
Dahinter steckt die Idee, keine aufwendige Risikoanalyse durchzuführen. Vielmehr wird von einer allgemeinen Gefährdungslage ausgegangen. Gefährdungen und Maßnahmen finden sich im BSI Grundschutzkatalog [GSHB]. Ein weiterer Vorteil ist, dass die möglichen Maßnahmen weit verbreitet und daher kostengünstig sind. Dies ist natürlich günstig für Schulen, wo oft wenig Budget für Sicherheitsmaßnahmen vorhanden ist. Außerdem ist der Aufwand für die Umsetzung relativ gering und es lässt sich schnell

[2] Vgl. Anhang B, Zeile 54

ein gutes Maß an Sicherheit erreichen, vor allem dann, wenn bisher noch wenig im Hinblick auf die Informationssicherheit getan wurde.

Grundschutzanalyse
Der erste Schritt bei der Grundschutzanalyse ist die Modellierung der vorhandenen IT-Systeme nach dem im GSHB dargestellten Schichtenprinzip (vgl. Abbildung 4.2).

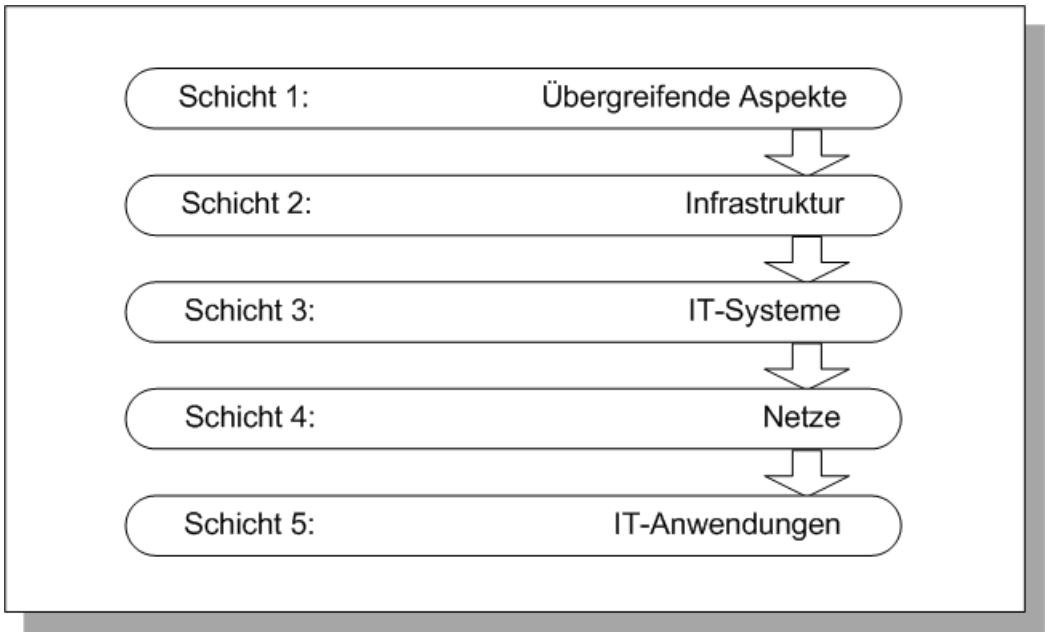

Abbildung 4.2: Schichten des IT-Grundschutzmodells nach [GSHB]

Schicht 1 beinhaltet Aspekte, die für alle Teile des Systems gleichermaßen gültig sind. Beispiele dafür sind Standardsoftware, wie Office-Pakete, oder das Virenschutzkonzept.
Schicht 2 beschäftigt sich mit baulich-physischen Maßnahmen wie Serverräumen oder der Verkabelung.
Schicht 3 betrachtet die einzelnen IT-Systeme näher wie beispielsweise Unix-Server, Unix-Client, Windows-Server oder Windows-Client.
Schicht 4 betrifft die Vernetzungsaspekte wie Netzmanagement, WLANs oder VPNs.
Schicht 5 beschäftigt sich schlussendlich mit den IT-Anwendungen wie Active Directory, Web-Server oder Mail-Server. Am Ende wird die Modellierung nochmals auf ihre Vollständigkeit überprüft.

Im zweiten Schritt der Grundschutzanalyse werden die bisher umgesetzten Maßnahmen mit den in den Maßnahmekatalogen ([GSHB], [OeSiH]) vorgeschlagenen verglichen. Dies liefert eine Liste von fehlenden Maßnahmen. Es kann natürlich vorkommen, dass Maßnahmen aus bestimmten Gründen nicht umgesetzt werden. Ist dies der Fall, so muss das dokumentiert werden.

Als Endergebnis der Grundschutzanalyse erhält man also eine Liste von noch umzusetzenden Maßnahmen.

4.2.3 Sicherheitskonzept

Nach der Durchführung der Risikoanalyse wird, aufbauend auf den Ergebnissen dieser, ein Sicherheitskonzept entwickelt. Ziel dabei ist es geeignete Maßnahmen auszuwählen. Dabei sind Kosten und Nutzen zu beachten. Es sollte also darauf geachtet werden, dass möglichst jene Maßnahmen gewählt werden, bei denen das Kosten-Nutzenverhältnis optimal ist (vgl. Abbildung 4.3). Das Sicherheitskonzept sollte also folgende Punkte

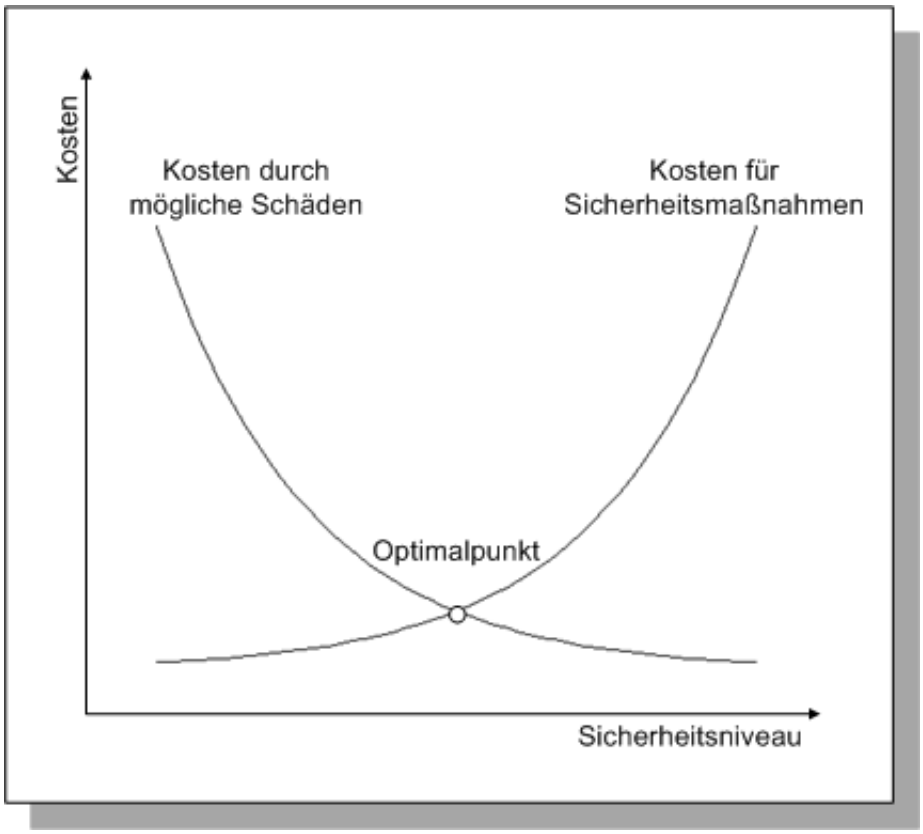

Abbildung 4.3: Auffindung des Optimalpunkts hinsichtlich der Kosten-Nutzen Relation bei der Wahl von Sicherheitsmaßnahmen

beinhalten:

- Beschreibung des Ausgangszustandes
- durchzuführende Maßnahmen
- Begründung dieser Maßnahmen
- Prioritäten-, Termin- und Ressourcenplanung

Zur Erstellung des Sicherheitskonzeptes sind dabei vier Schritte notwendig:

1. Auswahl der Maßnahmen
   Zuerst sind die möglichen Maßnahmen je nach Art (technisch, baulich, organisatorisch, personell) und nach Anwendungsbereich (also schulweit oder systems-

pezifisch) einzuteilen. Dabei können die unterschiedlichen Systeme in Gruppen eingeteilt werden (etwa „Geräte ohne Netzwerkanbindung“, „Arbeitsplatzrechner“, „Server“).
Beispielsweise ist ein abgesperrter Serverraum eine bauliche, systemspezifische Maßnahme, ein Virenschutz eine technische, systemweite Maßnahme.
Die möglichen Maßnahmen können, da vom Grundschutzansatz ausgegangen wird, aus Maßnahmenkatalogen entnommen werden, beispielsweise dem Maßnahmenkatalogen zum Grundschutz des BSI [GSHB] oder Teil 2 des Österreichischen Informationssicherheits-Handbuchs [OeSiH].
Danach ist eine Bewertung der Maßnahmen notwendig. Erfüllen diese den geplanten Zweck? Welche Bedrohungen werden durch diese Maßnahme abgeschirmt? Wie sieht es mit der Verträglichkeit mit anderen gesetzten Maßnahmen aus? Schlussendlich müssen noch die zeitlichen, finanziellen und technischen Rahmenbedingungen beachtet werden.

2. Restrisikoakzeptanz
   Durch die vorangegangene Risikoanalyse ist das Restrisiko bereits bekannt. Die noch übrigen Risiken sind nun als „akzeptabel“ oder „nicht akzeptabel“ zu kennzeichnen, wobei letztere danach natürlich einer weitere Prüfung benötigen.

3. Sicherheitsrichtlinien
   Für alle Systeme sollen eigene Richtlinien erstellt werden. Beispielsweise Sicherheitsrichtlinien für Arbeitsplatzrechner, mobile Geräte oder das Internet.
   Diese sollen eine Definition des Systems, also Ziele und Funktionalität, sowie Informationssicherheitsziele, beinhalten und aktuell gehalten werden.

4. Informationssicherheitsplan
   Im Informationssicherheitsplan wird beschrieben, wie die Maßnahmen eines Systems umgesetzt werden. Dabei soll für jedes System eine Liste der zu setzenden Maßnahmen erstellt werden. In dieser soll der Grad der Umsetzung („umgesetzt“ bzw. „noch umzusetzen“) jeder Maßnahme, die Priorität, sowie die dafür nötigen Kosten festgehalten werden.

Wie auch die Informationssicherheitspolitik muss das Sicherheitskonzept laufend aktualisiert werden. Dies kann unterschiedliche Gründe haben, so zum Beispiel das Eintreten sicherheitsrelevanter Ereignisse, wie etwa ein Angriff auf ein Service, das Bekanntwerden einer neuen Sicherheitslücke in einer Anwendung oder auch einfach nur ein Update nach einem festgesetzten Zeitraum.

4.2.4 Umsetzung

Die konkrete Umsetzung des Informationssicherheitsplanes erfolgt in drei Schritten.

1. Implementierung
   Die Maßnahmen werden, dem Informationssicherheitsplan folgend, je nach Priorität und den zur Verfügung stehenden Mitteln umgesetzt.

2. Tests
   Die nötigen Maßnahmen müssen korrekt umgesetzt werden. Dazu ist es vor allem bei technischen Maßnahmen nötig, diese in einer Testumgebung zu implementieren und zu testen. Dadurch soll die Funktionstüchtigkeit im regulären Einsatz abgesichert werden.

3. Prüfung hinsichtlich der Informationssicherheitspolitik
   Die Maßnahmen müssen lückenlos und korrekt implementiert werden. Dies lässt sich anhand eines Vergleichs mit der Informationssicherheitspolitik gewährleisten.

Gleichzeitig mit der Umsetzung des Informationssicherheitsplanes sollten Sensibilisierungs- und Schulungsmaßnahmen gesetzt werden. Ziel dabei ist es, bei den Anwendern ein Grundverständnis für Informationssicherheit zu wecken und diese, in den für sie notwendigen Bereichen für Sicherheitsmaßnahmen, zu schulen.

Notwendigkeit der Anwenderschulung

> „Mit neuesten Trends aus dem Bereich der Informationssicherheit konnte Joachim Seidler, Spezialist vom IT-Marktforscher IDC, aufwarten: 'Wie uns führende IT-Abteilungsleiter versicherten, ist der Wunsch nach verbesserter und erweiterter Mitarbeiterschulung momentan in der Wirtschaft größer als jener nach weiteren technischen Maßnahmen.'“[3]

Aus vorangegangenem Zitat lässt sich leicht die große Bedeutung der Mitarbeiterschulung in Unternehmen ablesen. Nicht nur in „normalen“ Unternehmen sondern auch in Schulen ist die Sensibilisierung und Schulung der Anwender von unverzichtbarer Bedeutung. Dabei ist eine Schulung nicht ausreichend, da diese alleine noch nicht ausreichend für ein sicherheitsgerechtes Verhalten der Anwender ist. Aus diesem Grund muss Anwendern durch Sensibilisierungsmaßnahmen die Notwendigkeit von Sicherheitsmaßnahmen bewusst gemacht werden. Dadurch soll den Anwendern der Stellenwert und die Wichtigkeit von Informationssicherheit klar werden.

Ziele der Anwenderschulung

Die durch Sensibiliserungs- und Schulungsmaßnahmen zu erreichenden Ziele sind:

- Die Anwender sollen über die Informationssicherheitspolitik der Schule Bescheid wissen.
- Die Anwender sollen die Informationssicherheitsziele kennen.
- Die Anwender sollen die Bedeutung der Informationssicherheit für die Schule erkennen.

[3] Vgl. e-center, "Datenschutz privat und im Unternehmen: e-center fragt nach", 2008. Online erhältlich via URL: <http://www.e-center.co.at/ecenter/security8/sec08.pdf>, (10. April 2009).

- Die Anwender sollen die Verantwortlichen hinsichtlich der Informationssicherheit kennen.
- Die Anwender sollen über die Sicherheitsklassifizierung von Daten Bescheid wissen.
- Die Anwender sollen die Bedrohungen der IT kennen.
- Die Anwender sollen die Auswirkung von sicherheitsrelevanten Ereignissen auf die gesamte Schule kennen.
- Die Anwender sollen die Notwendigkeit, sicherheitsrelevante Ereignisse umgehend zu melden, erkennen.
- Die Anwender sollen die Konsequenzen bei Nichtbeachtung der Sicherheitsvorgaben kennen.
- Die Anwender sollen über die Sicherheit der eingesetzten Software Bescheid wissen.

Für Lehrer, die Zugriff auf das Verwaltungsnetzwerk haben, gelten weitere Ziele:

- Die Anwender sollen Grundlagen der Netzwerksicherheit kennen.
- Die Anwender sollen über den Datenschutz personenbezogener Daten Bescheid wissen.

Inhalt der Anwenderschulung
Um die Anwender möglichst lückenlos zu Schulen muss überlegt werden, welche Inhalte für Lehrer und Schüler relevant sind. Dazu ist es nötig ein Curriculum zu entwickeln. Dies soll in Kapitel 5 versucht werden.

4.2.5 Laufender Betrieb

Das eigentliche Ziel eines ISMS ist es schlussendlich, das erreichte Sicherheitsniveau im laufenden Betrieb aufrechtzuerhalten.

Damit verbunden ist die regelmäßige Wartung aller eingesetzten Systeme und Maßnahmen. Zum Beispiel hat das beste Backup-System keine Wirkung, wenn die erstellten Sicherungsdaten nicht regelmäßig auf deren Integrität und auf die Wiederherstellungs-Fähigkeit getestet werden.
Ein weiter wichtiger Punkt ist die regelmäßige Überprüfung der Maßnahmen hinsichtlich der Informationssicherheitspolitik der Schule. Dabei soll durch Stichproben der korrekte Einsatz einzelner Maßnahmen überprüft werden.
Außerdem sollte eine ständige Überwachung der eingesetzten Systeme, mit dem Ziel, das erreichte Sicherheitsniveau beizubehalten, durchgeführt werden.

Im laufenden Betrieb von IT-Systemen kann es immer wieder zu Änderungen an den einzelnen Systemen kommen. Sei es durch Aktualisierung von Software, den Austausch

von Hardware oder durch bauliche Änderungen. In einem solchen Fall sind die daraus resultierenden Änderungen an den Sicherheitsmaßnahmen zu dokumentieren. Je nach Grad der Änderungen kann es auch nötig sein, erneut eine Risikoanalyse durchzuführen, etwa beim Einsatz völlig neuer Systeme.

Schlussendlich ist es sehr wahrscheinlich, dass es im laufenden Betrieb zu sicherheitsrelevanten Zwischenfällen kommt. Darum sollten alle Anwender darüber Bescheid wissen, was in einem solchen Fall zu tun, und wer zu informieren ist. Diese Informationen sollten im Zuge der Sensibilisierungs- und Schulungsmaßnahmen übermittelt werden.

Kapitel 5

Anwendersensibilisierung und -schulung

Ziel dieses Kapitels ist es die Wichtigkeit der Schulung und Sensibilisierung der IT-Anwender an Schulen aufzuzeigen. Außerdem sollen didaktische Überlegungen zur Schulung der einzelnen Benutzergruppen, also Schüler und Lehrer, an österreichischen Schulen durchgeführt werden. Schlussendlich sollen die Unterschiede bei der Schulung der beiden Benutzergruppen anhand einer Beispielschulung zum Thema „Passwortsicherheit“ verdeutlicht werden.

5.1 Vorüberlegungen zur Curriculumsentwicklung

Ein Curriculum sollte Lernziele, Lerninhalte und Lernorganisation (Methoden, Strategien, Evaluation) umfassen. Um diese Überlegungen für das Thema „Anwenderschulung zur Informationssicherheit in Schulen“ durchzuführen, gilt es zunächst einmal sich darüber klar zu werden, welches Ziel mit der Schulung erreicht werden soll.

Ziel ist es, die Anwender über die unterschiedlichen Gefahren für die Informationssicherheit in Schulen aufzuklären und sie hinsichtlich einer sicherheitsbewussten Benutzung der IT-Systeme zu schulen.

Schüler und Lehrer unterscheiden sich dabei sowohl im Lernen, aufgrund ihrer unterschiedlichen Lebenserfahrung, als auch bei den Aufgaben und Pflichten im Schulalltag. Deshalb ist es auch notwendig, unterschiedliche Curricula für Schüler und Lehrer zu entwickeln.

5.1.1 Lehrer

Bei der Entwicklung eines Curriculums zur Schulung der Lehrer muss darauf geachtet werden, dass im Dienst stehende Lehrer in einem anderen Rahmen geschult werden

müssen als in Ausbildung stehende Lehrer. Weiters muss zwischen Informatik-Lehrern und den übrigen Lehrern unterschieden werden.

Informatik Lehrer können im Rahmen ihrer Ausbildung an der Universität eine Einführung in die Informationssicherheit erhalten. Diese sollte im Rahmen der Evaluierungsmaßnahmen überprüft werden. Aus meiner Sicht wäre es aufgrund der immer größer werdenden Bedeutung der Informationstechnologie für die Gesellschaft notwendig, auch Studenten, die kein Informatik-bezogenes Studium absolvieren, ein Basiswissen in Informationssicherheit zu vermitteln. Damit würden auch Lehrer, die nicht Informatik unterrichten ein solches Basiswissen besitzen.

Für im Dienst stehende Lehrer muss eine grundlegende Einführung in die Thematik in geeigneten Kursen durchgeführt werden.

5.1.2 Schüler

Bei der Entwicklung eines Curriculums für die Schulung der Schüler sollte ebenfalls die immer größer werdende Bedeutung der Informationstechnologie für die Gesellschaft bedacht werden. Daher ist es aus meiner Sicht empfehlenswert den Schülern nicht nur Inhalte zu vermitteln, die unmittelbar für die Informationssicherheit in Schulen wichtig sind.
Vielmehr ist es empfehlenswert, Schülern so früh wie möglich in einem fächerübergreifenden Unterricht eine Basisausbildung in Informationssicherheit zu ermöglichen. Dadurch sollen alle Schüler bis zum Schulabschluss grundlegende Kenntnisse der Informationssicherheit erworben haben und vor allem auch dafür sensibilisiert werden.

Es bietet sich daher an, nicht nur ein Curriculum zur Schulung der Schüler hinsichtlich der Informationssicherheit in Schulen, sondern sogar ein Curriculum für ein Basiswissen der Informationssicherheit zu entwickeln.

5.2 Curriculum Schüler

5.2.1 Lernorganisation

Im Rahmen des Schulunterrichts soll bei den Schülern ein grundlegendes Verständnis hinsichtlich der Informationssicherheit geweckt werden. Tiefergehende Einblicke und Zusammenhänge bleiben einer weiterführenden Ausbildung (Studium, ...) überlassen.

Dabei sollte der Unterricht in Informationssicherheit nicht alleine dem Informatikunterricht überlassen werden. Besonders im sozialwissenschaftlichen Unterricht (Geschichte, Sozialkunde und Politische Bildung, Englisch, ...) soll das Thema ebenfalls aufgegriffen werden. Dabei sollen gesellschaftliche Bezüge zum Thema Sicherheit hergestellt und die Auswirkungen auf die Gesellschaft aufgezeigt werden [GI].

Die unterschiedlichen Aspekte der Informationssicherheit sollen dabei, je nach Fach und Alter der Schüler, unterschiedlich gewichtet werden.

Um die Schüler den Schülern nicht nur Theorie zu vermitteln ist es notwendig Projekte mit ihnen durchzuführen. Viele Aspekte der Informationssicherheit lassen sich sehr gut durch Übungen in einem Computerlabor unterrichten. Einzelne Themen können auch als Referat ausgearbeitet oder in der Gruppe diskutiert werden.

Für die Jugendlichen ist es besonders wichtig, Themen anzusprechen, mit denen sie im täglichen Leben konfrontiert werden. Es ist wichtig sie auf Gefahren im Zusammenhang mit dem Internet und den von ihnen preisgegebenen Informationen zu sensibilisieren. Die Sensibilisierung ist bei Schülern dabei wichtiger als technische Inhalte.

Eine Evaluation der Schüler kann etwa durch Übungsprotokolle ein eigenständiges Projekt der Schüler oder eine Überprüfung des Erreichens der Lernziele durch einen Test erfolgen.

5.2.2 Lerninhalte

1. Grundlagen: Den Schülern sollen wichtige Begriffe im Zusammenhang mit Informationssicherheit vertraut gemacht werden.
   - Was bedeuten Vertraulichkeit, Integrität und Verfügbarkeit?
   - Was ist ein Risiko?
   - Zugangskontrolle (Passwörter, Biometrie, Chipkarten, ...)
   - Kryptographie
2. Bedrohungen:
   - Was sind Viren, Würmer und Trojaner?
   - Wie funktionieren sie und welche Schwachstellen nutzen sie aus?
   - Was ist SPAM und Phishing?
   - Wie kann Datenverlust geschehen?
3. Schutz:
   - Was sind die wichtigsten Schutzmechanismen?
   - Wozu benötigt man einen Virenschutz?
   - Was ist eine Firewall?
   - Warum müssen Programme aktualisiert werden?
   - Was sind sichere Passwörter?
   - Wie funktioniert sichere E-Mail-Kommunikation?

- Wie schützt man seine Privatsphäre im Internet (Chaträume, Social Networking, ...)?
- Wie werden Daten gesichert?

4. Gesellschaftliche Auswirkungen:
   - Verlust der Privatsphäre im Internet
   - Missbrauch von E-Mails
   - Elektronische Wahlen
   - Gesetzliche Regelungen (Datenschutz, Urheberrecht, ...)

5.2.3 Lernziele

Die Lernziele wurden nach der Taxonomie von Bloom ausgearbeitet.

- Die Schüler sollen die Grundlagen der Informationssicherheit verstehen.
- Die Schüler sollen ein System hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit analysieren können.
- Die Schüler sollen den Sinn von Zugangskontrollen verstehen und die unterschiedlichen Ansätze bewerten können.
- Die Schüler sollen Grundlagen der Kryptographie verstehen und in einfachen Beispielen anwenden können.
- Die Schüler sollen die unterschiedlichen Bedrohungen an die Informationssicherheit kennen.
- Die Schüler sollen Angriffe (aktiv und passiv) erkennen und wirksame Schutzmechanismen auswählen können.
- Die Schüler sollen die Funktionsweise von wichtigen Schutzmechanismen verstehen.
- Die Schüler sollen in der Lage sein, sichere E-Mail-Kommunikation durchzuführen.
- Die Schüler sollen die Notwendigkeit von Software-Aktualisierungen erkennen.
- Die Schüler sollen sich ihrer mangelnden Privatsphäre im Internet bewusst sein.
- Die Schüler sollen gesetzliche Regelungen (wie Datenschutz oder Urheberrecht) wissen.
- Die Schüler sollen die gesellschaftlichen Auswirkungen der Informationstechnologie bewerten können.

5.3 Curriculum Lehrer

5.3.1 Lernorganisation

Da auch Lehrer, die nicht Informatik unterrichten, in vielen Situationen auf den Gebrauch von Informationstechnologie angewiesen sind, benötigen sie für ihre Arbeit ein grundlegendes Verständnis für Informationssicherheit. Dabei ist es vor allem wichtig besonders jene Lehrer, die noch wenig Erfahrung im Umgang mit IT-Systemen gesammelt haben, in angemessener Weise zu schulen.

Im Rahmen von Fortbildungsmaßnahmen zur Verwendung von IT-Systemen im Schulgebrauch muss auch auf die Sicherheit dieser Systeme eingegangen werden. Darüber hinaus sollen in eigens dafür abgehaltenen Seminaren die Grundlagen der Informationssicherheit erlernt werden. In diesem Zusammenhang würde sich auch der Erwerb eines Zertifikats zur Informationssicherheit (z. B.: OCG IT-Security Zertifikat[1]) anbieten.

Aufgrund der Verarbeitung sensibler Daten im Verwaltungsnetzwerk von Schulen müssen Lehrer besonders dahingehend geschult werden, die Vertraulichkeit, Integrität und Verfügbarkeit dieser Daten zu gewährleisten.

Zur Evaluierung des Lernfortschritts der Lehrer bieten sich einerseits die Erlangung eines Zertifikats und andererseits Gespräche des IT-Sicherheitsverantwortlichen mit den einzelnen Lehrern an.

5.3.2 Lerninhalte

1. Grundlagen:
   - Grundbegriffe (Vertraulichkeit, Integrität, Verfügbarkeit, Risiko, ...)
   - Wert von Informationen
2. Bedrohungen:
   - Bedrohungen durch die Umwelt (höhere Gewalt, ...)
   - Bedrohungen durch Personen (Social Engineering, Hacker, ...)
   - technische Bedrohungen (Viren, Würmer, Trojaner, ...)
   - SPAM, Phishing
3. Schutz:
   - wichtige Schutzmaßnehmen kennenlernen (Virenschutz, Firewalls, ...)
   - Funktionsweise der Schutzmaßnahmen

[1] vgl. OCG, „OCG IT-Security Syllabus Version 1.0“, 2008. Online erhältlich via URL: <http://www.ocg.at/zertifikate/downloads/it-security-syll-V1.pdf> (10. April 2009).

- Zugangskontrollen (Passwörter, Chipkarten, Biometrie, ...)

4. Schutz des Verwaltungsnetzwerkes:
   - grundsätzliches Verständnis für den Aufbau des Netzwerkes
   - rechtliche Grundlagen zum Schutz personenbezogener Daten (DSG 2000)
   - Kenntnis der Verschlüsselungssoftware zum Schutz der Vertraulichkeit und Integrität der Daten
   - Verständnis für die Notwendigkeit eines Backups zur Wahrung der Verfügbarkeit der Daten

5.3.3 Lernziele

Die Lernziele wurden nach der Taxonomie von Bloom ausgearbeitet.

- Die Lehrer sollen die Grundbegriffe der Informationssicherheit (wie Vertraulichkeit, Integrität und Verfügbarkeit) verstehen und eine Komponente eines IT-Systems dahingehend analysieren können.
- Die Lehrer sollen den Wert von Informationen erkennen können und so Daten klassifizieren können.
- Die Lehrer sollen Bedrohungen, die von der Umwelt ausgehen, kennen und eine dafür angemessene Reaktion finden können.
- Die Lehrer sollen wissen, welche Bedrohungen von Personen ausgehen und sich angemessen davor schützen können.
- Die Lehrer sollen technische Bedrohungen kennen und die davon ausgehende Gefahr bewerten können.
- Die Lehrer sollen die Funktionsweise der wichtigsten Schutzmechanismen verstehen und sie in den richtigen Situationen anwenden können.
- Die Lehrer sollen über die Qualität der unterschiedlichen Arten zur Zugangskontrolle Bescheid wissen.
- Die Lehrer sollen die Wichtigkeit der Informationssicherheit im Verwaltungsnetzwerk bewerten können.
- Die Lehrer sollen den Aufbau des Netzwerkes verstehen.
- Die Lehrer sollen die rechtlichen Anforderungen an die Informationssicherheit im Verwaltungsnetzwerk kennen.
- Die Lehrer sollen Verschlüsselungssoftware anwenden können.
- Die Lehrer sollen in der Lage sein, ein Backup der Verwaltungsdaten durchzuführen.

5.4 Beispiel: Passwortsicherheit

Um die Unterschiede zwischen Lehrern und Schülern, also Erwachsenen und Jugendlichen, hinsichtlich der Schulung und Sensibilisierung zur Informationssicherheit zu verdeutlichen möchte ich im Folgenden beispielhaft eine Schulung zum Thema „Passwortsicherheit“ für die beiden Gruppen anführen.

5.4.1 Didaktische Vorüberlegungen

Eine Didaktik zur Anwenderschulung in der IT-Sicherheit muss sich mit der Frage beschäftigen, „wer was wann mit wem wo wie womit warum und wozu lernen soll“[2].

Das „wer“ ist in Schulen eindeutig bestimmt. Lehrer und Schüler der jeweiligen Schule sollen, hinsichtlich der für die Informationssicherheit an der Schule notwendigen Inhalte, geschult und sensibilisiert werden. Dies wird jedoch insofern zu einer schwierigen Herausforderung als die Gruppe der Anwender in ihrer Gesamtheit sehr heterogen ist. Die Schüler sind mit der heutigen Technik groß geworden und haben dadurch einen völlig anderen Zugang zu Computern als der Großteil der im Dienst befindlichen Lehrer.
Die Gruppe der Lehrer ist in sich auch sehr heterogen. Viele Lehrer haben nicht die Zeit, teilweise fehlt sicherlich auch das Interesse, sich generell mit Informationstechnologie und speziell mit dem Thema IT-Sicherheit auseinanderzusetzen. Dies wurde mir auch in den Interviews bestätigt:

> Markus H.: „Generell ... ahm ... ja ... es wäre halt nett, ich meine ich verstehe es, es ist in jedem Beruf so, ahm, dass man nicht computertechnisch so gut drauf ist [...]und ich würde mir manches mal einfach eine höhere IT-Fitness wünschen, generell halt.“[3]

Deshalb ist bei Lehrern auch die Frage des „wie, warum und wozu“ sehr wichtig. Den Lehrern muss klar gemacht werden, warum Informationssicherheit eine große Bedeutung für das Funktionieren der IT-Systeme hat und welche Maßnahmen von jedem einzelnen gesetzt werden können, um diese Sicherheit zu gewährleisten. Da wohl eher nur wenige Lehrer dazu bereit sind, sich in ihrer Freizeit mit dem Thema auseinanderzusetzen wäre es eine Möglichkeit dies im Rahmen von Fortbildungen durchzuführen. Einen sehr guten Ansatz dazu gibt es seit April 2008 durch das IT-Security Zertifikat der Österreichischen Computergesellschaft (OCG). Dieses Zertifikat zielt auf Anwender in KMUs ab und ist damit auch für die Schulung von Lehrern bestens geeignet. Im Syllabus[4] des Zertifikats sind die dabei gelehrten Inhalte zu finden.

---

[2] Vgl. Wolf-Rüdiger Wagner, „Hat die Didaktik Antworten auf die technische Herausforderung?“, in: G. Banse u. a., „Zur Didaktik der IT-Sicherheit“, SecuMedia, Ingelheim, 1999.

[3] Vgl. Anhang B, Zeile 402-404

[4] Vgl. OCG, „OCG IT-Security Syllabus Version 1.0“, 2008. Online erhältlich via URL: `<http://www.ocg.at/zertifikate/downloads/it-security-syll-V1.pdf>` (10. April 2009).

Das Problem bei der Schulung von Erwachsenen ist, dass die Informationstechnologie oft nicht zum unmittelbaren Erfahrungsbereich gehört. Durch metaphorische Übertragungen der Alltagssprache soll den Benutzern von Computern der Umgang mit diesen erleichtert werden. Doch genau dies kann zum Problem bei unbedarften Anwendern werden. So sind sich viele Anwender nicht bewusst, dass „Löschen“ im alltäglichen Sinn nicht exakt dem „Löschen“ einer Datei auf einem Computer entspricht. Löscht man etwa die Tafel, so ist die darauf befindliche Information unwiderruflich entfernt. Löscht man hingegen eine Datei auf einem Computer durch Drücken der „Entfernen“-Taste, so wird sie nur in den Papierkorb verschoben. Selbst wenn dieser „geleert“ wird, sind die Informationen keineswegs vollends entfernt und können durch gewisse Techniken wiederhergestellt werden. Ein anderes Beispiel wäre der direkte Vergleich „Email“ - „Brief“. Verschickt man einen handgeschriebenen Brief, so erhält der Empfänger ein und dasselbe Blatt Papier. Bei Emails hingegen wird im Prinzip eine Kopie dessen, was man geschrieben hat, versandt.
Fallstricke wie diese können es besonderes für ältere Menschen schwer machen, sich der Informationssicherheit bewusst zu werden.

Die Frage nach dem „wie, warum und wozu“ lässt sich bei der Gruppe der Schüler etwas leichter beantworten. Schüler können im Rahmen des Informatikunterrichts generell auf die Wichtigkeit von Informationssicherheit aufmerksam gemacht werden. Je früher die Schüler dabei geschult werden, desto einfacher. Bereits für Kinder im Volksschulalter werden etwa genau für diesen Zweck Informationen auf der Website der Initiative „Sicher im Internet“[5] zur Verfügung gestellt.

Auch das „was“ bei der Schulung der Lehrer unterscheidet sich in gewissen Dingen von dem „was“ der Schüler. So ist es für Erwachsene beispielsweise selbstverständlich, persönliche Daten zu schützen. Schüler hingegen geben viele Informationen über sich selbst, beispielsweise im Rahmen einer Social Networking Plattform, wie zum Beispiel das populäre schuelerVZ[6], preis, ohne sich im Klaren zu sein, wer alles auf diese Informationen zugreifen kann und wie diese verarbeitet werden. Deshalb wird auch hinsichtlich der Inhalte zu differenzieren sein.

5.4.2 Wahl einer Methode

Aufgrund der Heterogenität der Gruppen Lehrer und Schüler untereinander und auch in den einzelnen Gruppen, kann die Schulung nicht als Vortrag oder ähnliches durchgeführt werden. Der Stoff muss für Schüler und Lehrer unterschiedlich aufbereitet werden.

Die beiden Gruppen sind in sich selbst auch meist noch heterogen. Daher bietet sich aus meiner Sicht als Methode die Verwendung einer eLearning-Plattform an. Dabei kann jeder Benutzer selbst sein Lernen organisieren indem er in eigenem Lerntempo

[5] Vgl. sicher-im-internet.at, „Sei sicher im Internet“, 2005. Online erhältlich via URL: `<http://www.sicher-im-internet.at/jugend/>` (10. April 2009).

[6] Vgl. `<http://www.schuelervz.net/>`

arbeiten kann. Das Problem der Heterogenität in Gruppen lässt sich dadurch umgehen, dass eine Differenzierung durch unterschiedliche Materialien erzielt werden kann. Wer mit den Basisinformationen unterfordert ist, kann sich durch Zusatzmaterial in gewissen Gebieten vertiefen. Dies ist vor allem beim Unterricht von Schülern von großer Bedeutung.

Für die Umsetzung der Inhalte zum Thema „Passwortsicherheit“ habe ich mich für die Verwendung der eLearning-Plattform Moodle entschieden. Zwar ist die Content-Aufbereitung bei dieser Lernplattform aus meiner Sicht nicht so leicht möglich, allerdings kann die Lernplattform sehr leicht erweitert und so an die individuellen Bedürfnisse angepasst werden.

5.4.3 Schulung für Lehrer

Die meisten Erwachsenen müssen sich bereits viele Passwörter merken. Nichtsdestotrotz ist es unerlässlich unterschiedliche und gute Passwörter zu verwenden [Gehringer]. In dieser Schulung soll den Lehrern, aufbauend auf den Informationen zum OCG Syllabus, beigebracht werden, wie Passwörter gewählt werden sollen. Die Lehrer sollen im Laufe der Schulung zur Passwortsicherheit folgende Lernziele erreichen:

- Die Lehrer sollen Passwortregeln kennen.
- Die Lehrer sollen wissen wie ein gutes Passwort aufgebaut ist.

Inhalt
Beim Einloggen in die Plattform sieht der Lehrer den in Abbildung 5.1 dargestellten Bildschirm.

Es können 5 Punkte durchgearbeitet werden. Die ersten 3 stellen Informationen zum Wissenserwerb zur Verfügung. Punkt 4 bietet Interessierten die Möglichkeit über weiterführende Links mehr Informationen zum Thema „Passwortsicherheit“ zu erhalten. Punkt 5 stellt eine Überprüfung des erworbenen Wissens dars.

1. Wozu Passwörter?
Der Zugriffsschutz auf Daten oder Einrichtungen sollte durch einen Identitätsnachweis sichergestellt werden. Es gibt dazu bereits viele unterschiedliche Verfahren:

- Information die nur eine gewisse Person kennt (Passwörter, PINs, ...)
- möglichst fälschungssichere Hardware (Chipkarte, Schlüssel, ...)
- unverwechselbare persönliche Merkmale (Fingerabdruck, Iris, ...)

Für die meisten Einsatzzwecke haben sich Passwörter als Standard durchgesetzt, da die Methode, diese zum Schutz einzusetzen, leicht zu implementieren ist.

2. Welche Kriterien muss ein gutes Passwort erfüllen?
Ein gutes Passwort sollte folgende Eigenschaften haben:

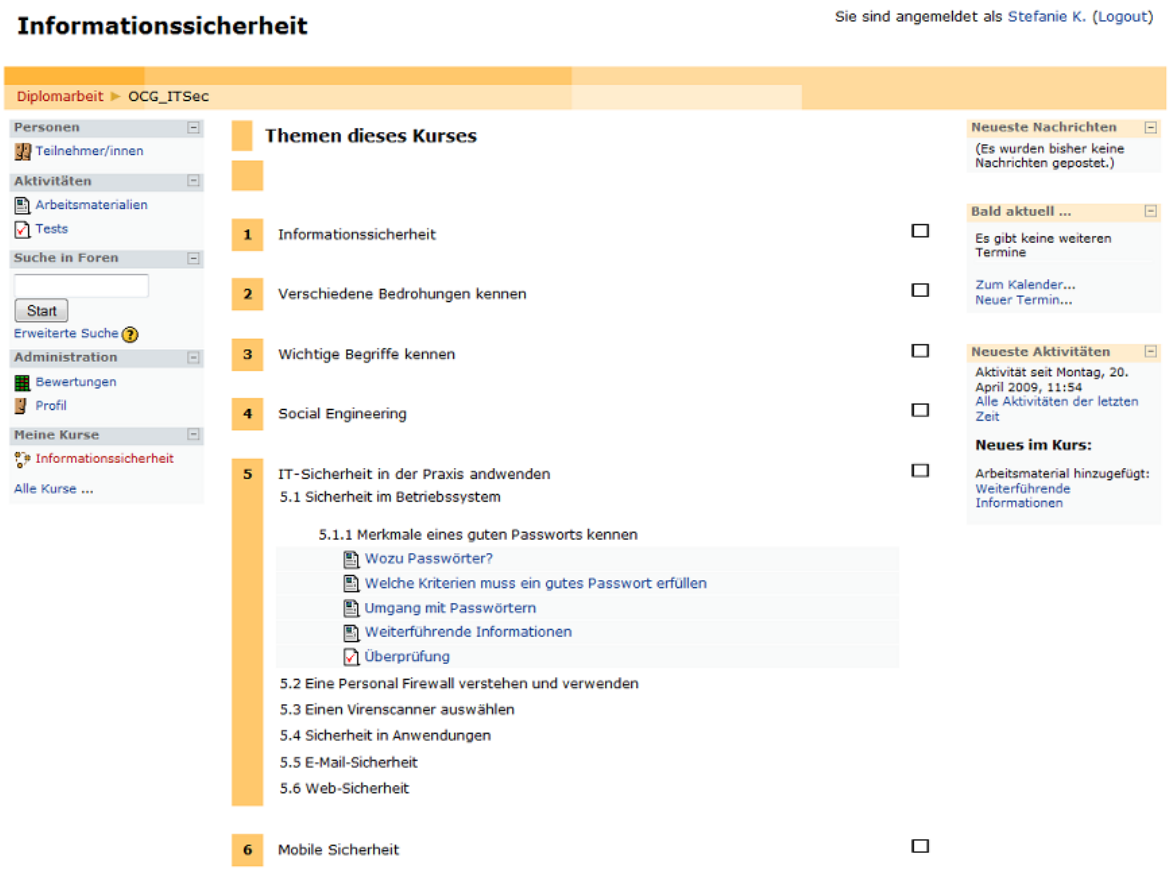

Abbildung 5.1: Startbildschirm beim Einloggen in die Schulung für Lehrer

- Länge: Das Passwort sollte aus mindestens 8 Zeichen bestehen.
- Inhalt: Das Passwort sollte in keinem Wörterbuch stehen. Es soll nicht in Zusammenhang mit dem Benutzer gebracht werden können (Name des Haustiers, Geburtsdatum, ...)
- Einsatz: Jedes Passwort soll nur für einen Zweck eingesetzt werden.
- Zeichen: Das Passwort sollte sowohl Klein- als auch Großbuchstaben, Sonderzeichen und Zahlen enthalten.

Ein gutes Passwort wäre also beispielsweise:
MKhM!Si1Ja.
Eine gute Möglichkeit solche Passwörter zu generieren ist es sich einen Satz zu überlegen, den man leicht im Kopf behält. Aus diesem Satz generiert man dann das Passwort. Obiges Beispiel ist folgendermaßen entstanden: **M**eine **K**atze **h**eißt **M**unki**!** **S**ie **i**st **1** **J**ahr **a**lt**.**
Bei der Generierung von Passwörtern durch Sätze sollte darauf geachtet werden, keine allgemein bekannten Sätze wie Zitate aus Musik oder Film zu verwenden. Dies würde des Knacken eines solchen Passworts erleichtern [Kuo].

3. Umgang mit Passwörtern
Es ist unter allen Umständen zu vermeiden, dass ein Passwort an eine unbefugte Person gerät. Deshalb sollten Passwörter nie ungeschützt einsehbar sein (Notizzettel, Post-It, ...).
Eine Möglichkeit zur Verwaltung mehrerer Passwörter bieten Programme wie Password Safe oder Keepass. Diese sind frei im Internet verfügbar. Dadurch soll das Notieren von Passwörtern auf Notizzetteln verhindert werden.
Weiteres sollte ein Passwort auch in regelmäßigen Abständen durch ein neues Passwort ersetzt werden.

4. Überprüfung
Durch die Überprüfung soll sichergestellt werden, dass die Lehrer gute von schlechten Passwörtern unterscheiden können und in der Lage sind, Passwortregeln zu nennen.

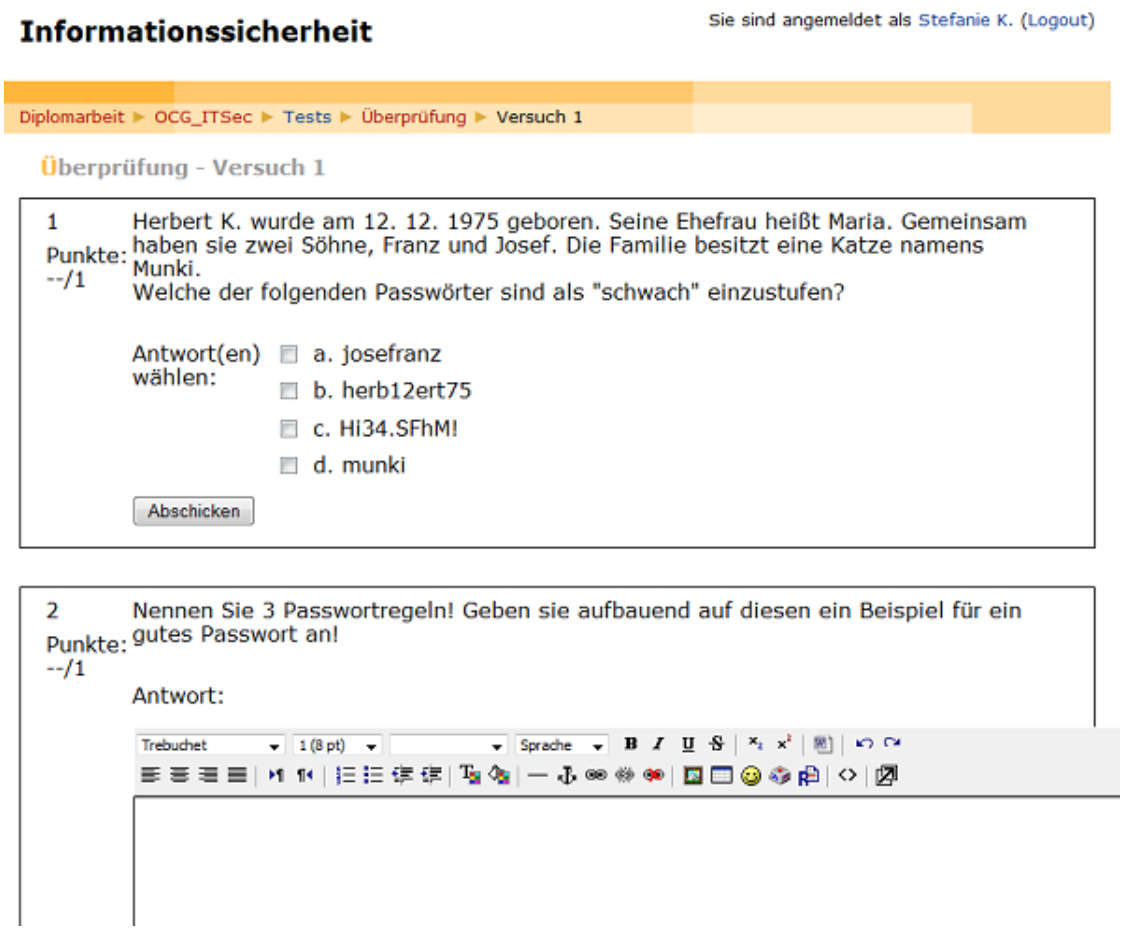

Abbildung 5.2: Überprüfung des Lernerfolgs für Lehrer

5.4.4 Schulung für Schüler

Passwörter werden als Zugangsbeschränkung fast überall eingesetzt. Sei es als PIN Code oder bei der Absicherung eines Mail-Accounts. Umso wichtiger ist es für Schüler über die Stärken und Schwächen von Passwörtern Bescheid zu wissen. Das nun Folgende ist für einen Informatikunterricht in der 9. Schulstufe konzipiert.

Die Schüler sollen im Laufe der Schulung zur Passwortsicherheit folgende Lernziele erreichen:

- Die Schüler sollen wissen wozu Passwörter eingesetzt werden.
- Die Schüler sollen ein schwaches Passwort erkennen.
- Die Schüler sollen in der Lage sein, gute Passwörter zu erzeugen.

Für Schüler bietet sich ein entdeckender Zugang an. Sie sollen mit Hilfe des Passwortcrackers „John the Ripper“ unterschiedlich schwierige Passwörter knacken. Dazu erhalten sie vom Lehrer eine geeignete Anleitung um sich mit dem Kommandozeilentool zurechtzufinden. Die Schüler sollen dann selbst auf Ideen stoßen, wie Passwörter verbessert werden können. Schüler die die ersten Passwörter recht schnell geknackt haben können mit schwierigeren Passwörtern beschäftigt werden.
Wichtig bei dem Einsatz von Tools wie „Jack the Ripper“ ist es, die Schüler auf den gezielten Einsatz hinzuweisen. Es sollte klar gemacht werden, dass es verboten ist zu versuchen die Passwörter eines Systems ohne Erlaubnis zu cracken.

Inhalt
Einstieg in das Thema Passwortsicherheit bietet eine Diskussion zum Thema „Einsatz von Passwörtern“. Die Schüler sollen hierbei selbst erarbeiten, in welchen Situationen Passwörter zum Einsatz kommen und warum gerade diese als Zugangsschutz für manche Systeme genutzt werden.

Im zweiten Teil der Arbeit bekommen die Schüler in Gruppen das Programm „John the Ripper“, eine Wordlist sowie mehrere Passwort-Dateien unterschiedlicher Schwierigkeitsstufen zur Verfügung gestellt. Zuerst wird mit allen Schülern gemeinsam der Umgang mit dem Programm geübt. Danach sollen die Schüler selbst versuchen unterschiedlich starke Passwörter zu knacken.

Ziel dieses Teils ist es, dass die Schüler erkennen, dass einfache Passwörter relativ rasch geknackt werden. Je komplexer die Passwörter werden, desto länger dauert der Crack-Vorgang.

Nach einiger Zeit soll eine weitere Diskussion stattfinden. Zuerst werden die gefundenen Passwörter verglichen, danach soll über die Qualität von Passwörtern diskutiert werden. Ziel dieser Diskussion ist es dabei, eben jene Punkte herauszufinden, die ein starkes Passwort ausmachen. Man vergleiche dazu die bei der Schulung der Lehrer angeführten Punkte.

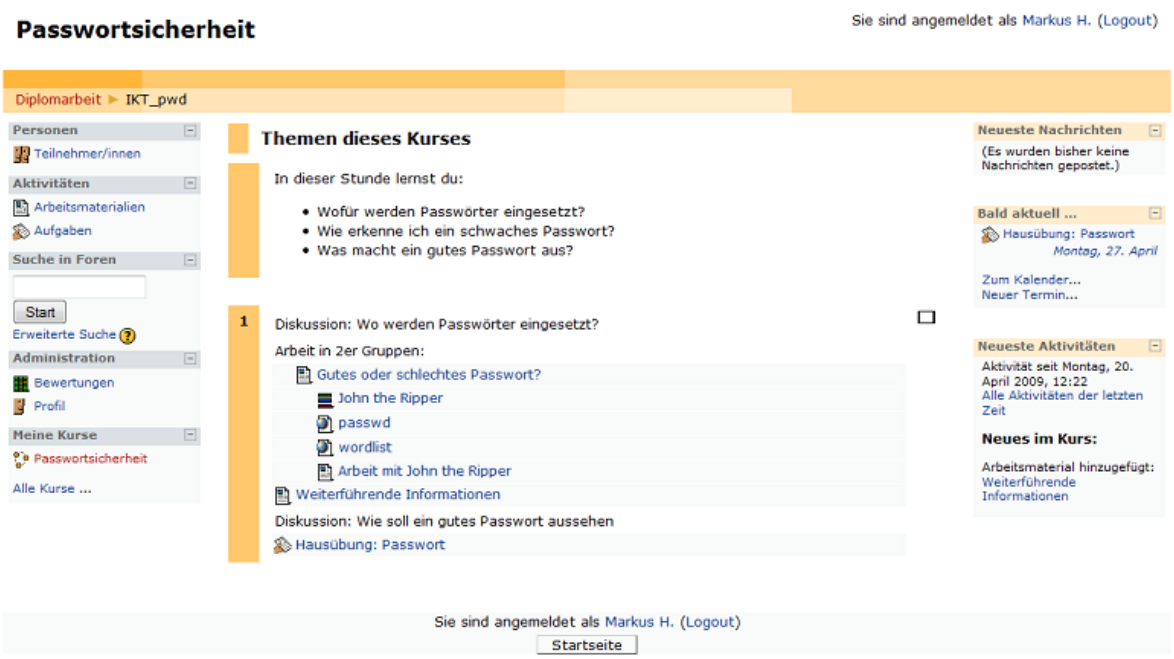

Abbildung 5.3: Startbildschirm beim Einloggen in die Schulung für Schüler

Als Hausübung sollen die Schüler schlussendlich 3 Beispiele für gute Passwörter angeben.

5.4.5 Unterschiede

Der Unterschied beim Lernen von Schülern und Lehrern bzw. Kindern und Erwachsenen allgemein ist groß.
Beim Lernen sind für Erwachsene vor Allem die Anforderungen Verwertbarkeit und Anschaulichkeit zu erfüllen. Die Informationen müssen also derart aufbereitet werden, dass Erwachsene den Sinn dahinter unmittelbar erkennen können. Gut gewählte Beispiele erleichtern so das Lernen von Erwachsenen. Kinder hingegen wachsen erst in eine bestehende Welt hinein. Durch selbstständiges Erarbeiten von Inhalten erkennen sie unmittelbar den Nutzen gewisser Dinge.

Genau aus diesem Grund wurden im Vorangegangenen die beiden unterschiedlichen Zugänge bei den Zielgruppen Lehrer und Schüler gewählt.
Für die Lehrer wurde der Inhalt konkret dargelegt und um geeignete Beispiele ergänzt. Für die Schüler wurde ein entdeckender Zugang gewählt. Durch experimentieren sollen die Schüler schlussendlich ähnliche Regeln, wie sie den Lehrern vorgegeben wurden, erarbeiten können.

Kapitel 6

Schlussbetrachtungen

6.1 Ergebnisse der Arbeit

Bei der Betrachtung des Themas „Informationssicherheit an Schulen mit besonderem Augenmerk auf die Anwenderschulung“ bin ich hauptsächlich von der Frage ausgegangen, welche Bedeutung der Informationssicherheit an österreichischen Schulen zugemessen wird.

Nach einer theoretischen Einarbeitung in das Thema habe ich mich darangemacht, einen Leitfaden für qualitative Interviews mit direkt Betroffenen in Schulen zu entwickeln. Die Aufgabe des Informationssicherheitsverantwortlichen bleibt meist am ohnehin schon ausgelasteten IT-Administrator hängen. Deshalb waren auch ebendiese meine Interviewpartner.

Bei der Analyse der Interviews (vgl. Kapitel 3) nach der grounded theory von Strauss entwickelte sich die Kategorie „Probleme“ immer mehr zur Schlüsselkategorie. Die angesprochenen Probleme sind dabei vielseitig. Von Seiten der übergeordneten Stellen in Form des Stadtschulrats bzw. der Landesschulräte gibt es zwar Weisungen hinsichtlich der Informationssicherheit, es wird jedoch kein Verantwortlicher bestimmt. Dies sollte durch die Schulleitung geschehen, die sich jedoch über die vielseitigen Bedrohungen nicht im Klaren ist.
Dass ein gewisser Schutzbedarf vorhanden ist, kam auch in den Interviews zur Sprache. Vor allem die in den Verwaltungsnetzwerken verarbeiteten Daten (personenbezogene Daten, Kontoinformationen, Schularbeits- und Maturaaufgaben, . . .) haben einen hohen Schutzbedarf. Den Schutzbedarf für das pädagogische Netz kategorisierten die Befragten jedoch durchgehend als „gering“.

Um systematisch geeignete Maßnahmen zur Herstellung von Informationssicherheit zu implementieren, bedarf es eines Informationssicherheitsmanagementsystems (ISMS).
Aufbauend auf dem Österreichischen Informationssicherheits-Handbuch [OeSiH] wurde in Kapitel 4 ein eben solches Schritt für Schritt beschrieben. Durch die Umsetzung dieses ISMS in Schulen können die Verfügbarkeit, Integrität und Vertraulichkeit der

verarbeitenden Daten in den Schulnetzwerken sichergestellt werden.

Ein wichtiger Punkt im laufenden Betrieb eines ISMS ist die Schulung und Sensibilisierung der Anwender. Ohne jegliche Schulungsmaßnahmen kann der sichere Betrieb eines IT-Systems nicht garantiert werden. Die Benutzer müssen sich über die Gefahren, die beispielsweise von Computerviren ausgehen, im Klaren sein.

In Schulen sind die Hauptanwender die Lehrer und Schüler. Aufgrund der Heterogenität der beiden Gruppen werden die Schulungs- und Sensibilisierungsmaßnahmen zusätzlich erschwert. Um die Schulungsmaßnahmen möglichst einheitlich zu gestalten ist die Entwicklung eines Curriculums notwendig. Ein solches wurde in Kapitel 5 entwickelt. Um den Unterschied bei der Schulung der beiden Benutzergruppen „Schüler“ und „Lehrer“ zu verdeutlichen, wurde zur Illustration eine Schulung am Beispiel "Passwortsicherheit"beschrieben. Dabei wurden sowohl didaktische Überlegungen zum Einsatz einer eLearning Plattform durchgeführt als auch konkrete Inhalte angegeben.

6.2 Diskussion und Ausblick

Ich bin mir vollkommen darüber im Klaren, dass meine in dieser Arbeit dargestellten theoretischen, methodologischen und analytischen Ausführungen alles andere als vollständig sind. Dies war jedoch auch nie mein Anspruch.

Die wohl größten Schwächen sind in den Kapiteln 3 und 5 zu finden.
Nach der Durchführung der Interviews und der Analyse dieser hätte ich mir gewünscht, noch weitere Interviewpartner zu der Thematik befragen zu können. Leider hätte dies vor allem meinen zeitlichen Rahmen gesprengt. So musste ich mich mit den bereits erhaltenen Informationen begnügen.
Ich habe mich auch durch die Auswahl der Interviewpartner zu sehr eingeschränkt. Durch die alleinige Befragung von IT-Sicherheitsverantwortlichen in Form von IT-Administratoren an Schulen habe ich nur einen Standpunkt erfahren können. Dadurch wurden die Standpunkte der Anwender und der der Schulleitung vernachlässigt. Es würde sich daher anbieten weiter Interviews mit Beamten des Stadtschulrats bzw. der Landesschulräte sowie mit Lehrern und Schülern durchzuführen. Dadurch könnte das Thema aus anderen Blickwinkeln betrachtet werden.

Nach der Erstellung der Hypothesen am Ende des dritten Kapitels hätte ich mir gewünscht diese durch eine quantitative Umfrage mit IT-Administratoren in ganz Österreich abzusichern bzw. mich mehr in das Thema und die Problematik vertiefen zu können. Es würde sich zum Beispiel anbieten die Fragen meines Interviewleitfadens dahingehend umzuformulieren, dass sie quantitativ auswertbar werden. Dadurch wäre es möglich eine größere Anzahl von IT-Sicherheitsverantwortlichen in Schulen zu dem Thema zu befragen.
Das Problem an Kapitel 5 ist, dass zwar ein Curriculum zur Anwenderschulung bezüglich der Informationssicherheit in Schulen entwickelt wurde, dass dieses jedoch noch nicht auf seine Praxistauglichkeit getestet wurde. Nach Möglichkeit sollte in einem

Modellversuch überprüft werden inwieweit die von mir geforderten Inhalte ausreichend bzw. praxisrelevant sind.

In einem nächsten Schritt würde ich also gerne zuerst eine quantitative Befragung von IT-Sicherheitsverantwortlichen an Schulen in ganz Österreich durchführen um einen tieferen Einblick in das Thema Informationssicherheit an Schulen gewinnen zu können. Es wäre mir auch ein Anliegen, aufbauend auf dem von mir entwickelten Curriculum, eine umfassende Schulung zu entwickeln, die dann möglicherweise einen Beitrag zu mehr Informationssicherheit in Schulen liefern könnte.
Interessant wäre es auch unterschiedliche Formen der Anwenderschulung zu testen, um herauszufinden, welche sich besonders gut für den Einsatz in Schulen eignen.

Anhang A

Leitfaden zur Durchführung der Interviews

Einstiegsfragen zum Schaffen einer angenehmen Atmosphäre.

- Welche Fächer unterrichten Sie?
- Wie lange sind Sie bereits an dieser Schule?
- Wie lange betreuen Sie bereits die IT an dieser Schule?

Sondierungsfrage zum Einstieg ins Thema.

- Was fällt Ihnen spontan zum Thema „IT-Sicherheit“ ein? Haben Sie sich schon näher mit dem Thema auseinandergesetzt?

Hauptfragen (inkl. möglicher ad-hoc Fragen).

1. Wie sieht die IT-Infrastruktur an Ihrer Schule aus?
   - Welche Geräte sind vorhanden?
   - Wie werden diese eingesetzt?
   - Wer hat darauf Zugriff?
   - Gibt es unterschiedliche Rechte für die Benutzung?
2. Wie hoch schätzen Sie den Schutzbedarf der IT an Ihrer Schule?
   - Gibt es sensible Daten, wenn ja welche?
3. Sind Ihnen in Ihrer Laufbahn als IT-Administrator an einer Schule schon Bedrohungen für die IT begegnet? Wenn ja, welche?
   - Wer oder was hat die IT bedroht?
   - Wie wurde das Problem gelöst?
4. Werden, etwa von der Direktion, Sicherheitsmaßnahmen gefordert?

- Welche Sicherheitsmaßnahmen setzen Sie um?

5. Gibt es Sicherheitsrichtlinien für die Benutzer?
   - z.B. Passwortregeln, Richtlinien für die Benutzung des Internetzugangs, ...
6. Nehmen Sie an, Sie hätten die Möglichkeit, alle Benutzer an Ihrer Schule zum Thema IT-Sicherheit zu schulen. Was würden Sie sich wünschen, dass Schüler, Lehrer, Direktor usw. nach dieser Schulung wissen?
   - z.B. Grundlagen, gute/schlechte Passwörter, Schadcode, Datensicherung, Angriffe, ...

Anhang B

Transkription

Im Rahmen meiner Diplomarbeit habe ich vier Interviews mit IT-Administratoren an allgemeinbildenden und berufsbildenden höheren Schulen durchgeführt. Da eine Auflistung aller Transkriptionen zuviel Platz in Anspruch nehmen würde, habe ich mich dazu entschlossen, eine der Transkriptionen exemplarisch anzuführen. Aufgrund der Vielzahl an Informationen, die ich im Interview mit Markus H. erhalten habe, entschloss ich mich daher für die Transkription dieses Interviews.

Interviewer [I]: Martin Gruber (Interview am Dienstag, 31.03.2009, 10.30 Uhr)
Befragter [L]: Der Befragte Markus H. (Name zwecks Anonymisierung geändert) unterrichtet die Fächer Mathematik und Physik und ist IT-Administrator an einer berufsbildenden Schule.

Vor dem eigentlichen Interview fand ein kurzes Gespräch zum Kennenlernen des Interviewpartners statt.

00:00	1	I	Gut ... also welche Fächer unterrichtest du ... an der Schule?
	2	L	Mathematik, Physik
	3	I	m-h.
	4	L	ahm. Ja und heuer einmal nicht Informatik.
	5	I	Nicht Informatik.
	6	L	Zuviele Stunden.
	7	I	Gibt es ... wieviele Informatik Lehrer gibt es dann noch, sonst?
00:20	8	L	*(zählt)* Eins, zwei, drei, vier, fünf, se ... also eigentlich acht, die geprüft wären
	9	I	Ja
	10	L	Wobei nur fünf jetzt unterrichten.
	11	I	aha.
	12	L	Ich glaube fünf oder sechs, so irgendetwas.
	13	I	m-h. ahm. Wie lange bist du bereits an der Schule?
00:40	14	L	Ich habe jetzt das achte Dienstjahr. Ja, achte Dienstjahr.
	15	I	Das achte Dienstjahr, m-h. Und die IT betreust du schon seit ...
	16	L	Seit ...

17 I ... Anfang an?
18 L ... Beginn an.
19 I m-h. Und hast ... ist da der Kollege in Pension gegangen, oder?
20 L Die Kollegin ist in Pension ...
21 I Die Kollegin.
22 L ... naja eigentlich ist sie noch nicht in Pension gegangen, aber die war überfordert eigentlich.
23 I Ja. Na ok.
24 L Ich meine das darf man nicht laut sagen, aber wird ja eh aufgenommen, oder?
25 I *(lacht)*
26 L Nein sie war, das haben sie ihr damals einfach draufgedrückt und ...
01:00 27 I Ja.
28 l ... wie ich das Netz übernommen habe, da waren wir im Container, da hats genau gegeben 19 PCs ...
29 I m-h.
30 L ... und jetzt ist es halt doch schon gewachsen.
31 I Ja. Ok, ahm. Was fällt dir jetzt spontan zum Thema IT-Sicherheit ein? Hast du dich damit schon auseinandergesetzt irgendwie?
32 L Ja sicher ...
33 I Ja.
01:20 34 L ... ich meine das muss man in Schulen unbedingt.
35 I Ja.
36 L Ahm. Das ist ein breitgefächertes ... Thema. Das beginnt bei ... angefangen bei Datenschutz bis hin zu Web-Security, ahm, generell Net... Netz-Sicherheit ...
37 I m-h.
01:40 38 L ... ahm, ja, *(pff)* das ist wirklich ... Backup und und und, also das ist alles ... fällt für mich alles unter Daten- ...
39 I Ja.
40 L ... sicherheit alles, nicht? Ahm, das ist ein Riesen ... ein Riesengebiet eigentlich.
41 I Ein Riesengebiet, ja.
02:00 42 L Darum ... ahm, ja. Was bei uns an den Schulen, ahm, sehr wichtig ist, bei uns ist weniger das Backup wichtig ....
43 I Ja.
44 L ... eigentlich. Wobei man sagen muss, in der Verwaltung, dadurch dass man das Verwaltungsnetz auch mit betreut, obwohl es eigentlich dafür ... ahm ... vom Gesetzgeber her keinen ... keinen Verantwortlichen gibt eigentlich.
45 I m-h.
46 L Das macht man halt so mit.
02:20 47 I Ja.

48 L Ahm, da ist dann die Datensicherheit schon wieder ein Thema, nicht?
49 I Ja.
50 L Datensicherheit von ... Backups und so weiter.
51 I Ja.
52 L Ja. Und wenn bei mir an der Schule einmal der Mailserver nicht gehen sollte, dann wäre das im Prinzip kein Problem, wenn der jetzt einmal vier Stunden weg ist.
53 I m-h.
54 L Ahm. Im pädagogischen Bereich ... im Verwaltungsbereich eine Katastrophe.
02:40 55 I Ja, ist klar.
56 L Das ist das, was es einfach manches Mal ein bisschen schwierig macht.
57 I m-h.
58 L Ja, weil die Verwaltung einfach ... der Landesschulrat ... es passen da die Schnittstellen nicht ganz.
59 I Ja.
60 L Ahm, das Ministerium denkt sich da permanent neue Dinge aus, die eigentlich dann, wenn sie kommen, nicht mehr zeitgemäß sind.
03:00 61 I m-h.
62 L Ahm, ja, es ginge ja einfacher, aber es ist halt so. Ahm, und da muss man sich halt da, ich meine, dahin- ... retten irgendwie.
63 I *(lacht)*. Gibt es also vom Landesschulrat keine Weisungen in Richtung IT-...
64 L Oja ...
65 I ... Sicherheit. Schon.
66 L ... gibt es prinzipiell schon, wobei man andererseits sagen muss, es gibt aber keinen Verantwortlichen der es durch- ... ausführen sollte, nicht ...
03:20 67 I m-h.
68 L ... eigentlich. Ahm, es ist bei uns zum Beispiel das Netzwerk, eigentlich habe ich zwei Netzwerke. Ich habe ein pädagogisches und ein ... ein Verwaltungsnetzwerk ...
69 I Ja.
70 L ... die physikalisch komplett getrennt sind ...
71 I Ja.
72 L ... bei mir. In vielen anderen Schulen, auch in unserem Schulbereich, ist es nicht so. Da pfeifen sich die Netzwerkadministratoren etwas und sagen, „Danke, das genügt mir, ich ... *(pff)*... betreue keine zwei Netze“.
73 I Ja.
03:40 74 L Bei mir sind sie getrennt ... ahm ... ja, wobei man früher sogar zwei getrennte Internetanbindungen gehabt hat, nicht.
75 I Ja.

76 L Bis ich dann ... und der Landesschulrat hätte das eigentlich fortgesetzt, nicht. Wir haben ...

77 I Ja.

78 L ... teilweise so VPN-Server hergestellt und haben ... und die *(lacht)* Verwaltung hat über den VPN-Server mit dem Landesschulrat gearbeitet ... nicht ... mit einer zweiten Internetanbindung.

04:00 79 I Ok.

80 L Und dann haben sie das umgestellt, weil sie draufgekommen sind, es geht vielleicht ein bisschen anders auch. Und dann haben wir zwei Internetanbindungen gehabt, nicht.

81 I m-h.

82 L Ahm, und dann hat es vom Landesschulrat eine Lösung gegeben, dass man zum Beispiel, ich weiß nicht, da gibt es irgend so ein FortiGate 40, wäre das gewesen, irgend so eine Firewall, eine billige, ahm die hätte man da kaufen können als Schule, und dann hätten wir im Prinzip das Verwaltungsnetz und das pädagogische Netz mit zwei Firewalls getrennt ...

04:23 83 I Getrennt, ja.

84 L ... im Prinzip, nicht ... ahm ... hätte ein Schweinegeld gekostet und dadurch, dass wir eigentlich eine gute Firewall haben, habe ich gesagt ...

85 I Ja.

86 L ... das ... genügt bitte sehr ...

87 I Ja.

88 L ... nicht, und dort läuft das Verwaltungs-pädagogische Netz dann einfach zusammen.

89 I m-h. Ja. Ahm, wie sieht denn die Infrastruktur von der IT an eurer Schule so aus?

04:42 90 L Ahm, ich bin gerade zur Zeit im Umbruch. Wir haben jetzt bei mir im Netz 160 PCs.

91 I m-h.

92 L Wobei die eigentlich ... da ist keiner älter als zwei-ein-halb Jahre ... eigentlich, ahm von dem her sind wir top ausgestattet nur spiel ich ...

93 I Welches Betriebssystem habt ihr momentan?

05:00 94 L Wir fahren jetzt Windows XP.

95 I Das XP, ja.

96 L Komplett. In unserem Schulbereich, wir sind einfach ein berufliches Schulwesen.

97 I Ja.

98 L Ahm ... ist mit Open Source Geschichten wenig zu tun ... sage ich ganz ehrlich. Wobei ich fast ... das versuche, weil ich selber ... ahm, ja vom Prinzipiellen ... für prinzipielle Überlegungen gerne mehr Open Source nutzen würde.

05:23 99 I m-h.

100 L Weil es mir einfach eine Herzensangelegenheit ist, aber das ist in unserem Schulbereich einfach nicht möglich ...
101 I Ist nicht möglich, ja.
102 L ... weil wir hören immer, die Wirtschaft gibt vor und wir sind eine berufsbildende Schule und damit ist ... bleibt ...
103 I Ist klar, ja.
104 L ... Microsoft, fertig. Ja, das einzige ist vielleicht Open Office oder so irgendwas ...
105 I m-h.
05:40 106 L ... was man nutzen kann, aber Betriebssystem-mäßig nicht.
107 I Gar nicht? Auch nicht im Serverbereich, oder?
108 L Im Serverbereich schon ...
109 I Schon.
110 L ... teilweise, wobei ich da jetzt komplett umstelle gerade zurzeit. Ich virtualisiere das ganze Netz.
111 I m-h.
112 L Auch mit Client-Virtualisierung, also Desktop-Virtualisierung ... ahm ... im Prinzip, ja ... stelle ich es komplett um.
06:03 113 I m-h.
114 L Einfach zwei ... zwei gescheite ESX-Server ...
115 I m-h.
116 L ahm ... redundant ausgelegt zumindest halt ... gescheite Storage und fertig.
117 I Ja.
118 L Ja, und weil man da einfach viele Kosten sparen kann.
06:17 119 I m-h.
120 L Weil einfach die ... weil einfach die ... ahm ... finanziellen Möglichkeiten zwar da sind, da dürfen wir uns im ... im berufsbildenden Bereich gar nicht beschweren, nur ahm Server-seitig immer ein Problem, weil das sieht ...
121 I m-h.
122 L ... keiner, nicht, an der Schule, wenn man viele Arbeitsplätze hat, schaut das gut aus.
123 I m-h, ja, sicher.
124 L Was sich da drüben in meinem Server Raum tut, das interessiert die wenigsten ...
06:40 125 I *(lacht)*
126 L ... was sich da abspielt, aber jetzt stelle ich halt gerade um ahm und das wird dann einfach ... ja, ab nächsten Schuljahr werde ich jetzt einmal 20 ahm virutelle Desktops machen ...
06:59 127 I m-h.
128 L ... also einen ganzen EDV-Raum ersetze ich, mache ich jetzt einmal ... mache ich jetzt einmal virtuell und dann, ja ist irgendwann so die letzte Ausbaustufe, alles virutell zu machen.
129 I Ja.

130 L Hat für unsere Schüler einen großen Vorteil, sie könnten von zuhause im Prinzip mit der Schulsoftware arbeiten, nicht.
131 I Sehr gut, ja.
132 L Ahm, und wir haben Spezialsoftware, die einfach teuer ist, wo eine Lizenz, Schnittzeichensoftware-Lizenz über tausend Euro kostet.
07:19 133 I m-h.
134 L Ahm, das wo die Schüler sich das zuhause nicht leisten können und es wird auch bildbearbeitungstechnisch zum Beispiel der Photoshop vorgegeben.
135 I m-h.
136 L Ja, und den kann man ...
137 I Kann man sich nicht leisten.
138 L ... sich als Schüler nicht leisten ...
139 I Ja, ist eh klar.
140 L ... wenn man es offiziell macht.
141 I Ja. *(lacht)*
142 L Ahm, und darum ist das für mich eine Lösung, eigentlich und dadurch, dass ich ein Physiker bin ist das Energiesparen und Green IT einfach ein Thema für mich.
07:42 143 I Ja.
144 L Muss ich ganz ehrlich sagen.
145 I m-h.
146 L Und jetzt war der Zeitpunkt im Prinzip ganz gut, weil jetzt haben wir ... ahm, jetzt habe ich Server-seitig sowieso etwas machen müssen, jetzt machen wir es dann gleich „gscheit".
147 I m-h.
148 L Und das ist eigentlich für eine Schule, ahm, eigentlich eine tolle Sache, nicht.
149 I Ja, wenn ich das mit anderen Schulen vergleiche, wo ich schon etwas gesehen habe.
08:01 150 L Ja, also von dem her ... darf ich mich nicht beklagen.
151 I Ja.
152 L Das ist jetzt ein Projekt, das ich ... das ich jetzt gestartet habe im letzten Schuljahr. Jetzt plane ich ungefähr ein Jahr schon daran.
153 I m-h.
154 L Weil das ja nicht so ohne ist.
155 I Ja.
156 L Ahm, aber ich bin eigentlich schon relativ weit, und nächstes Schuljahr ... habe ich da drüben keinen Server mehr rennen, außer den zweien.
08:23 157 I m-h.
158 L Und fertig.
159 I Ja. Ahm, inwiefern werden die Geräte eingesetzt, also im Schulunterricht, und die Schüler haben so auch noch Zugriff darauf?
160 L Die Schüler haben rund um die Uhr Zugriff ...

161 I Rund um die Uhr.
162 L ... im Prinzip. Wenn die Schule offen ist, können sie immer herein. Sie können ... ahm, ja, sogar in ... sich in Stunden dazu setzen.
08:46 163 I m-h.
164 L Wenn Arbeitsplätze frei sind. Ahm, ja eigentlich ... Pausen ... immer. Also rund um die Uhr.
165 I Ahm, und mit der Rechteverwaltung schaut es wie aus? Sind Schüler, Lehrer ...
166 L Ja.
167 I ... Administrator, Direktor getrennt und so weiter.
168 L Genau.
09:00 169 I Schon.
170 L Im Prinzip ja.
171 I Ja.
172 L Im Prinzip ... ahm, Lehrer – Schüler.
173 I Ja.
174 L Ahm, und mich.
175 I m-h.
176 L Im Prinzip. Ahm, ja und dann halt über Gruppenrichtlinien ...
177 I m-h.
178 L ... gewisse Dinge, einfach gesteuert. Ahm von der ... von den Net Shares auch teilweise halt so, dass die Lehrer auf die ... auf die Home-Laufwerke der Schüler zugreifen können.
09:23 179 I m-h.
180 L Dass jeder Schüler ein eigenes Home-Laufwerk hat und ein Klasse-Laufwerk hat.
181 I m-h.
182 L Ahm, wo halt die Schü ... die Lehrer dann drauf zugreifen können.
183 I Ja.
184 L Ja, jeder Schüler hat eine eMail-Adresse, natürlich, ahm, wo wir sogar Schularbeiten machen, im Prinzip darüber.
09:39 185 I Ja.
186 L Das habe ich mir einmal überlegt vor ein paar Jahren, das ist eigentlich ganz ... ganz geschickt. Man schickt ihnen die Angabe ...
187 I Ja.
188 L ... und sie antworte, schicken es zurück und damit war das die ganze Schularbeit, nicht.
189 I Sehr gut, ja.
190 L Damit habe ich einen genauen Abgabetermin und alles, nicht.
191 I m-h.
192 L Ahm, Intranet haben wir im Prinzip ... habe ich auch über ... weil wir einen Exchange halt rennen haben über öffentliche Ordner realisiert, ahm, da steht unser ganzes Wissen ...
10:03 193 I Ja.

194 L ... der Schulinfrastruktur drinnen. Wie Supplierpläne, ...
195 I m-h.
196 L ..., ???, und, und, und. ... Ahm, hat sich deshalb eigentlich gut ergeben, weil wir eigentlich im Prinzip die Microsoft-Lizenzen gratis kriegen, nicht.
197 I m-h.
198 L Und damit brauche ich mir nicht selber eine Lösung überlegen, wenn es ...
10:20 199 I Ja.
200 L ... das schon gibt, nicht.
201 I Ist richtig, ja ... ahm, haben, zum Beispiel die Lehrer, die ... das Recht, irgendwelche Programme zu installieren ...
202 L Nein.
203 I ... auf Rechnern. Nein ...
204 L Nein.
205 I ... also das Recht hast wirklich nur du?
206 L Habe nur ich.
207 I Das ist sehr gut, ja. ... Gut, ahm, wie hoch würdest du selbst den Schutzbedarf von IT an Schulen einschätzen?
10:38 208 L Das kommt darauf an. Ich sage es ganz ehrlich, es kommt auf den Schultyp darauf an.
209 I Ja.
210 L Wir leben hier auf einer Insel der Seligen.
211 I Ja.
212 L Ich muss keine Mäuse anhängen, ich muss keine Computer zusperren. In HTLs kommt es vor, wenn ich mit anderen Administratoren rede, die fladern ihnen RAM raus.
213 I *(lacht)*
214 L Ahm *(lacht)* fladern ihnen Tastaturen, Maus ...
215 I Ja.
216 L ... alles was nicht angebunden ist, ist fort, nicht.
217 I Ja.
10:59 218 L Und das merkst du nicht einmal. Da sind zwei ... zwei Bänke belegt, und ...
219 I Ja.
220 L ... und bei ... bei einem nehmen sie es heraus, nicht.
221 I *(lacht)*
222 L Kommst du nie drauf.
223 I Nein, eh nicht. ... Und sensible Daten sind halt hauptsächlich die Verwaltungsdaten?
224 L Sensible Daten sind die Verwaltungsdaten ...
11:12 225 I Genau.

226 L ... eigentlich, wie, ja auch Schüler ... Schülerinnenverwaltung, ahm, das ist halt das, was ... was ein wenig sensibel ist, wobei man ... ja, man muss halt aufpassen mit jedem ... jedem Traffic der hinausgeht und hereingeht, dadurch ...

11:27 227 I Ja.

228 L ... dass wir einen eigenen Webserver auch betreiben, das sind halt so Dinge, die ...

229 I m-h.

230 L ... da muss ich einfach dicht sein nach außen.

231 I m-h. Bist du in deiner Laufbahn als IT-Administrator da an der Schule, oder generell, ahm, schon irgendwelchen Bedrohungen für die IT begegnet. Also Virenangriffe und so weiter?

11:42 232 L J... *(pff)* ... Ja, wie ich in die Schule gekommen bin ... Virenangriffe, ich meine ich habe jetzt, Gott sei Dank, vor ein paar Jahren in eine sehr, sehr gute Firewall investiert.

233 I m-h.

234 L Ahm, seit dem schlafe ich ruhiger.

235 I Ja.

236 L Muss man ganz ehrlich sagen. Ahm, damit sind wir eigentlich bis jetzt eigentlich sicher gewesen. Einmal, das war diese Sasser-Zeit, und ...

12:03 237 I m-h.

238 L ... die war einfach ein wenig ein Problem, weil die, ja ... Microsoft halt, nicht.

239 I Ja.

240 L Sicherheitslücken, das ist halt immer so ein bisschen ein heikles ...

241 I m-h.

242 L ... Problem. Ahm, wo i generell a Problem hab, ich habe schon einmal ein Netzwerk geschossen, weil ich einen Domain Controller upgedated habe.

12:20 243 I m-h.

244 L Und der hat mir dann das Active Direcotry hin gemacht ...

245 I *(pff)*

246 L ... und war alles ... alles hin, wirklich alles hin. Also darum bin ... habe ich ein bisschen ein zwiegespaltenes Verhältnis mit den Microsoft Updates. Ich würde gerne und ich mache sie auch jetzt eigentlich immer und das ist auch ein Thema warum ich virtualisiere, weil ich da einfach das testen ...

247 I Testen.

248 L ... kann.

12:38 249 I m-h.

250 L Und so ist es halt jetzt. Ich bin hardwareunabhängig, also wenn mir jetzt der Server drüben ... drüben ein ... wenn mir jetzt ein Server eingeht, habe ich ein Problem einfach.

251 I Ja.

252 L Weil ... die Hardware bekomme ich wahrscheinlich gar nicht mehr.
253 I Ja.
254 L Das ist halt dann immer so ... da muss man halt immer schauen, glaube ich, dass man ... dass man sich mit den gegebenen Möglichkeiten, die man hat in einer Schule, ahm, ja so gut als möglich irgendwie zurechtfindet.
13:03 255 I Ja.
256 L Ahm, weil man ja eigentlich für das was man, muss man auch ganz ehrlich sagen, bezahlt bekommt, und für das, was man eigentlich kann, ahm, muss man es sich halt einfach so, finde ich, so, ahm ... wie kann man sagen ... so wenig riskant wie möglich machen, nicht.
13:20 257 I m-h.
258 L Weil es ist schon ein riesen Netz, ich meine es sind, ich habe 550 Benutzer ...
259 I Ja.
260 L Ahm, es sind wirklich Daten, die wirklich sensibel sind, und das gibt es im Prinzip in einer ... und habe dafür, ja zehn Werteinheiten ungefähr, so rund.
261 I m-h.
262 L Das gibt es ... gäbe es in einer ... in einem Wirtschaftsbetrieb nie, nicht?
263 I Ja.
13:40 264 L Und, ahm es wird ja immer mehr gefordert, ich meine wir haben ... es sollte der Computer im Unterricht auch eingesetzt werden.
265 I m-h.
266 L Und da muss man halt dann einfach entscheiden, nicht? Wenn ein Kollege mir schreibt ... ich weiß nicht ... ahm ... keine Ahnung, bei ihm ist ein Symbol vom Desktop verschwunden, dann muss ich mir meine Prioritäten so einteilen, wie ich das richte.
267 I Ja.
14:00 268 L Und wenn der Kollege dann halt zwei Wochen warten muss, das macht es halt bei uns so schwer. Weil im Prinzip bist du als Netzwerkadministrator ein Kollege wie jeder andere, nicht?
269 I m-h.
270 L Ahm, und trotzdem brauchen sehr viele Leute etwas von dir.
271 I Ja.
272 L Und das ist halt, ja ... manchmal nicht so toll, weil man ... weil man, weil die Kollegen das dann nicht verstehen, dass man eben Prioritäten setzen muss.
14:21 273 I m-h.
274 L Weil ich habe da ja wirklich eine gescheite Infrastruktur dahinter, nicht?
275 I m-h.

276 L Da ... wenn einmal ein PC in einem Raum nicht geht, ja, da muss sich der Schüler auf einen anderen Platz setzen.
277 I Ja.
278 L Aber, ja, das ist halt so.
279 I m-h.
280 L Aber sonst mit Viren eigentlich ... kein Problem.
281 I Nein. Jetzt auch nicht, mit dem Conficker oder so?
14:40 282 L Nein, gar nichts ... null ...
283 I Ja.
284 L ... die Firewall ist wirklich gut ... ist eine (Produktbezeichnung)-Firewall
285 I Ja.
286 L Die ... die ist echt ok.
287 I Das heißt, die Hauptmaßnahmen, die du setzt sind eigentlich die Firewall ...
288 L Die Firewall.
289 I ... dann Virenschutz, wahrscheinlich?
290 L Virenschutz, DMZ.
291 I Ja.
292 L Und ...
293 I m-h.
294 L Ja.
295 I In der DMZ sind der Webserver und der Mailserver.
14:59 296 L Der Webserver und der Mailserver, ja.
297 I Ok. Ahm, gibt es von dir, oder von irgendwem Sicherheitsrichtlinien für die Benutzer? Also wie sollen sie das Passwort wählen, oder so etwas ...
298 L Nein, das ...
299 I ... in der Art.
300 L ... haben wir im Prinzip nicht. Warten nach dem ... wie sagt man, wie heißt es ... Passwortkomplexität? ...
301 I m-h.
302 L ... glaube ich, habe ich ausgeschalten, weil es einfach nicht administrierbar war. Weil bei 500 Schülern ...
15:23 303 I Ja.
304 L ... die gebens ...
305 I Kommt ständig wer.
306 L ... einmal, da kommt ständig wer, Passwort vergessen.
307 I m-h.
308 L Man könnte es im Prinzip den Kolleginnen dann, ahm, ja ich könnte einen Konto ... Konto ... Kont ... Kontooperator im Prinzip erstellen ...
309 I m-h.

310 L ... aber das mache ich dann im Prinzip auch nicht, ahm, weil das einfach vom Aufwand her ... es sind jetzt pro Jahr ... werden es sein, 10 Schüler, die das Passwort vergessen haben. Ahm, ich muss aber dazu sagen, sie können sich wählen, was sie wollen und sie sind selbst dafür verantwortlich ...

15:49 311 I m-h.

312 L ... ahm, wenn mit den Daten etwas passieren würde.

313 I m-h.

314 L Da übernehme ich, das ist auch bei uns so ausgemacht, generell keine Haftung. Auch, wenn sie jetzt, ahm, ihre Projekte auf dem H:-Laufwerk haben, die Schüler wissen, sie müssen sich das genauso auf den USB-Stick speichern.

16:06 315 I Das heißt, die Schüler sind selbst für ihre Datensicherheit ...

316 L Sie sind für ihre Datensicherung verantwortlich. Das tue ich nicht, weil das ... das würde den Rahmen sprengen ...

317 I Ja.

318 L ... bei 500 Schüler. Da brauche ich Backup Lösungen, die, ja, die kann sich auch die Schule nicht leisten, das ist ...

16:20 319 I Ja.

320 L ... darum muss man sich, muss man da immer ein bisschen erfinderisch sein.

321 I m-h.

322 L Und die Schüler, für die Schüler-Daten übernehme ich prinzipiell keine Haftung.

323 I Ja.

324 L Überhaupt nicht.

325 I m-h.

326 L Ahm, und das wissen sie auch. Vor kurzem hat ein Schüler gehabt, glaube ich eineinhalb Gigabyte an eMails ...

327 I m-h.

328 L ... da wird das Postfach geleert, fertig.

16:37 329 I Ja.

330 L Das nehme ich mir heraus, das zu tun.

331 I Ja.

332 L Ahm, weil einfach der Mailserver in die Knie gegangen ist, nicht?

333 I Ja.

334 L Und da muss ich schauen ... habe ich Platz suchen müssen.

335 I m-h. Ahm, angenommen, du hättest die Möglichkeit, dass alle Benutzer an der Schule, ahm zur IT-Sicherheit geschult werden.

16:56 336 L Ja.

337 I Ahm, was würdest du dann wollen, dass jetzt zum Beispiel, nachdem es ja unterschiedliche Rechte gibt für Schüler und Lehrer, was sollen die Schüler wissen, hinsichtlich IT-Sicherheit, und was sollen vielleicht die Lehrer wissen?

338 L Schüler sollten IT-Sicherheit ... IT-Sicherheit ist ja so ein dehnbarer Begriff. Ich habe letztes Jahr einen Herrn da gehabt, der ist Internet Broker gewesen. Ahm ich glaube, dass da ein The ... das ein Thema für die Schüler ... auch Datensicherheit.

17:25 339 I Ja.

340 L Was gebe ich im Internet von mir Preis? Wie sensibel gehe ich mit meinen Daten im Internet um?

341 I m-h.

342 L Ahm, im Netzwerk selbst, ahm, sie sind einfach ... ja, sie ... sie ... wie kann man sagen ... sie schauen immer wieder, wenn ich ihnen zeige, was geht, ja?

343 I Ja.

344 L Ahm, sie wissen das alles. Sie sehen, wo ich gesurft bin, nicht?

17:44 345 I m-h.

346 L Also mit so Dingen, ahm, dass sie im Internet im Prinzip gläsern sind, das ist ihnen nicht bewusst.

347 I Ja.

348 L Sie glauben, das ist etwas anonymes.

349 I m-h.

350 L Und das ist nicht nur im Internet so, sondern auch generell, im Netz so einfach. Sie glauben ... sie, ja sie können machen, was sie wollen.

18:00 351 I m-h.

352 L Ein Schüler ... ich habe ihnen über einen Content-Filter auf der Firewall einfach auf Grund ... ich bin eigentlich ein ... ein Mensch, der nicht gerne etwas sperrt, im Gegenteil, ich denke mir es ist immer Angebot und ... und ... wie sagt man da, ahm ... Geben und Nehmen ... ein Geben und Nehmen einfach, nicht?

18:18 353 I Ja.

354 L Wie viel gebe ich her, wie viel nehmen sie? Ahm, da habe ich einmal vor einem Jahr, nein vor zwei Jahren, wird das schon her sein, ahm, habe ich ihnen die Spiel ahm Spiele gesperrt im Internet, einfach, nicht?

355 I m-h.

356 L Weil sie im Unterricht ... weil Kollegen an mich heran getreten sind, ob man da was machen kann, weil sie spielen im Unterricht, nicht?

357 I m-h.

358 L Jetzt habe ich ihnen generell über einen Content-Filter Spiele gesperrt und ein Schüler hat das gesehen, wie ich in die Fire ... wie ich mich in Firewall eingeloggt habe und zwei Tage später sitze ich zuhause vor meinem Computer und plötzlich bekomme ich ein eMail von der Firewall, es probiert wer, mit meinem Benutzernamen, in die Firewall einzusteigen, nicht?

18:51 359 I *(pff)* Arg!

360 L Ich meine ... der hat das zufällig gesehen, wie es am Videobeamer gelaufen ist, nicht?

361 I Ja.

362 L Nur hat er mein Passwort nicht gewusst und ich habe sofort, weil das ja ... um ... ahm, wie sagt man, ahm eine fehlerhafte Anmeldung war, bekomme ich ein eMail, nicht, aus Sicherheitsgründen. Und ich habe dann halt gleich geschaut, woher das gekommen ist erstens ...

19:10 363 I m-h.

364 L ... und wo der gesessen ist *(lacht)* und habe halt dann von daheim ahm, ja nachgeschaut und bin draufgekommen der sitzt im EDV-Raum 1 am vierten PC links ...

365 I Ja.

366 L ... und habe in der Schule angerufen und habe gesagt, verbinde mich hinunter zur Sekretärin, EDV-Raum, und habe zu der Kollegin gesagt, sage ich gib mir den Matthias gleich, der sitzt da vorne rechts am dritten Computer ...

19:29 367 I *(lacht)*

368 L ... ich muss mit ihm reden. Das war genau 2 Minuten nachdem er probiert hat, da in die Firewall zu kommen.

369 I Ja.

370 L Und das dürfte sich dann ... dann habe ich ihm ein bisschen den Kopf gewaschen ... und das dürfte sich dann auch herumgeredet haben in der Schule. Und seit dem ist alles ein bisschen besser.

371 I Ja.

372 L Generell. Also, ahm, ja, sie würden probieren, aber dadurch, dass wir so einen hohen Mädchenanteil haben, eigentlich ...

373 I m-h.

374 L mehr die Buben.

375 I Die Buben. Also gibt es schon irgendwie teilweise Versuche von ihnen, dass ...

376 L Ja sicher.

377 I ... sie sich die Rechte erweitern, oder soetwas?

19:57 378 L Sicher.

379 I Ja.

380 L Klar.

381 I m-h.

382 L Klar, ich muss schon aufpassen mit den ... den Netzwerkfreigaben und so ...

383 I Ja.

384 L ... Dingen. Also auf das muss ich aufpassen. Weil das hören sie oder sehen sie irgendwo. Was ich zum Beispiel abdrehen habe müssen, war der Nachrichtendienst.

385 I m-h.

386 L Weil über netsend haben sie geschummelt.

387 I *(lacht)*
388 L War so.
389 I *(lacht)* Ja.
390 L Fertig. Das haben sie einmal in der Hauptschule irgendwo gelernt ...
20:23 391 I Ja.
392 L ... mit netsend kann man etwas schicken, und plötzlich ... ahm, *(pff)* ja.
393 I *(lacht)*
394 L An das hätte ich am Anfang gar nicht gedacht, nicht?
395 I Ja.
396 L Und da muss man dann schon aufpassen. Sie ... von dem her, da ... *(pff)* ... da sind sie nicht ungeschickt.
397 I m-h.
20:39 398 L Wenn sie da bemerken, was da geht und wie und was, also da muss man da, von dem her muss man aufpassen.
399 I Ja.
400 L Aber sonst sind wir da auf einer Insel der Seligen.
401 I m-h. Und hinsichtlich der Lehrer, was hättest du da gerne, dass die wissen?
402 L Generell ... ahm ... ja ... es wäre halt nett, ich meine ich verstehe es, es ist in jedem Beruf so, ahm, dass man nicht computertechnisch so gut drauf ist.
21:05 403 I m-h.
404 L Aber dass es Berufe gibt, wo man, bei uns ist es halt so, jeder braucht bei uns Computer Kenntnisse, und ich würde mir manches mal einfach eine höhere IT-Fitness wünschen, generell halt. Generell muss ich ganz ehrlich sagen, weil es wird immer wieder, kommt die V... kommt der Wunsch, Schularbeiten am PC zu machen, zum Beispiel in Deutsch.
21:26 405 I m-h.
406 L Ich habe schon Seminare angeboten in der Schule, ahm ... wo wir eben, was weiß ich, schulinterne Seminare zwecks Ausdrucken und so weiter. Und da gibt es halt wirklich Kollegen, die das nicht können.
21:39 407 I m-h.
408 L Aber durch den Druck, weil andere Kollegen Schularbeiten machen im EDV-Raum oder gerne machen würden, das auch machen und das ist dann ein Problem, wenn dann im Prinzip jemand in den EDV-Raum geht und das Netzwerk gar nicht einmal versteht, mit den ganzen ...
409 I Ja.
410 L Laufwerken und wie und was, nicht? Dann wird es schon schwer, dass man dann auch dementsprechend auch mit den Schülern ...
21:59 411 I m-h.

412 L ... arbeitet. Und das ist bei uns einfach ... ja es ist halt dann leicht. Man sagt dann meistens „Nix geht“, nicht?

413 I Ja.

22:07 414 L Ahm, und das ist halt ... da würde ich mir gerne wünschen, dass man da ein wenig, ahm, einfach ein wenig sensibler ist, und sich ein bisschen ... auch von den Kollegen her ... einfach, ahm, das ist halt so schwer, nicht? Wenn man zum Beispiel einen Zugang zum Intranet von ... von außen bietet und dann kommen Kollegen und sagen „Bei mir geht es nicht“, und dann sage ich „Wieso geht es nicht“, „Nach ich weiß nicht, das geht bei mir nicht“ und dann stellt sich irgendwann heraus, dass die Internet-Anbindung auch nicht geht und dann sollte ich ihnen helfen, warum das Internet auch nicht geht und das sprengt dann einfach den Rahmen, nicht? Weil bei 60 Kollegen ...

22:45 415 I m-h.

416 L ... ich kann ja nicht schauen ... gestern sollte ich ... hat mich eine Kollegin gefragt, weil der Maler da war, der hat die Post-Dose von der Wand heruntergeschraubt ...

417 I m-h.

418 L ... wie ich die Dose wieder anschraube und ob ich die nicht anschrauben könnte, nicht? Und das, irgendwann ist das dann nicht lustig.

22:59 419 I Ja.

420 L Muss man ganz ehrlich sagen, nicht?

421 I Ja.

422 L Muss man auch manchmal eine Grenze ziehen, nicht? Und die ist manchmal nicht so sch ... nicht so leicht, weil man halt einfach ein ganz normaler Kollege ist, so wie alle anderen auch.

423 I m-h.

424 L Das ist ein bisschen schwierig. Aber sonst würde ich mir einfach von den Kollegen netzwerksicher ... sicherheitstechnisch ... ahm, wünschen, dass, ja, von dem her, ja sie können es eh gar nicht so viel, sie haben im Konferenzzimmer vier Geräte ... fünf Geräte, da können sie das Intranet abrufen, da können sie ein wenig arbeiten.

23:28 425 I m-h.

426 L Da können sie drucken, wenn sie irgendetwas brauchen, aber netzwerktechnisch, also sicherheitstechnisch ...

427 I m-h. Was ich noch gar nicht gefragt habe, ist, habt ihr WLAN?

428 L Ja.

23:40 429 I Ja. Zugänglich für alle Schüler und Lehrer, nein?

430 L Ahm, nein. Ich habe einen EDV-Raum über WLAN ...

431 I Ja.

432 L ... gemacht. Weil das war einmal eine Werkstätte, da hat es keine Verkabelung gegeben.

433 I Ja.

434 L Ahm, das ist mitunter auch ein Grund warum ich jetzt diesen Raum virtualisiere.
435 I m-h.
436 L Weil ich einfach mit den Übertragungsraten ein Problem habe.
437 I m-h.
00:02 438 L Weil ich das nicht schaffe mit ...
439 I Ja.
440 L ... mit zwei Access-Points. Das ist ...
441 I Ja.
442 L ... bei Bildbearbeitung zu wenig. Aber es war einfach Vorgabe vom Landesschulrat, es darf, wenn wir diese Werkstätte als EDV-Raum führen, keine finanziellen Aufwendungen geben, also es darf nichts kosten auf Deutsch.
00:17 443 I m-h.
444 L Folglich habe ich das so machen müssen und jetzt, ich glaube wenn ich den ... den virtualisiere ist das Problem behoben, weil ...
445 I Ja.
446 L ... es wird ja nichts mehr übertragen über RTP und fertig.
447 I Ja.
448 L Ja, aber sonst ist der eigentlich zu. Die Schüler ... da würden sie es manchmal probieren, des ...
449 I Die Verschlüsselung zu knacken?
450 L Naja nicht zu knacken, aber einfach ... einfach teilzunehmen. Aber ja, ich meine der ist hoffentlich ... hoffentlich dicht. Ich weiß nicht ob WPA2 schon ...
451 I WPA2.
452 L WPA2 gesichert, schon geknackt ist?
453 I Nein, noch nicht.
454 L Ich glaube der ist noch nicht geknackt.
455 I Nein, das einzige was da glaube ich durchgeht sind Wörterbuchattacken.
00:59 456 L Ja, so irgendwas.
457 I Aber das wird ja kein Wörterbuch-Passwort sein?
458 L Nein, richtig.
459 I Also so gesehen.
460 L Eben, darum, so ist er noch gar nicht ... der Algorithmus noch nicht geknackt.
461 I Ja. Gut, dann sage ich einmal Dankeschön?
462 L War's das schon?

Literaturverzeichnis

[Banse] G. Banse u.a., „Zur Didaktik der IT-Sicherheit“, SecuMedia, Ingelheim, 1999.

[BMUKK1] Bundesministerium für Unterricht, Kunst und Kultur, „Erlass Einfaches und sicheres Schulnetz“, Online-Quelle, 2008. Online erhältlich via URL: <http://elsa20.schule.at/uploads/media/erlass_schulnetz.pdf> (30. März 2009).

[BMUKK2] Bundesministerium für Unterricht, Kunst und Kultur, „Empfehlung Einfaches und sicheres Schulnetz“, Online-Quelle, 2008. Online erhältlich via URL: <http://elsa20.schule.at/uploads/media/empf_schulnetz.pdf> (30. März 2009).

[Bogolea] B. Bogolea, K. Wijekumar, „Information security curriculum creation: a case study“, in: InfoSecCD '04: Proceedings of the 1st Annual Conference on information Security Curriculum Development, pp. 59-65, ACM, New York, 2004.

[BSI 100-2] Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standard 100-2 IT Grundschutz-Vorgehensweise“, BSI, Bonn, 2008.

[BSI-B1.5] Bundesamt für Sicherheit in der Informationstechnik, „B 1.5 Datenschutz“, Online-Quelle, 2008. Online erhältlich via URL: <http://www.bsi.bund.de/gshb/baustein-datenschutz/html/index.htm> (30. März 2009).

[BSI-L] Bundesamt für Sicherheit in der Informationstechnik, „Leitfaden IT-Sicherheit“, BSI, Bonn, 2007.

[BSI-S] Bundesamt für Sicherheit in der Informationstechnik, „Webkurs IT-Grundschutz“, Online-Quelle, 2006. Online erhältlich via URL: <http://www.bsi.de/gshb/webkurs/gskurs/seiten/s1000.htm> (30. März 2009).

[Dark] M. J. Dark, „Civic responsibility and information security: an information security management, service learning course“, in: InfoSecCD '04: Proceedings of the 1st Annual Conference on information Security Curriculum Development, pp. 15-19, ACM, New York, 2004.

[Eschweiler] J. Eschweiler, D. E. Atencio Psille, „Security@Work“, Springer, Berlin, 2006.

[Gehringer] E. F. Gehringer, „Choosing Passwords: Security and Human Factors“, in: ISTAS '02: International Symposium on Technology and Society, pp. 369-373, IEEE, New York, 2002.

[GI] Gesellschaft für Informatik, „IT-Sicherheit in der Ausbildung“, in: Datenschutz und Datensicherheit, Volume 31, Number 5, pp. 367-371, Vieweg Verlag, Wiesbaden, 2007.

[GSHB] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutz-Kataloge“, BSI, Bonn, 2008.

[ISTR] Symantec Corporation, „Symantec Global Internet Security Threat Report Trends for 2008“, Online-Quelle, April 2009. Online erhältlich via URL: <http://www.symantec.com/content/de/de/about/downloads/PressCenter/ISTR_XIV_Global.pdf> (16. April 2009).

[Kuo] C. Kuo, S. Romanosky and L. F. Cranor, „Human Selection of Mnemonic Phrase-based Passwords“, in: SOUPS '06: Proceedings of the second symposium on Usable privacy and security, pp. 67-78, ACM, New York, 2006.

[Moodle] Moodle, Dokumentation und Downloads, URL: <http://moodle.org/> (10. April 2009).

[Müller] K.-R. Müller, „IT-Sicherheit mit System“, Vieweg, Wiesbaden, 2008.

[OCG-Security] Autorengruppe der Secure Business Austria, „Informationssicherheit kompakt und verständlich“, OCG, Wien, 2008.

[OeSiH] Bundeskanzleramt Österreich, „Österreichisiches Sicherheits-Handbuch“, OCG, Wien, 2007.

[Pohlmann] N. Pohlmann, H. Blumberg, „Der IT-Sicherheitsleitfaden“, mitp, Heidelberg, 2006.

[Skoudis] E. Skoudis, „Counter Hack Reloaded“, Prentice Hall, Upper Saddle River, NJ, 2006.

[Strauss] A. L. Strauss, „Grundlagen qualitativer Sozialforschung“, Fink, München, 1991.

[Theoharidou] M. Theoharidou, D. Gritzalis, „Common Body of Knowledge for Information Security“, in: Security & Privacy, Volume 5, Number 2, pp. 64-67, IEEE, New York, 2007.

[Wang] A. J. Wang, „Web-based interactive courseware for information security“, in: SIGITE '05: Proceedings of the 6th Conference on information Technology Education, pp. 199-204, ACM, New York, 2005.

[Whitman] M. E. Whitman, H. J.Mattord, „Designing and teaching information security curriculum“, in: InfoSecCD '04: Proceedings of the 1st Annual Conference on information Security Curriculum Development, pp. 1-7, ACM, New York, 2004.

[Witt] B. C. Witt, „IT-Sicherheit kompakt und verständlich“, Vieweg, Wiesbaden, 2006.