Rechner- und Netzwerksicherheit im Hochschulbereich

Konzeptstudie

Prof. Dr.-Ing. Jürgen Quade
Dipl.-Ing. Arne Sprick
Dipl.-Ing. Harald Mürmann
Peter Bartosch

Herausgeber :

Prof. Dr.-Ing. Hans Dieter Beims

Fachbereich Elektrotechnik und Informatik
Hochschule Niederrhein

Autoren :

Prof. Dr.-Ing. Jürgen Quade
Dipl.-Ing. Arne Sprick
Peter Bartosch

Fachbereich Elektrotechnik und Informatik
Hochschule Niederrhein

Dipl.-Ing. Harald Mürmann

Datenverarbeitungszentrale
Hochschule Niederrhein

Schriftenreihe des Fachbereichs Elektrotechnik und Informatik

herausgegeben von

Prof. Dr.-Ing. Hans Dieter Beims
Fachbereich Elektrotechnik und Informatik
Hochschule Niederrhein

Band 1/2002

Jürgen Quade, Arne Sprick,
Harald Mürmann, Peter Bartosch

Rechner- und Netzwerksicherheit im Hochschulbereich

Shaker Verlag
Aachen 2002

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Quade, Jürgen:
Rechner- und Netzwerksicherheit im Hochschulbereich / Jürgen Quade, Arne Sprick, Harald Mürmann, Peter Bartosch.
Aachen : Shaker, 2002
(Schriftenreihe des Fachbereichs Elektrotechnik und Informatik ; Bd. 1/2002)

ISBN 3-8322-0962-X

ISBN 3-8322-0962-X
ISSN 1610-9392

Shaker Verlag GmbH • Postfach 101818 • 52018 Aachen
Telefon: 02407 / 95 96 - 0 • Telefax: 02407 / 95 96 - 9
Internet: www.shaker.de • eMail: info@shaker.de

Vorwort des Dekans

Band 1 der Schriftenreihe ist erschienen und läutet damit ein neues Kapitel des Fachbereichs Elektrotechnik und Informatik an der Hochschule Niederrhein ein. Die Fachhochschulen beschäftigen sich seit längerer Zeit mit Forschungen und Entwicklungen, die sich von der Forschung an klassischen Universitäten durch starken Anwendungsbezug unterscheiden.

Neue Felder der Technik werden erschlossen und beschäftigen die Wissenschaftler. Da ist es nur konsequent, dass die Ergebnisse der Forschungen und Entwicklungen einem größeren Publikum bekannt gemacht werden. Aus diesen Überlegungen heraus ist die Schriftenreihe des Fachbereichs Elektrotechnik und Informatik entstanden.

Wir sind dem Herausgeber Herrn Prof. Dr.-Ing. Hans Dieter Beims dankbar, dass er die Initiative ergriffen hat, und den Autoren unter Leitung von Herrn Prof. Dr.-Ing. Jürgen Quade, dass sie den ersten Band mit ihrem Beitrag gestaltet haben.

Ich wünsche der Schriftenreihe Erfolg, eine interessierte Leserschaft und ein „langes Leben".

Prof. Dr.-Ing. Rainer Wallnig
Dekan des Fachbereichs Elektrotechnik und Informatik

Vorwort des Herausgebers

„Rechner- und Netzwerksicherheit" – wem fällt dabei nicht spontan die letzte unangenehme Begegnung mit einem der unzähligen „Computer-Viren" ein. Es ist einem glücklichen Umstand zu verdanken, dass sich der erste Band der *„Schriftenreihe des Fachbereichs Elektrotechnik und Informatik"* gerade diesem Thema widmet, zeigt dies doch, welchem Wandel sowohl der Alltag als auch die Fragestellungen bei Forschungs- und Entwicklungsaufgaben in einem Fachbereich unterliegen.

Ben Shneiderman, einer der Protagonisten moderner Mensch-Maschine-Schnittstellen, beschreibt in seinem „creativity framework"[1] die Aktivitäten *Collect*, *Relate*, *Create* und *Donate* als die wesentlichen Bestandteile kreativer Prozesse.

Ganz im Sinne der Aktivität *Donate* stellt die neue Schriftenreihe den vielen Kreativen im Fachbereich und ihren Partnern aus Industrie und Wirtschaft ein Forum zur Präsentation ihrer Ideen, ihrer aktuellen Forschungs- und Entwicklungsarbeiten und den gemeinsam erreichten Zielen zur Verfügung.

Dem Rektorat der Hochschule Niederrhein und dem Förderverein des Fachbereichs danke ich für die Unterstützung bei der Veröffentlichung des ersten Bandes.

Prof. Dr.-Ing. Hans Dieter Beims

[1] Shneiderman, B. Creating Creativity: User Interfaces for support innvovation. ACM Transactions on Computer-Human Interaction 7, 1 (March 2000)

Inhaltsverzeichnis

Vorwort ..... **vii**
1. Einleitung **1**
1.1. Zur Durchführung der Studie 5
1.2. Gefährdungspotenzial 6
1.3. Angriffstechniken 8
1.4. Die Angreifer 11
2. Istzustand **13**
2.1. Struktur 13
2.1.1. Physikalische Netzstruktur 13
2.1.2. Logische Netzstruktur 14
2.1.3. Software 15
2.1.4. Managementstrukturen 16
2.1.5. Personalsituation 17
2.1.5.1. DV-Zentrale 17
2.1.5.2. Bibliothek 17
2.1.5.3. Verwaltung 17
2.1.5.4. Labore 18
2.1.5.5. Mitarbeiterrechner 18
2.1.6. Installierte Sicherheitsmaßnahmen 18
2.2. Mitarbeiterbefragung 18
2.3. Ergebnisse Penetrationstest 24
2.3.1. Allgemeine Bemerkungen zur Testdurchführung 24
2.3.2. Ergebnisse 25
2.4. Sicherheitsrelevante Ereignisse 29
2.4.1. Vorbemerkungen 29
2.4.2. Chronologische Aufzählung 30
2.5. Geplante Netzerweiterungen 42
2.5.1. Funknetzbereich 43
2.5.2. Selbstbedienungsfunktionen 43
2.6. Sicherheitsrelevante Bewertung der gegenwärtigen IT-Struktur 43
3. Bedrohungs- und Schadensanalyse **47**
3.1. Zentrale Dienste 48
3.2. Verwaltung 49
3.3. Bibliothek 50
3.4. Labore 51
3.5. Mitarbeiter-Arbeitsplätze 53
3.6. Sonstige vernetzte Komponenten 54
3.7. Bewertung 55

4. Maßnahmen 59
4.1. Strukturelle Maßnahmen 60
4.1.1. Umstellung auf private Netzadressen 60
4.1.2. Absicherung von Rechnerpools über Firewalls 61
4.1.3. Zentrale User-Authentifizierung 64
4.1.4. Physikalische Entkopplung geschäftskritischer Rechner 65
4.1.5. Demilitarisierte Zone (DMZ) für die Verwaltungs-DV 67
4.2. Personal 67
4.2.1. Site Security Manager 67
4.2.1.1. Aufgabenbeschreibung 68
4.2.1.2. Position innerhalb der Hochschule 69
4.2.1.3. Qualifikation des SSM 69
4.2.2. Schulungsmaßnahmen 70
4.2.2.1. Sicherheitsbroschüren 70
4.2.2.2. Schulungen 70
4.2.3. Verbesserung des Informationsaustausches 72
4.3. Management 72
4.3.1. Einführung eines Melde- bzw. Berichtswesens 72
4.3.2. Aufstellen von Notfallplänen 73
4.3.3. Verfahrensanweisungen 75
4.3.4. Regelmäßige Security Audits (Penetrationstests) 75
4.4. Software 76
4.4.1. Virenüberwachung 76
4.4.2. Einsatz abhörsicherer Software 77
4.4.2.1. Secure Shell 77
4.4.2.2. Pop 77
4.4.2.3. Verschlüsselter E-Mail-Verkehr 77
4.4.3. Tripwire für die zentralen Rechner 78
4.4.4. Einsatz von Open-Source-Software 79
4.4.5. Logfileüberwachung manuell und automatisch (IDS) 79
4.5. Realisierung 80
5. Zusammenfassung 85
A. Zur Durchführung der Studie 89
A.1. Kerninhalte und Zielgruppenbestimmung 89
A.1.1. Lagebestimmung 90
A.1.2. Maßnahmenkatalog 90
A.1.3. Schwerpunktsetzung 91
A.2. Organisatorische Aspekte 92
A.2.1. Durchführende Instanz 92
A.2.2. Handhabung der Ergebnisse 94
A.3. Arbeitsphasen 95
A.3.1. Vorbereitung 95

A.3.2. Istanalyse ... 96
A.3.2.1. Mitarbeiterbefragung. ... 96
A.3.2.2. Interviews. ... 97
A.3.2.3. Penetrationstest ... 98
A.3.2.4. Auswertung ... 99
A.3.3. Konzept- und Maßnahmenentwicklung ... 100
A.3.4. Schriftliche Abfassung ... 100
Literatur- und Quellennachweis ... 103

Tabellenverzeichnis

2-1. Gesamtergebnis des Penetrationstests 25
2-2. Sicherheitslöcher nach gescannten IP-Blöcken 28
3-1. Bedrohungs- und Schadensanalyse bezüglich externer Angriffe 56
4-1. Maßnahmen der Stufe 1 80
4-2. Maßnahmen der Stufe 2 81
4-3. Maßnahmen der Stufe 3 83
4-4. Auslastung des Site Security Manager 83

Abbildungsverzeichnis

1-1. Gecrackter Webserver der FH-Düsseldorf (30.12.2001) 1
1-2. Gecrackter Webserver der FH-Düsseldorf (3.1.2002) 2
1-3. Defacements pro Jahr [mi2g2002] 2
1-4. Gecrackter Webserver der FH-Düsseldorf (14.1.2002) 3
1-5. Bewußtsein und Verantwortlichkeiten im Absicherungsprozeß 4
1-6. Gecrackter Webserver der FH-Düsseldorf (17.1.2002) 5
2-1. Physikalische Struktur 13
2-2. Art des Rechners 19
2-3. Genutzte Dienste 20
2-4. Selbsteinschätzung der Nutzer 21
2-5. Datenwerte auf Mitarbeiterrechnern 22
2-6. Datensicherung 22
2-7. Häufigkeit von Virenprüfungen 23
2-8. Sicherheitslöcher nach IP-Blöcken 26
2-9. Sicherheitswarnungen nach IP-Blöcken 27
2-10. Sicherheitshinweise nach IP-Blöcken 27
2-11. Angegriffene Server der DVZ 38
2-12. Zurückverfolgung von Einzelangriffen 39
2-13. Zurückverfolgung von Mehrfachangriffen 39
2-14. Netzverkehr eines DV-Labors (KW5) 41
2-15. Netzverkehr eines DV-Labors (23.01.2002) 41
2-16. Gefilterter Mitschnitt eines Netzverkehrs per tcpdump 45
3-1. Faktoren, die die Kritikalität beeinflussen 47
3-2. Kritikalität bezüglich externer Angriffe 55
4-1. Hochschulnetz mit über Firewall abgesicherten Rechnerpools 62
4-2. Einsatz einer Firewall zur Sicherung eines Rechnerpools 63
4-3. Einsatz einer Firewall zur Sicherung eines Rechnerpools mit Server 63
4-4. Einsatz einer Demilitarisierten Zone zur Sicherung gegen Angriffe von Außen und von Innen 64
4-5. Ankopplung ans Verwaltungsnetz per VPN 65

Gleichungen

3-1. Berechnungsgrundlage der Kritikalität 56

Vorwort

Die vorliegende Studie ist das Ergebnis einer Untersuchung des Sicherheitszustandes der IT-Infrastruktur der Hochschule Niederrhein. Ziel bei der Erstellung war es, nicht allein den Zustand zu erfassen und mögliche Maßnahmen zur Erhöhung der Sicherheit abzuleiten, sondern zugleich diese Maßnahmen so zu präsentieren, dass die Studie als Entscheidungsvorlage und Entscheidungsgrundlage dienen kann.

Wie erwartet und wie evaluiert ist der Sicherheitszustand der IT-Infrastruktur an der untersuchten Hochschule erschreckend: jeder zweite Rechner der Hochschule weist Sicherheitslöcher auf, durch die ein Cracker in den Rechner einbrechen kann, die Netzkomponenten sind ständigen Angriffen - durchaus auch erfolgreichen - ausgesetzt, und über 50% des Personals gibt zu, mangelhafte Kenntnisse bezüglich Rechner- und Netzwerksicherheit zu haben. Ratschläge der DVZ werden nicht beachtet, Netzerweiterungen werden geplant, ohne sicherheitstechnisch ausreichend beleuchtet worden zu sein und Fachbereiche bestellen Virenbeauftragte, die sich selbst explizit aus der Informationskette bezüglich Virenproblematik ausschließen.

Drei primäre Ursachen lassen sich für dieses Ergebnis nennen: Erstens fehlt es an der Sensibilisierung aller Verantwortlichen, insbesondere auch des Managements bezüglich des Themas, zweitens an personellen und drittens an finanziellen Mitteln. So ist das Netz der Hochschule aus rein funktionaler Hinsicht gewachsen, Sicherheitsaspekte haben kaum eine Rolle gespielt.

Die heutige Situation ist durch die drei erwähnten Defizite gekennzeichnet, wobei die fehlende Sensibilisierung das größte Manko darstellt. Das Thema Rechner- und Netzwerksicherheit ist aktueller denn je und längst zu einem Managementthema geworden: Security-Strukturen und -Strategien müssen im Leitungsgremium beschlossen, etabliert und überprüft werden!

Daher bilden Managementmaßnahmen die erste Stufe eines dreistufigen Konzeptes, welches den Zustand der Rechner- und Netzwerksicherheit an der untersuchten Hochschule auf ein akzeptables Maß bringen kann. Die Realisierung des Konzeptes ist mit finanziellen Aufwänden verbunden, insbesondere durch die Schaffung einer in der Industrie und an modernen Hochschulen längst üblichen Stelle, die des Site Security Managers (siehe hierzu beispielsweise [heise250102]). Durch Besetzung einer derartigen Position kann mit vergleichsweise geringem Aufwand ein erhebliches Plus an Sicherheit erreicht werden.

Dennoch sollte von vornherein klar gestellt werden, dass die vorgeschlagenen Maßnahmen einen möglichen Schaden nicht gänzlich verhindern, sondern nur minimieren können.

Der Maßnahmenkatalog zur Steigerung der Rechner- und Netzwerksicherheit wurde auf Basis des Gefährungspotenzials - ermittelt über eine

Mitarbeiterbefragung - und des gegenwärtigen Sicherheits-Istzustandes - erfaßt durch einen Penetrationstest - aufgestellt. Die dabei vorgeschlagenen Maßnahmen wurden in Interviews mit in der Hochschul-DV tätigen Mitarbeitern diskutiert und an die Anforderungen einer modernen Hochschule angepaßt.

Die vorliegende Studie hat ergeben, dass als erstes strategische Entscheidungen notwendig sind. Sie richtet sich daher zunächst an das Management und die Entscheidungsträger der Hochschule. Allerdings helfen die vorgestellten technischen Maßnahmen auch den Systemadministratoren bei der Etablierung geeigneter Vorkehrungen.

Einen schnellen Überblick über die Studie verschafft sich der, der zunächst das Kapitel *Sicherheitsrelevante Bewertung der gegenwärtigen IT-Struktur* und schließlich die *Zusammenfassung* liest. Die Teile, die zur eigentlichen Entscheidungsvorlage gehören, finden sich im Kapitel *Realisierung*.