Hochschule Wismar
Fachhochschule für Technik, Wirtschaft und Gestaltung
Fachbereich Wirtschaft

Hochschule Wismar
University of Technology, Business and Design
Department of Business

Dietrich Nöthens/Ulrike Mauritz

IT-Sicherheit an der Hochschule Wismar

Heft 11 / 2003

W D P

Wismarer Diskussionspapiere / Wismar Discussion Papers

Der Fachbereich Wirtschaft der Hochschule Wismar, Fachhochschule für Technik, Wirtschaft und Gestaltung bietet die Studiengänge Betriebswirtschaft, Management sozialer Dienstleistungen, Wirtschaftsinformatik und Wirtschaftsrecht an. Gegenstand der Ausbildung sind die verschiedenen Aspekte des Wirtschaftens in der Unternehmung, der modernen Verwaltungstätigkeit im sozialen Bereich, der Verbindung von angewandter Informatik und Wirtschaftswissenschaften sowie des Rechts im Bereich der Wirtschaft.

Nähere Informationen zu Studienangebot, Forschung und Ansprechpartnern finden Sie auf unserer Homepage im World Wide Web (WWW): http://www.wi.hs-wismar.de/.

Herausgeber: Prof. Dr. Jost W. Kramer
Fachbereich Wirtschaft
Hochschule Wismar
Fachhochschule für Technik, Wirtschaft und Gestaltung
Philipp-Müller-Straße
Postfach 12 10
D – 23966 Wismar
Telefon: ++49 / (0)3841 / 753 441
Fax: ++49 / (0)3841 / 753 131
e-mail: j.kramer@wi.hs-wismar.de

ISSN 1612-0884
ISBN 3-910102-36-0

JEL-Klassifikation Z00

Inhaltsverzeichnis

Analyse und Bewertung der Anforderungen an das Sicherheitsniveau der Informationssysteme an einer Hochschule zur Ableitung der Sicherheitsstrategie

Dietrich Nöthens

1. Problemstellung

Eine IT-Sicherheitsstrategie muss bestimmten Anforderungen genügen, insbesondere Gewährleistung von:

- Integrität
- Vertraulichkeit
- Verfügbarkeit
- Authentizität
- Beweisbarkeit
- Sicherheit gegen Ressourcen-Missbrauch

Der Nachweis des IT-Sicherheitsniveaus ist zu erbringen.

IT-Sicherheit ist nicht zum Null-Tarif zu haben:

-> Differenziertes Vorgehen entsprechend dem Sicherheitsbedarf erforderlich.

Zielstellung einer differenzierten IT-Sicherheitsstrategie:

- Ermittlung des Schutzbedarfs der Daten und der sie verwaltenden bzw. übertragenden Ressourcen.
- Ableitung des Schutzbedarfs in Abhängigkeit der zu erwartenden Schadenswirkungen bei Angriffen von Außen und Innen (-> Problem der Kostenoptimalität zwischen Aufwand und Nutzen).
- Anwendung geeigneter organisatorischer und technischer Verfahren und Maßnahmen zur Gewährleistung der IT-Sicherheit entsprechend dem erforderlichen Schutzbedarf.
- Verbindliche Regelung der Anwendung der Verfahren und Maßnahmen für die Fachbereiche der Hochschule in einer Richtlinie mit:
  - Auswahl der anzuwenden Verfahren
  - Regelung der Kontrolle der durchzuführenden Maßnahmen
  - Regelung von Verstößen gegen die vorgeschriebenen
  - Maßnahmen
  - Festlegung der Verantwortlichkeiten zur Durchsetzung der Maßnahmen
  - IT-Sicherheits-Management zum Erreichen des erforderlichen Sicherheitsniveaus

Abgrenzung Beitrag: Primärer Bezug auf **Daten**sicherheit. Ergänzung durch Überlegungen für vernetzte Rechner- und Netzwerk-Systeme

2. Datenanalyse

Klassifizierung der Daten nach ihrer Sensibilität einschließlich der die Daten verwaltenden und übertragenden Systeme (Ressourcen):

Sensibilität (Schutzbedürftigkeit):

- Bedarf an Vertraulichkeit
- Bedeutung der Daten und Ressourcen für die Erfüllung der
- Zielstellung der Einrichtung

2.1. Öffentliche Daten (public)

Merkmale:

- Informationen für Mitarbeiter und Öffentlichkeit
- Uneingeschränkt lesender Zugriff für alle
- Schreibender Zugriff für eingeschränkten Personenkreis
- Weitergabe von Rechten im Ermessen des Personenkreises

Hierzu: Webseiten, Bibo, LV-Skripte

2.2. Private Daten (private)

Merkmale:

- Daten in persönlicher Nutzung
- Lesender und schreibender Zugriff für den Besitzer
- Weitergabe der Zugriffsrechte im Ermessen des Besitzers

Hierzu: Mail- und Schriftverkehr, Lehrvorbereitungen, personenbezogene Daten in Verantwortung des Besitzers, Arbeitsaufgaben und Ergebnisse, Ausarbeitungen zu F&E- Themen

2.3. Systemdaten (administration)

Merkmale:

- Daten für die Systemverwaltung
- Lesender und schreibender Zugriff für eingeschränkten Personenkreis
- Weitergabe von Rechten im Ermessen des Personenkreises

Hierzu: System-, User-Verwaltung, Domain Name Service

2.4. Vertrauliche Daten (confidential)

Merkmal:

- Vertraulich zu behandelnde Daten über Personen, Einrichtungen, Vorgänge und Ergebnisse der Einrichtung
- Lesender und schreibender Zugriff für eingeschränkten Personenkreis
- Zentrale Vorgabe für Weitergabe von Rechten

Hierzu: Personenbezogene Daten außerhalb der Verantwortung der sie betreffenden Person, nicht für die Öffentlichkeit bestimmte Daten über Geschäftsprozesse, Forschungsergebnisse mit kommerzieller Nutzung.

3. Schadensbewertung

Voraussetzung: Anwendung von Backup- und Archivierungskonzepten für die Rekonstruktion im Störungsfall.

3.1. Öffentliche Daten

Relevante Schädigungen:

- Datenmanipulation
- Löschen
- Ausfall der Ressourcen

Schadensarten:

- Eingeschränkte Verfügbarkeit der Daten
- Verletzung der Datenintegrität

Schadenswirkung:

- Informationsdefizite
- Nutzung fehlerhafter Daten
- Vertrauensverlust
- Recovery
- ggf. Beseitigung von Malware

Schadensbewertung:

Folgeschäden für Einrichtung begrenzt
Eindeutige Reaktionen bei Schadenseintritt

-> Schadensbewertung auf der Basis angebbarer Verluste (u. a. Kosten für Recovery, Beseitigung von Malware)

-> **Schutzklasse I**

3.2. Private Daten

Relevante Schädigungen:
- Datenmanipulation
- Löschen
- Ausfall der Ressourcen
- Einsichtnahme in private Daten (Personenbezogene Daten, F&E)

Schadensarten:
- Verlust an Verfügbarkeit der Daten
- Verletzung der Datenintegrität
- Auskundschaften von Daten

Schadenswirkung:
- Informationsdefizite
- Missbrauch personenbezogener Daten
- Nutzung fehlerhafter Daten
- Recovery
- ggf. Beseitigung von Malware
- Nachnutzung von persönlichem Know-How
- Vertrauensverlust für Einrichtung bei Bekanntwerden der Einsichtnahme bzw. des Datenmissbrauchs

Schadensbewertung:
- Folgeschäden für Einrichtung begrenzt
- Eindeutige Reaktionen bei Schadenseintritt
- Persönliche Folgeschäden nicht einschätzbar

-> Schadensbewertung auf der Basis messbarer Verluste (u. a. Kosten für Recovery, Beseitigung von Malware)
-> **Schutzklasse II**

3.3. Systemdaten

Relevante Schädigungen:
- Manipulation Systemdaten
- Löschen Systemdaten
- Ausfall wichtiger Ressourcen
- Unbefugte Nutzung von Ressourcen
- Einsichtnahme in System- und personengebundene Daten

Schadenswirkung:
- Verfügbarkeitsverluste von System-Ressourcen
- Fehlleitung von Nutz- und Steuerungs-Informationen
- Sniffing von Informationen

- Missbrauch von System- und personen- bezogenen Daten
- Hoher Vertrauensverlust für Einrichtung bei Bekanntwerden

Schadensbewertung:

- Folgeschäden nicht begrenzt und nicht abschätzbar
- Reaktionen bei Schadenseintritt komplex in Abhängigkeit der Schädigung

-> Schadensbewertung auf der Basis der Begrenzung der Schadenswirkung mit besonderen Maßnahmen bei Schadenseintritt.

-> **Schutzklasse III**

3.4. Vertrauliche Daten

Relevante Schädigungen:

- Manipulation personenbezogener Daten, Geschäftsprozesse, F&E
- Einsichtnahme in personenbezogene Daten, Geschäftsprozesse, F&E-Ergebnisse
- Löschen
- Verfügbarkeitsverluste
- Ausfall der Ressourcen

Schadenswirkung:

- Missbrauch personenbezogener Daten, Geschäftsprozesse, F&E
- Identitätsschwindel
- Betrug

Schadensbewertung:

- Folgeschäden nicht begrenzt und nicht abschätzbar
- Reaktionen bei Schadenseintritt komplex in Abhängigkeit der Schädigung
- Hohe Vertrauensverluste für die Einrichtung bei Bekanntwerden
- Geschäftliche Verluste
- Verluste an Know-How
- Besonderheit: Personenbezogene Daten unterliegen dem Datenschutzgesetz

-> Schadensbewertung auf der Basis der Vermeidung des Schadenseintritts mit besonderen Maßnahmen bei Schadenseintritt.

-> **Schutzklasse IV**

4. Risikoanalyse und -bewertung

Problem der Quantifizierbarkeit von Schäden
-> Grundsätzliche Strategien:
- Quantitative Bewertung bei messbaren Verlusten
- Qualitative Bewertung

Bewertung des Risikos in zwei Sicherheitsstufen:

4.1. Sicherheitsstufe A

Bewertungsgrundlage: Messbare Verluste durch Schäden
- Berücksichtigung der Schutzklassen I und II
- Das Risiko ist die Schadenserwartung

Risikobewertung:
Risiko (S) = H(S) * W(S)

S : Schaden
H(S) : Quantifizierbare Schadenshöhe bei Schadenseintritt (~ Kosten für Recovery)
W(S) : Eintrittswahrscheinlichkeit für Schaden

-> Aufgabe: Ermittlung von H(S) und W(S) auf der Grundlage von statistischen Schadensfall-Analysen
-> Fragebögen!
-> Näherung: Qualitative Schätzung aufgrund von Erfahrungswerten

Qualitative Risikobewertung für Stufe A:
Relationen $R_q(S) = H_q(S) * W_q(S)$

$R_q(S)$ = gering * gering = gering
$R_q(S)$ = gering * mittel = gering/mittel
$R_q(S)$ = gering * hoch = mittel
$R_q(S)$ = mittel * mittel = mittel
$R_q(S)$ = mittel * hoch = mittel/hoch
$R_q(S)$ = hoch * hoch = hoch

4.2. Sicherheitsstufe B

- Die Schadenshöhe und die Folgeschäden sind grundsätzlich nicht begrenzt und quantifizierbar
- Bewertungsgrundlage ist die Eintrittswahrscheinlichkeit des Schadens bzw. der Erwartungswert der Zeit bis zum Vorfall

- Berücksichtigung der Schutzklassen III und IV
- Risiko ist die Wahrscheinlichkeit des Schadenseintritts

Risikobewertung:
Risiko(S) = W(S)

5. Sicherheitsstrategien

5.1. Sicherheitsstufe A

Grundsätzliche Zielstellung:

- Senkung der Eintrittswahrscheinlichkeit eines Schadens
- Begrenzung der Schadenswirkung

-> Verhinderung des unerlaubten Zugangs zu den Ressourcen
-> Erkennung des unerlaubten Zugangs
-> Zugriffsschutz für die Daten

- Realisierung der Zielstellung mit geeigneten technischen und organisatorischen Maßnahmen unter Beachtung der Verhältnismäßigkeit der Mittel:
  -> Alles, was nicht verboten ist, ist erlaubt
- Die Schutzmaßnahmen richten sich nach der Schadenserwartung (= Risiko für Sicherheitsstufe A). Anhaltspunkte ergeben sich aus der qualitativen Risiko-Bewertung (z. B. Anwendung kombinierter Schutzmaßnahmen bei hohem Risiko).
- Die Schutzmaßnahmen sind so auszuwählen, dass sie von den meisten bekannten Angriffsmethoden nur in Ausnahmefällen zu überwinden sind („Stark mit Ausnahmen“).
- Für Schutzklasse II:
  Anwendung von Krypto-Verfahren und der Digitalen Unterschrift liegt im Ermessen des Eigentümers der Daten. Entsprechende K.-Verfahren sind zur Verfügung zu stellen.
- Angriffe auf Daten und Ressourcen der Sicherheitsstufe A mit Überwinden der Schutzmaßnahmen dürfen nicht zum Zugang zu Daten und Ressourcen der Sicherheitsstufe B führen.
- Forderung nach allgemein gültigen, verbindlichen Back-Up- und Archivierungsstrategien.
- Verbindlich geregelte Anwendung aktueller Antiviren-Software.
- Verbindliche Regelungen für Implementierung von Patches.

5.2. Sicherheitsstufe B

Grundsätzliche Zielstellung:

- Minimale Eintrittswahrscheinlichkeit des Schadens
- Senkung des Zugangsrisikos auf eine geringe Restwahrscheinlichkeit
- Die Restwahrscheinlichkeit wird bei vertraulichen Daten durch Anwendung von Krypto-Verfahren berücksichtigt

Ziele:

-> Besondere Regelungen für den Zugriff auf Daten und Ressourcen
-> Erkennung und Meldung des unerlaubten Zugangs im Angriffsfall mit Sicherungsmaßnahmen

Realisierung der Zielstellung mit besonders wirksamen technischen und organisatorischen Maßnahmen: Alles, was nicht erlaubt ist, ist verboten

- Wirksame Maßnahmen sind solche, die für die bekannten Angriffsmethoden nicht überwindbar sind („Unüberwindbar mit Ausnahmen“).
- Die Anwendung von Krypto-Verfahren für sensible Daten der Schutzklassen III und IV ist verbindlich und in einer Krypto-Verordnung zu regeln. Die öffentlichen Schlüssel sind durch Zertifizierung zu beglaubigen.
- Die Regelung des Zugriffs auf sensible Daten und Ressourcen der Sicherheitsstufe B erfolgt über spezielle Verfahren der Nutzerauthentifikation.
- Für sensible Informationen, Schriftverkehr, Dokumente, Geschäftsprozesse der Sicherheitsstufe B ist die Authentizität der Objekte und des Absenders auf der Basis der Digitalen Unterschrift verbindlich nachzuweisen. Einzelheiten hierzu sind in der Krypto-Verordnung festzulegen.
- Für externe Kommunikationsbeziehungen mit sensiblen Daten sind Verfahren anzuwenden, die die Vertraulichkeit der Daten gewährleisten, die Integritätskontrolle ermöglichen und die Teilnehmer und Ressourcen gegenseitig eindeutig und zweifelsfrei identifizieren.
- Der unerlaubte Zugang zu Daten und Ressourcen der Sicherheitsstufe B ist mit entsprechenden Methoden zu erkennen, nachzuweisen und zu melden. Gleichzeitig sind automatisierte Verfahren anzuwenden, die die angegriffenen Ressourcen in einen nicht kritischen Zustand ohne weitere Gefährdung überführen.
- Zusätzlich gelten die für Sicherheitsstufe A angegebenen Forderungen (Backup, Antiviren, Patches usw.)

6. Zusammenfassung der Schutzmaßnahmen

- Verhinderung des unerlaubten Zugangs zu den Daten und Ressourcen durch organisatorische und technische Mittel in zwei Stufen der Stärke A und B.
- Automatische Erkennung des unerlaubten Zugangs in beiden Sicherheitsstufen A und B mit Meldung und Nachweisführung.
- Automatisierte Überführung der angegriffenen Ressourcen in einen unkritischen Zustand für Sicherheitsstufe B.
- Optionale Anwendung von Krypto-Verfahren und der Digitalen Unterschrift für Daten der Sicherheitsstufe A.
- Verbindliche Anwendung von Krypto-Verfahren und der Digitalen Unterschrift für sensible Daten der Sicherheitsstufe B.
- Anwendung spezieller Verfahren der Nutzerauthentifikation für den Zugriff auf Daten und Ressourcen der Sicherheitsstufe B.
- Anwendung zusätzlicher konventioneller Sicherheitsmaßnahmen.
- Nachweis des Sicherheitsniveaus
- Richtlinie mit verbindlich anzuwendenden organisatorischen und technischen IT- Sicherheitsregeln an der HS

Offene Türen im Netz - Untersuchungen zur Gewährleistung der Sicherheit in den IuK-Systemen am Beispiel ausgewählter Fachbereiche

Ulrike Mauritz

1. Einleitung

Die Notwendigkeit, sich intensiver mit dem Thema Informations- und Kommunikationssicherheit (IuK) an der Hochschule Wismar zu beschäftigen, wurde spätestens seit der Einführung der P2P-Tauschbörsen aktuell. Täglich erhält die Hochschule E-Mails und Briefe von Konzernen wie Warner Bros. mit der Aufforderung, Systeme auf MP3s oder Videos zu überprüfen. Die heruntergeladenen Dateien beschränken sich aber nicht nur auf Videos, Spiele und Musik, die Dateien können auch Viren und Trojanische Pferde enthalten, die Schäden und hohe Kosten auf den Systemen verursachen können. Neben diesen Tauschbörsen weisen die heterogenen Hochschulnetze weitere Sicherheitslücken auf, die ein Angreifer gezielt ausnutzen kann, um weitere Angriffe an „begehrteren“ Institutionen wie Microsoft oder der New Yorker Universität zu starten. Aus diesem Grund wurde eine Sicherheitsarbeitsgruppe der Hochschule Wismar ins Leben gerufen. Ein Teil der Forschungsarbeit der Gruppe bestand in der Vergabe von Diplomarbeiten zu dem Thema: Untersuchungen und Vorschläge zur Gewährleistung der Sicherheit in den IuK-Systemen der Hochschule Wismar. Zwei dieser Diplomarbeiten befassen sich mit Untersuchungen zur Gewährleistung der Sicherheit in den IuK-Systemen; eine Arbeit ist speziell auf die Verwaltung ausgerichtet, die andere auf ausgewählte Fachbereiche.

2. Portscanning

Die Grundlage für die von Herrn Marcel Zager und mir bearbeitete Diplomarbeit bildete ein Fragebogen, der mit den Administratoren der Fachbereiche Architektur, Design/Innenarchitektur, Bauingenieurwesen, Elektrotechnik und Informatik, Maschinenbau/Verfahrens- und Umwelttechnik sowie Wirtschaft zusammen beantwortet wurde. Durch diesen Fragebogen sollten hauptsächlich grundlegende Fragen wie zum Beispiel verwendete Betriebssysteme und Dienste oder Angriffsarten ermittelt werden. Darauf aufbauend wurde ein Portscan mit den Scannern NMapWin und Superscan 3.0 für die Fachbereiche Architektur, Bauingenieurwesen und Wirtschaft veranlasst, um die am häufigsten geöffneten Ports zu ermitteln. Ein Port ist der Ort, wo Daten/Informationen in und aus einem Rechner kommen; das Portscanning identifiziert dem-

nach die offenen Türen eines Systems. Das Scannen von Ports ist legitim und dient normalerweise der Verwaltung von Netzwerken. Angreifer verwenden das Scannen als ersten Schritt, um in ein System einzubrechen.

In einem weiteren Schritt wurden Angriffsszenarien an der Hochschule Wismar vorgestellt, die unter anderem durch die offenen Ports möglich sind. Es wurden außerdem Daten und Dienste analysiert und das Risiko der auftretenden Häufigkeit und des angerichteten Schadens ermittelt. Abschließend wurden allgemeine Maßnahmen vorgeschlagen, die Ausgangspunkt einer weiteren Forschungs-/Diplomarbeit sein könnten. Die Untersuchungen haben gezeigt, dass einige Sicherheitslücken bereits geschlossen wurden. Trotzdem ist eine konsequente Durchführung von weiteren Maßnahmen nötig, um die Hochschule auf ein gleich hohes Sicherheitsniveau zu bringen. Die Portscans in den Fachbereichen Architektur und Bauingenieurwesen stellten sich als Problem dar. Viele der Rechner waren ausgeschaltet, so dass eine Ermittlung der Sicherheitslücken nicht erfolgen konnte. Wenn man bedenkt, dass der SQL Slammer Wurm sich innerhalb von 10 Minuten weltweit verbreitet hat, kann man davon ausgehen, dass einer dieser Rechner, wenn er angeschaltet ist, einem Angreifer Raum für weitergehende Attacken bietet.

Autorenangaben

Prof. Dr.-Ing. Dietrich Nöthens
Fachbereich Wirtschaft
Hochschule Wismar
Philipp-Müller-Straße
Postfach 12 10
D – 23966 Wismar
Telefon: ++49 / (0)3841 / 753 606
Fax: ++49 / (0)3841 / 753 131
E-mail: d.noethens@wi.hs-wismar.de

Dipl. Wirtsch.-Inf. Ulrike Mauritz
Fachbereich Wirtschaft
Hochschule Wismar
Philipp-Müller-Straße
Postfach 12 10
D – 23966 Wismar
Telefon: ++49 / (0)3841 / 753 606
Fax: ++49 / (0)3841 / 753 131
E-mail: u.mauritz@stud.hs-wismar.de

WDP - Wismarer Diskussionspapiere / Wismar Discussion Papers

Heft 01/2003	Jost W. Kramer: Fortschrittsfähigkeit gefragt: Haben die Kreditgenossenschaften als Genossenschaften eine Zukunft?
Heft 02/2003	Julia Neumann-Szyszka: Einsatzmöglichkeiten der Balanced Scorecard in mittelständischen (Fertigungs-)Unternehmen
Heft 03/2003	Melanie Pippig: Möglichkeiten und Grenzen der Messung von Kundenzufriedenheit in einem Krankenhaus
Heft 04/2003	Jost W. Kramer: Entwicklung und Perspektiven der produktivgenossenschaftlichen Unternehmensform
Heft 05/2003	Jost W. Kramer: Produktivgenossenschaften als Instrument der Arbeitsmarktpolitik. Anmerkungen zum Berliner Förderungskonzept
Heft 06/2003	Herbert Neunteufel/Gottfried Rössel/Uwe Sassenberg: Das Marketingniveau in der Kunststoffbranche Westmecklenburgs
Heft 07/2003	Uwe Lämmel: Data-Mining mittels künstlicher neuronaler Netze
Heft 08/2003	Harald Mumm: Entwurf und Implementierung einer objektorientierten Programmiersprache für die Paula-Virtuelle-Maschine
Heft 09/2003	Jost W. Kramer: Optimaler Wettbewerb - Überlegungen zur Dimensionierung von Konkurrenz
Heft 10/2003	Jost W. Kramer: The Allocation of Property Rights within Registered Co-operatives in Germany
Heft 11/2003	Dietrich Nöthens/Ulrike Mauritz: IT-Sicherheit an der Hochschule Wismar