Entwicklung einer IT-Sicherheitsstrategie für eine deutsche Hochschule am Beispiel der Universität Hannover

Diplomarbeit

zur Erlangung des Grades eines Diplom-Ökonomen der Wirtschaftswissenschaftlichen Fakultät der Universität Hannover

vorgelegt von

Name: **Günthel** Vorname: **Simon**

[redacted]

Erstprüfer: Herr Prof. Dr. Michael H. Breitner

Hannover, den 30.06.2004

Inhaltsverzeichnis

1 Einleitung

1.1 Motivation

In der modernen Informations- und Kommunikationsgesellschaft erfordert ein leistungs- und wettbewerbsfähiger[1] Hochschulbetrieb im zunehmenden Ausmaß die Integration von Abläufen und Verfahren, die sich auf Informationstechnik (IT) und hierbei insbesondere auf vernetzte informationstechnische Systeme (IT-Systeme) stützen. Dementsprechend gibt es auch an der Universität Hannover[2] (UH) im Wesentlichen keinen Bereich mehr, der nicht IT-Systeme zur Bewältigung seiner Aufgaben einsetzt.[3] Parallel zu dieser Entwicklung nimmt allerdings auch die Abhängigkeit von der Funktionsfähigkeit und permanenten Verfügbarkeit der eingesetzten IT-Systeme zu.[4]

Beobachtungen und Erfahrungen des Regionalen Rechenzentrums für Niedersachen[5] (RRZN) zeigen, dass die Bedrohungen und Gefahren, denen die IT-Ressourcen der UH täglich aus dem Internet aber insbesondere auch aus dem internen Hochschulnetz ausgesetzt sind, keinesfalls zu unterschätzen sind. Dabei steigt die Anzahl gezielter Angriffe auf IT-Systeme und Störungen im Hochschulnetz stetig.[6] Für die signifikante Zunahme der Vorfälle gibt es viele Ursachen.

Die Gründe liegen u. a. in der weiten Verbreitung und zunehmenden Vernetzung technischer Systeme, im technologischen Fortschritt, in der unkomplizierten Beschaffung von leicht zu bedienenden Angriffstools[7] im Internet und natürlich im immer breiter werdenden Allgemeinwissen der Anwender. Die IT ist mittlerweile aus dem Schul- und Arbeitsalltag nicht mehr wegzudenken. Detailliertes Hintergrundwissen über IT-Systeme, die ihnen zugrundeliegenden Informations- und Kommunikationstechnologien (IuK-Technologien) und potentielle Schwachstellen sind daher heutzutage weit verbreitet. Entsprechend gering sind die Einstiegsbarrieren für potentielle Angreifer.

Die zunehmende Zahl von Störungen und Schwachstellen lässt sich z. B. auf sehr komplexe und umfangreiche Softwarepakete mit dynamischen Bibliotheken und

---

[1] Nach h. M. wird als sicher angenommen, dass ein Bestehen im nationalen und internationalen Hochschulwettbewerb ohne entsprechenden IT-Einsatz nicht mehr vorstellbar ist.
[2] http://www.uni-hannover.de.
[3] Vgl. **UH** [2002, S. 1]; Vgl. **Rossa**, C. [2003, S. 3].
[4] Vgl. **Gaulke**, M. [1996, S. 9].
[5] http://www.rrzn.uni-hannover.de.
[6] Vgl. **Plehn**, H./**Reichling**, M./**Rossa**, C. [2003, S. 31].
[7] Hierbei handelt es sich um Software-Werkzeuge.

Plug-Ins[8], die organisationsinterne und –übergreifende Vernetzung von technischen Systemen sowie die drahtgebundene und drahtlose Anbindung von diversen Endgeräten zurückführen.[9] In Abbildung 1 wird die angesprochene Entwicklung noch einmal, am Beispiel einer CERT-Statistik (vgl. Abschnitt 5.4.2.4) über sicherheitsrelevante Ereignisse, verdeutlicht.

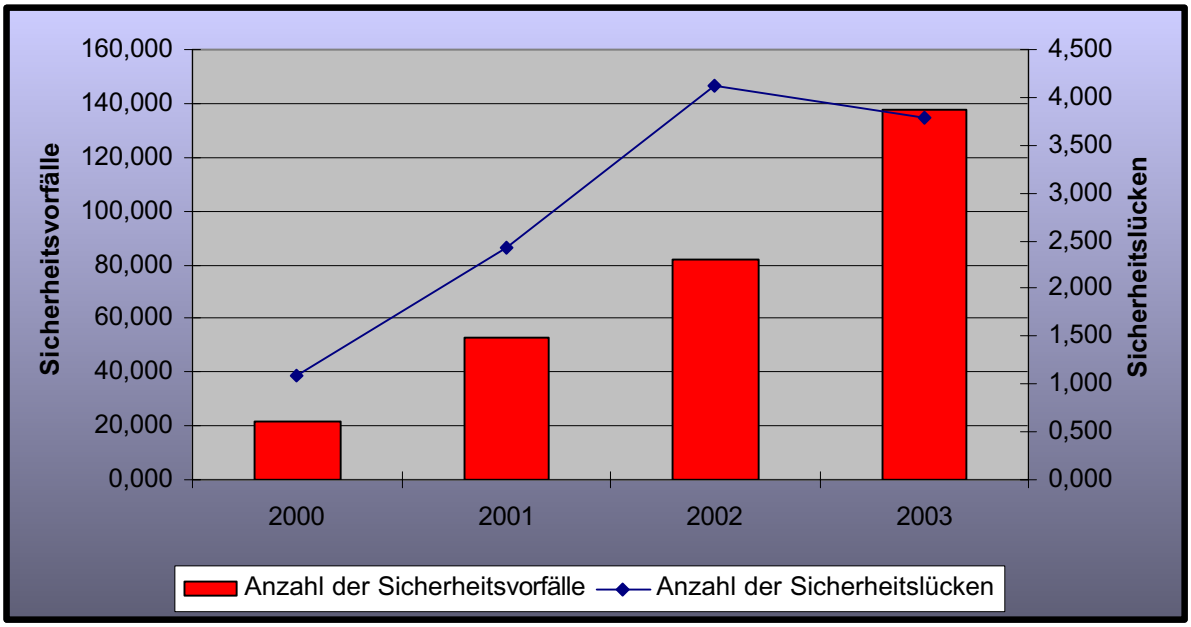

Abbildung 1: Sicherheitsvorfälle und Sicherheitslücken[10]

Vor diesem Hintergrund wird deutlich, dass die Sicherheit in der Informationstechnik (IT-Sicherheit) von zentraler Bedeutung für die Hochschulen ist und deshalb auch der Sicherung der IT-Strukturen entsprechender Stellenwert zukommen muss. Hierfür ist die Sicherstellung der Integrität, Verbindlichkeit, Vertraulichkeit und Verfügbarkeit von Daten, Diensten und Anwendungen unumgänglich. Viele Entscheidungsträger in den Hochschulen sind sich durchaus über die Notwendigkeit der Erreichung und Verbesserung der Informations- und Datensicherheit bewusst. Allerdings führt dieses Bewusstsein nicht immer zu entsprechenden Maßnahmen und Verhaltensänderungen.

[8] Ein Plug-In bezeichnet spezialisierte Software, die in Anwendungen für die Verarbeitung von besonderen Dateiformaten oder Inhalten zuständig ist. Hierfür benutzt es definierte Schnittstellen der Wirts-Software. So kann neue Technik auch mit älteren Anwendungen genutzt werden.
[9] Vgl. **Müller**, K. R. [2003, S. 1]; Vgl. **Hoppe**, G./**Prieß**, A. [2003, S. 16].
[10] http://www.cert.org/stats/cert_stats.html.

Häufig werden zwar einzelne Sicherheitsmaßnahmen[11] verwirklicht, allerdings liegt diesem Vorgehen nur selten ein durchdachtes und abgestimmtes Gesamtkonzept oder gar eine Strategie zugrunde.[12]

Ein strategisches Vorgehensmodell, wie Informations- und Datensicherheit in den Hochschulen systematisch, zielorientiert und effizient aufgebaut und weiterentwickelt werden kann, fehlt daher vielfach. Die Folgen sind unzureichende Transparenz und Nachvollziehbarkeit, Mehrfacharbeiten, eine latente Bedrohung für die Handlungsfähigkeit und das Image der Hochschulen, unnötige Kosten sowie zahlreiche Sicherheitslücken. Letztere finden häufig erst Beachtung, wenn akute Sicherheitsverletzungen auftreten, die vorhandene IT-Sicherheit versagt hat und wirtschaftlicher Schaden von schwer abschätzbarem Ausmaß entstanden ist.

Weitere Probleme ergeben sich vor allem dann, wenn rein reaktives Vorgehen dazu führt, dass Sicherheitslücken kurzfristig und symptomorientiert geschlossen, anstatt langfristig, ganzheitlich und insbesondere ursachenorientiert beseitigt zu werden.[13]

Ein wichtiger Schluss aus diesen Ausführungen und gleichzeitig Motivation für diese Diplomarbeit ist die Erkenntnis, dass eine bereichsspezifische Vorgehensweise in Sicherheitsfragen nicht zielführend sein kann. Hieraus ergibt sich die unmittelbare Notwendigkeit zur Entwicklung, Umsetzung, Fortschreibung und kontinuierlichen Anpassung einer einheitlichen und hochschulweit gültigen IT-Sicherheitsstrategie, bei einer umfassenderen Betrachtung, sogar besser noch einer Informationssicherheitsstrategie.

1.2 Zielsetzung

Die vorliegende Diplomarbeit soll dazu beitragen, für das Thema Informations- und Datensicherheit in den Hochschulen zu sensibilisieren, anhand konkreter Gefährdungen Bewusstsein zu wecken und zu motivieren, um die Informationen und IT-Systeme in den Hochschulen angemessen zu analysieren und adäquat zu schützen.

Dazu muss insbesondere auch das Informationssicherheitsmanagement effizient gestaltet werden.

---

[11] Aus einzelnen sicheren Komponenten entsteht nicht notwendigerweise ein sicheres Gesamtsystem.

[12] Vgl. **Stelzer**, D. [1993, S. 2]; Vgl. zu ähnlichen Einschätzungen **Badenhorst**, K. P./**Eloff**, J. H. P. [1989, S. 433] und **Weese**, E./**Lessing**, G. [1988, S. 14].

[13] Vgl. **Müller**, K. R. [2003, S. 3, 25].

Sicherheitsmaßnahmen können nur selten als Aktivitäten mit positivem Erfolgsbeitrag dargestellt werden und verursachen dem ersten Anschein nach nur Kosten.[14] Im Verlauf dieser Arbeit wird allerdings deutlich werden, dass diese Maßnahmen einen nicht unerheblichen Beitrag zur Erreichung der Organisationsziele und zur Reduktion von Schadenskosten leisten können. Informationssicherheit soll vom unangenehmen Randaspekt zu einem primären Qualitätsmerkmal und damit zu einem integralen Bestandteil eines leistungsfähigen Hochschulbetriebs werden und das Informationssicherheitsmanagement zu einem kontinuierlichen Prozess mit hoher Bedeutung avancieren.[15]

Im Rahmen dieser Arbeit wird daher der Entwicklungsprozess einer hochschulweiten Informationssicherheitsstrategie für eine deutsche Hochschule am Beispiel der UH dargestellt, welche die Realisierung eines generischen Sicherheitskonzepts unter Berücksichtigung der besonderen Bedingungen und Anforderungen einer Hochschule ermöglicht.

Die Sicherheitsstrategie hat dabei insbesondere zum Ziel, dazu beizutragen, alle Bereiche und Einrichtungen der Hochschule auf ein adäquates Sicherheitsniveau zu bringen, den gesamten Sicherheitsprozess effizient zu gestalten und dadurch die Leistungs- und Wettbewerbsfähigkeit der Hochschule langfristig zu verbessern.[16]

1.3 Methodische Vorgehensweise und Abgrenzung

Die Entwicklung und Umsetzung einer ganzheitlichen, bereichsunabhängigen und hochschulweiten Informationssicherheitsstrategie kann aufgrund der komplexen Materie, der sich permanent weiterentwickelnden technischen Gegebenheiten und der begrenzten finanziellen Budgets nur in einem kontinuierlichen Sicherheitsprozess erfolgen, der den speziellen Bedingungen der UH mit ihren vielen dezentralen Einrichtungen gerecht wird.[17]

Im Verlauf dieser Arbeit wird daher wie folgt vorgegangen: Nach dieser kurzen Einführung werden im zweiten Kapitel wichtige Grundlagen im Zusammenhang mit der Informationssicherheit behandelt. Im Anschluss daran folgt im dritten Kapitel ein

[14] Vgl. **Stelzer**, D. [1993, S. 69].
[15] Vgl. **Korden**, M. [2003, S. 1]; Vgl. **Pohlmann**, N./**Blumberg**, H. [2004, S. 122].
[16] Vgl. **Pohlmann**, N./**Blumberg**, H. [2004, S. 122].
[17] Vgl. **UH** [2002].

Überblick über die relevanten Rahmenbedingungen an der UH. Zur Erreichung und Aufrechterhaltung des angestrebten Sicherheitsniveaus im laufenden Hochschulbetrieb werden im Hauptteil dieser Arbeit zunächst eine Informationssicherheitsstrategie (vgl. Kapitel 4) und anschließend daran ein generisches Informationssicherheitskonzept (vgl. Kapitel 5) entwickelt. Die Schlussbetrachtung (vgl. Kapitel 6) beinhaltet sowohl eine Zusammenfassung wesentlicher Aspekte als auch einen Ausblick für die Zukunft.

In der vorliegenden Diplomarbeit wird weder der Versuch unternommen einen vollständigen Überblick über alle denkbaren Bedrohungen und Gefahren für die Informations- und Datensicherheit in den Hochschulen zu vermitteln, noch einen vollständigen Maßnahmenkatalog zu erstellen. Alle dargestellten Gefahren und Sicherheitsmaßnahmen sind daher lediglich exemplarischer Natur. Dies ist insbesondere vor dem Hintergrund der rasanten Fortentwicklung im IT-Bereich zu sehen, wo Bedrohungs- und Maßnahmenkataloge bereits zum Zeitpunkt ihres Erscheinens meist schon wieder unvollständig sind und daher permanenter Aktualisierung bedürfen.[18] An den entsprechenden Stellen wird jedoch stets auf aktuelle und weitergehende Informationsquellen verwiesen.

Bei der Darstellung der beispielhaften Sicherheitsmaßnahmen wird zudem auf technische bzw. operative Details weitgehend verzichtet, da es im Rahmen dieser Arbeit primär darum geht, die strategische Bedeutung dieser Schutzmaßnahmen für die Informations- und Datensicherheit in den Hochschulen deutlich zu machen.
Außerdem möchte ich an dieser Stelle noch darauf hinweisen, dass alle in dieser Arbeit verwendeten Funktionsbezeichnungen selbstverständlich geschlechtsneutral zu verstehen sind.

[18] Vgl. **Strauß**, C. [1991, S. 28f.].

6 Schlussbetrachtung

6.1 Zusammenfassung

In den Hochschulen gibt es heutzutage nur noch sehr wenige Bereiche, die keine IT-Systeme zur Bewältigung ihrer Aufgaben einsetzen. Einige Hochschuleinrichtungen sind mittlerweile so stark von der Funktionsfähigkeit und permanenten Verfügbarkeit dieser Systeme abhängig, dass sie ohne deren Einsatz erheblich beeinträchtigt und z. T. sogar Funktionsunfähig wären. Darüber hinaus ist die Nutzung von Informations- und Kommunikationsdiensten im Hochschulnetz und im weltweiten Internet für zahlreiche Hochschulangehörige inzwischen unverzichtbar geworden.

Parallel zu dieser Entwicklung nimmt die Anzahl und Vielfältigkeit gezielter Angriffe auf Rechnersysteme und Störungen im Hochschulnetz stetig zu. Aufgrund der daraus resultierenden zentralen Bedeutung der Informations- und Datensicherheit für die Hochschulen, muss insbesondere auch der Sicherung der IT-Strukturen entsprechender Stellenwert zukommen.

Vor dem Hintergrund der relativ komplexen Materie, der begrenzten Budgets und der sich ständig weiterentwickelnden technischen Gegebenheiten kann dies i. d. R. nur in einem systematisch geplanten Sicherheitsprozess erfolgen, der den besonderen Bedingungen und Anforderungen einer Hochschule gerecht wird.

Hierfür ist die Entwicklung, Umsetzung und regelmäßige Fortschreibung einer ganzheitlichen und hochschulweit gültigen Informationssicherheitsstrategie erforderlich. Die Sicherheitsstrategie muss zu einem wesentlichen Bestandteil der allgemeinen Hochschulpolitik werden und ist gezielt darauf auszurichten, Informations- und Datensicherheit in der Hochschule aufzubauen, langfristig zu erhalten und kontinuierlich zu verbessern. Die Strategie muss demzufolge langfristig angelegt und schriftlich fixiert sowie allen Beteiligten bekannt gemacht werden. Da ihre Wirksamkeit nicht zuletzt von der Akzeptanz aller Hochschulangehörigen abhängt, sollten diese sich zumindest grundsätzlich mit der Strategie identifizieren können und zu ihrer Einhaltung verpflichtet werden.

Alle Sicherheitsanstrengungen sind sowohl unter aufbau- als auch unter ablauforganisatorischen Aspekten zu konzipieren. Zur Planung, Durchführung und situationsspezifischen Umsetzung der Sicherheitsstrategie müssen entsprechende Verantwortungsbereiche abgegrenzt, Aufgaben und Befugnisse festgelegt und organisatorische Einheiten gebildet werden. Hierzu wird die Institutionalisierung eines Informationssicherheitsmanagements empfohlen.

Um potentiellen Sicherheitsproblemen vorzubeugen und bei sicherheitsrelevanten Ereignissen entsprechend reagieren zu können, gehört zur Strategieentwicklung insbesondere auch die Erstellung eines generischen Sicherheitskonzepts. Dieses Konzept soll die globalen Zielvorgaben der Sicherheitsstrategie konkretisieren und auf operativer Ebene realisieren.
Das Primärziel ist dabei, mit einem adäquaten Maßnahmenpaket, vorhandene Sicherheitslücken und Bedrohungen auf ein wirtschaftlich akzeptables Maß zu reduzieren bzw. im Notfall angemessen zu reagieren und somit die Informations- und Datensicherheit im laufenden IT-Betrieb der Hochschule zu gewährleisten.

6.2 Grenzen des Vorgehensmodells

Eine einfache und idealtypische Abarbeitung der einzelnen Phasen des Informationssicherheitsprozesses wird in der Praxis nicht möglich sein, da der Verlauf der Strategieentwicklung i. d. R. durch rekursive Strukturen gekennzeichnet ist.
So wird eine Hochschule beispielsweise nur selten in der Lage sein, bereits zu Beginn der Entwicklung einer Informationssicherheitsstrategie realistische Sicherheitsziele festzulegen, da es sich bei einem adäquaten Sicherheitsniveau grundsätzlich um einen Kompromiss aus Kosten für Schutzmaßnahmen und antizipierter Risikoreduzierung handelt. Die Kostenbestimmung für konkrete Sicherheitsmaßnahmen kann jedoch i. d. R. erst zu einem viel späteren Zeitpunkt der Strategieentwicklung durchgeführt werden.[397]
Die Entwicklung einer Informationssicherheitsstrategie ist weder ein einmaliger Vorgang noch ein zeitlich begrenztes Projekt, sondern ein kontinuierlicher und prinzipiell nie abgeschlossener Prozess.[398] Die grundsätzliche Bedeutung einzelner Gefahren und Sicherheitsmaßnahmen für die Informations- und Datensicherheit in den Hochschulen unterliegt im Zeitablauf einer permanenten Veränderung.
Eine Schutzmaßnahme, die zurzeit als sicher und angemessen eingestuft wird, kann schon in naher Zukunft unwirksam sein. Die Informationssicherheitsstrategie muss

[397] Vgl. **Stelzer**, D. [1993, S. 86].
[398] Vgl. **Hughes**, P. J. [1984, S. 66]; Vgl. **Liesen**, A. [1991, S. 286].

deshalb fortwährend an die dynamischen Einflussfaktoren der Sicherheit angepasst werden.[399]

Bei allen Sicherheitsanstrengungen muss prinzipiell darauf geachtet werden, dass die Bereiche Forschung und Lehre nicht unnötig durch Sicherheitsmaßnahmen eingeengt oder behindert werden. Andererseits sind die Aufgaben dieser beiden Bereiche kein wirkliches Argument für Forderungen nach einer völlig ungehinderten Nutzung der IT-Ressourcen auf Kosten der Informations- und Datensicherheit im Hochschulbereich.[400]

[399] Vgl. **Stelzer**, D. [1993, S. 86].
[400] Vgl. **Rossa**, C. [2003, S. 36].