

Jahrbuch der
Heinrich-Heine-Universität
Düsseldorf

2004

Heinrich-Heine

HEINRICH HEINE
UNIVERSITÄT
DÜSSELDORF



Heinrich-Heine

ISBN 3-9808514-3-5

stitute, die ähnliche Anforderungen an Konnektivität und Sicherheit aufweisen, zu einem Subnetz mit gemeinsamen Firewallregeln zusammenfasst.

Die bisherigen Erfahrungen belegen einen drastischen Rückgang an sicherheitskritischen Vorfällen wie Vireneinfektionen und Hackerangriffen in den firewallgeschützten Bereichen. Ein gewisses Restrisiko stellen allerdings mobile Computer dar, die zeitweise im Netz der Heinrich-Heine-Universität, zwischen durch aber am häuslichen Internetanschluss, auf Reisen, bei Tagungen oder an ähnlichen Orten betrieben werden, an denen die Gefahr einer „Kontamination“ mit Schadsoftware relativ hoch ist. Sie werden dann virenverseucht ins Institutsnetz eingebracht, wo sie im eigentlich geschützten Bereich andere Computersysteme attackieren. Hiergegen hilft zurzeit nur ein diszipliniertes Umgang mit mobilen Systemen; dazu gehört die gründliche Überprüfung des Rechners mit aktueller Antivirensoftware, bevor er mit dem Universitätsnetz verbunden wird. Mittelfristig wird in besonders gefährdeten Bereichen an die Einrichtung eines besonderen Laptopnetzes zu denken sein, von dem aus nur ein streng kontrollierter Zugang zum stationären Institutsnetz gestattet wird.

Literatur

- „Datenschutzordnung der Heinrich-Heine-Universität Düsseldorf“ vom 23. November 2004, http://www.uni-duesseldorf.de/cert/docs/Datenschutzordnung_23112004.pdf.
- GORDON, Lawrence A., Martin P. LOEB, William LUCYSHYN und Robert RICHARDSON: „2004 CSI/FBI Computer Crime and Security Survey“, 2004. http://compnet.com/goosidb_area/pdfs/fbi/FBI2004.pdf (14.07.2005).
- LABISCH, Alfons: „IT-Sicherheitskonzept der Heinrich-Heine-Universität Düsseldorf vom 6. Dezember 2004“, 2004. http://www.uni-duesseldorf.de/cert/docs/IT-Sicherheits-Rahmenkonzept_06122004.pdf (14.07.2005).
- SYMANTEC CORPORATION: „Symantec Internet Security Threat Report, Vol. VII“, 2005. <http://enterprisecurity.symantec.com/content.cfm?articleid=1539>.
- THE SANS INSTITUTE: „The Most Critical New Vulnerabilities Discovered or Patched During the First Quarter of 2005“, 2005. <http://www.sans.org/top20/Q1-2005update/> (14.07.2005).

entgegen wie die im Vergleich zu Unternehmen und gemessen an der Menge vorhandener IT-Arbeitsplätze geringe Zahl hauptamtlicher Fachkräfte für Installation und Betreuung der Systeme. Diese Aufgaben werden oft nebenbei von Personen übernommen, die schwerpunktmäßig in der Forschung und Lehre beziehungsweise am eigenen Studien- oder Promotionsabschluss arbeiten.

Um diesen Gegebenheiten Rechnung zu tragen und die IT trotz der vielfältigen, sich wandelnden Bedrohungen funktionsfähig zu erhalten, legt das IT-Sicherheitskonzept der Heinrich-Heine-Universität⁸ Verantwortlichkeiten sowie Pflichten der Nutzer und Betreiber von IT-Systemen fest. In Übereinstimmung mit den Regelungen der Datenschutzordnung⁹ liegt die Verantwortung für die Sicherheit bei den Dekanen bzw. den Leiterinnen und Leitern der zentralen Einrichtungen. Sie können durch interne Regelungen und Delegation von Zuständigkeiten den individuellen Gegebenheiten der Fakultäten und der Einrichtungen Rechnung tragen. Darüber hinaus trifft das Sicherheitskonzept allgemeine Festlegungen, die insbesondere die Funktionsfähigkeit des Gesamtnetzes sicherstellen und Grundlage sind für Maßnahmen im Störfall. Detailliertere Regelungen werden in einer ergänzenden Technischen Anleitung getroffen, die an die jeweiligen Erfordernisse und technischen Möglichkeiten angepasst wird.

Technische Maßnahmen: Viren-/Spamfilter, Firewalls

Im Jahr 2004 wurde die Bearbeitung ein- und ausgehender E-Mail umstrukturiert und ein zusätzlicher Server in Betrieb genommen, der virenverseuchte Mail ausfiltert, sowohl zum Schutz der Computersysteme im eigenen Netz als auch mit dem Ziel, die Virenverbreitung durch infizierte Rechner innerhalb der Heinrich-Heine-Universität zu unterbinden. Inzwischen findet auch eine Spamfilterung statt, damit E-Mail als Kommunikationsmedium auch angesichts der noch immer anwachsenden Flut unverlangter (und in aller Regel unerwünschter) Werbeemail überhaupt benutzbar bleibt.

Zum Einsatz kommt ein kommerzielles Produkt der Firma Sophos, denn es erscheint unabdingbar, auf die immer neuen Tricks der Spammer, eine Filterung zu unterlaufen, durch ständige Anpassung des Regelwerks zu reagieren. Dies kann derzeit, ähnlich wie beim Virenschutz, nur eine professionelle und damit auch kostenpflichtige Dienstleistung sicherstellen.

Große Teile des Netzes der Heinrich-Heine-Universität sind mittlerweile durch Firewallsysteme gegen Angriffe von außen wie auch aus fremden Bereichen innerhalb der Universität sowie gegen unkontrollierte Verbreitung von Computerviren und -würmern geschützt, wie es auch das IT-Sicherheitskonzept¹⁰ der Universität fordert. Die Firewalls werden in einigen Fällen anwenderseitig betrieben; das URZ setzt zudem zentrale Firewallserver ein, die auf zwei getrennte Standorte verteilt sind, separate Netzwerkbindungen aufweisen und damit eine erhöhte Ausfallsicherheit bieten. Diese werden derzeit zum Schutz von ca. 40 verschiedenen Bereichen genutzt, die je nach Umfang, Netztopologie und organisatorischen Gegebenheiten unterschiedliche Einheiten vom einzelnen Institut bis hin zu einer kompletten Fakultät umfassen. In den meisten Fällen sind mehrere In-

⁸ Vgl. Labisch (2004).

⁹ Vgl. Datenschutzordnung der Heinrich-Heine-Universität Düsseldorf vom 23. November 2004.

¹⁰ Vgl. Labisch (2004).

te Aktivitäten entfalten. Adware stellt nicht immer ein direktes Sicherheitsproblem dar; sie belästigt die Nutzerin oder den Nutzer beispielsweise durch gelegentlich erscheinende Fenster mit Werbebotschaften. Der angerichtete Schaden besteht eher in der Mühe und dem Zeitaufwand, diese Programme wieder loszuwerden. Manche Formen der Adware hingegen sammeln Informationen über das Nutzerverhalten im Web und machen diese einem Anbieter zugänglich, damit er seine Werbung optimal platzieren kann. Es ergeben sich dadurch fließende Übergänge zur Spyware, die gezielt Aktionen des Anwenders überwacht und zum Beispiel versucht, eingegebene Passwörter und Kreditkartennummern abzufangen und Fremden für betrügerische Zwecke verfügbar zu machen.

Modeme Computer sind in der Lage, große Mengen an Informationen, die durch Ad- und Spyware heimlich beschafft wurden, auszuwerten und lohnende Ziele herauszufinden, die anschließend mit Werbung bedacht oder als Betrugspotential ausersieht werden. Insofern ist damit zu rechnen, dass diese Arten von Schadsoftware noch wesentlich weiterentwickelt werden.

Smartphones – wachsende Leistung, wachsende Gefährdung

Viele Kommunikationsgeräte weisen heute intern regelrechte Computerarchitekturen auf, die denen der PCs und Laptops sehr ähnlich sind und oft auch ähnliche Betriebssysteme nutzen. So ist es nur folgerichtig, dass schon die ersten Wirmen und Trojanischen Pferde aufgetreten sind, die sich über Smartphones, moderne „intelligente“ mobile Telefone, ausbreiten. Auch hier sind verschiedene Schadensszenarien denkbar und teilweise schon realisiert: Die Eindringlinge können die Sicherheitseinstellungen des Telefons ändern oder außer Kraft setzen, das Benutzerverhalten ausspionieren, Fremden die Kommunikation auf Kosten des Eigentümers ermöglichen, Werbung verbreiten oder das Telefon schlicht unbrauchbar machen – auch daraus lässt sich womöglich noch Kapital schlagen.

Unterstützt wird diese Entwicklung dadurch, dass die heutigen Handynetze permanenten Kontakt zum Internet bieten und die Geräte zudem schwer kontrollierbare Ad-hoc-Netzwerkverbindungen (meist nach dem Bluetooth-Standard) aufbauen können. So ergeben sich vielfältige Angriffsmöglichkeiten. Zieht man in Betracht, dass auch Drucker, Kopierer, Webcams und Geräte der Unterhaltungselektronik zunehmend vernetzt und mit PC-ähnlicher Hardware ausgestattet werden, so lässt sich das daraus erwachsende Gefährdungspotenzial nur erahnen.

Herausforderungen für die Heinrich-Heine-Universität

Die Universität ist naturgemäß von den Gefahren, denen vernetzte IT-Systeme ausgesetzt sind, mindestens in gleichem Maße betroffen wie ein Wirtschaftsunternehmen vergleichbarer Größenordnung. Die Risiken für die universitäre IT sind eher noch höher einzuschätzen; sie ist stärker mit der Außenwelt vernetzt, denn Forscherinnen und Forscher, Lehrende und Lernende nutzen ein breiteres Spektrum an Anwendungen und Kommunikationsprotokollen, als dies im Unternehmensbereich üblich ist, und in einigen Bereichen werden Inhalte oder technische Aspekte der Kommunikation selbst zum Forschungsgegenstand.

Die ausgeprägt heterogene Geräte- und Softwareausstattung innerhalb der Heinrich-Heine-Universität, die den sehr unterschiedlichen Einsatzumgebungen Rechnung tragen soll, steht ebenso der durchgängigen Realisierung einer einheitlichen Sicherheitspolicy

hen viele auf Aufforderungen ein, auf E-Mails zu reagieren, die scheinbar von der Bank oder vom Auktionshaus kommen und zur Eingabe von persönlichen Daten, Kreditkartennummern, Passwörtern und Ähnlichem auf Webseiten auffordern, die den Originalseiten des jeweiligen Anbieters täuschend echt nachgemacht sind – dass die Mails ebenso wie die Webseiten häufig haarsträubende Rechtschreib- und Grammatikfehler aufweisen, wird inzwischen wohl als normal hingenommen...

Symantec gibt an, Ende 2004 33 Millionen Phishing-E-Mails⁶ pro Woche abgefangen zu haben, was einem Anstieg auf nahezu das Vierfache innerhalb eines halben Jahres entspricht. Damit stellen diese Aktivitäten nicht nur eine Gefahr für unvorsichtige Privatpersonen dar, sondern könnten auch zu einem Vertrauensverlust für die E-Commerce-Anbieter führen und deren Geschäftsmodelle nachhaltig schädigen. Einen absolut zuverlässigen Schutz vor solchen betrügerischen Machenschaften gibt es nicht – die beste Abwehr besteht in einem gesunden Misstrauen: Wer dubiose Mails von einem Unternehmen erhält, sollte lieber telefonisch oder per E-Mail an eine zuvor bekannte Adresse um eine Bestätigung bitten. Wünschenswert wäre zudem der vermehrte Einsatz von signierten E-Mails im Verkehr zwischen Unternehmen und ihren Kunden, damit Fälschungen erschwert werden.

Webanwendungen in Gefahr

Webanwendungen erfreuen sich zunehmender Beliebtheit, sowohl im Internet wie im Intranet. Bei ihnen wird der Webbrowser, der (mit lediglich standardisiertem Funktionsumfang) heute auf jedem PC verfügbar ist und eine Kompatibilität über Betriebssystem- und Plattformgrenzen hinweg aufweist, zum Teil einer Anwendung. Programmeile, die in einer der populären Skript-Programmiersprachen erstellt sind, sorgen server- oder clientseitig (oder auf beiden Seiten) für die Präsentation und Verarbeitung dynamischer Inhalte. Dadurch können Aufwand und Kosten für die Implementation verteilter Anwendungen gering gehalten werden, und die Nutzer finden eine vertraute Bedienoberfläche – die ihres Browsers – vor.

Insofern verwundert es nicht, dass solche Webanwendungen in steigendem Maße zum Ziel netzgestützter Angriffe werden; Symantec⁷ verzeichnet eine jährliche Steigerungsrate von 70 Prozent bei den Schwachstellen, die in Webanwendungen entdeckt und ausgenutzt werden. Dem Angreifer bietet sich dabei zudem die Möglichkeit, Sicherheitsvorkehrungen zu umgehen: Die Webserver, auf denen beispielsweise Skripte in der (besonders anfälligen) Sprache PHP ablaufen, liegen oft hinter Firewalls oder in einer so genannten demilitarisierten Zone; gelingt es, in den Server einzubrechen, ist bereits eine wichtige Hürde auf dem Weg ins interne Netz des Betreibers der Anwendung genommen. Die Antivirenexperten erwarten, dass diese Angriffsmethode in Zukunft noch weiter an Bedeutung gewinnt.

Weiterer Zukunftstrend: Datenklau

Auf dem Vormarsch sind des Weiteren Programme, die als „Adware“ und „Spyware“ klassifiziert werden und dadurch gekennzeichnet sind, dass sie die Nutzbarkeit des betroffenen Computers zwar nicht (wesentlich) einschränken, aber im Verborgenen unerwünscht

⁶ Vgl. Symantec Corporation (2005).

⁷ Vgl. Symantec Corporation (2005).

Jahrbuch der Heinrich-Heine-Universität Düsseldorf 2004

Herausgegeben vom Rektor
der Heinrich-Heine-Universität Düsseldorf
Univ.-Prof. Dr. Dr. Alfons Labisch

Konzeption und Redaktion:
em. Univ.-Prof. Dr. Hans Stüssmuth

desselben Angreifers, aber auch beispielsweise die Durchführung von Denial-of-Service-Attacken gegen Webserver im Internet oder die Verbreitung von Spam.

Aktuelle Studien⁴ gehen davon aus, dass täglich mehrere Tausend Computer im Internet mit Bot-Programmen neu infiziert und damit zu einem Werkzeug von Hackern werden, die als Einzelpersonen oder als organisierte Gruppen diese Systeme immer häufiger für kriminelle Zwecke einsetzen.

Die rasante Ausbreitung der Bots hängt offenbar auch mit der zunehmenden Verfügbarkeit breitbandiger Internetzugänge für Privatpersonen ab: Ein Computer mit gelegentlicher Einwahl per (langsamem) Analogmodem ins Internet ist für den Angreifer nur von geringem Nutzen, im Gegensatz zum PC am ADSL-Anschluss – oder zu einem Computer im universitären Netz, das eine noch einmal deutlich schnellere Anbindung ans Internet bietet.

Die Fernsteuerbarkeit „seiner“ Bot-Netze bietet dem Angreifer die Chance, kurzfristig auf neu entdeckte Schwachstellen in Computersystemen zu reagieren und den Schadcode zu ihrer Erkennung und Ausnutzung auf die von ihm gesteuerten Rechner zu übertragen, so dass er in kürzester Zeit seinem Netz neue Opfer hinzufügen kann. Umso geringer werden die Aussichten für gewissenhafte Computernutzer, durch frühzeitiges Einspielen von Korrekturen ihr System auf einem sicheren Stand zu halten; die wirksamsten Maßnahmen gegen Infektionen mit Bot-Software sind zurzeit der Schutz des PCs durch Firewalls mit restriktiven Einstellungen sowie ein vorsichtiger Umgang mit E-Mail-Anhängen und Downloads, in denen Schadcode verborgen sein kann, selbst wenn sie von vertrauenswürdiger Stelle zu kommen scheinen.

Ist auf einem PC erst einmal ein Bot eingerichtet, so wird es zunehmend schwerer, seine Kommunikation mit dem „Owner“ (dem Hacker, der ihn in seine Gewalt gebracht hat) zu unterbinden. Frühere Methoden, einen speziellen TCP/IP-Port zu öffnen, auf den man sich von außen verbinden kann, oder über das IRC⁵-Netzwerk Kontakt aufzunehmen, scheitern heute oft an Firewalls und Intrusion-Detection-Systemen, die diese Verbindungen verhindern beziehungsweise erkennen und melden. Daher werden zunehmend unverständliche Protokolle benutzt, wie z. B. Webzugang (HTTP) und Mailabruf (POP3), die weder blockiert werden noch besondere Aufmerksamkeit erregen.

Phishing: Jagd auf Arglose

Unter Phishing versteht man den Versuch, unberechtigt auf vertrauliche Informationen einer Einzelperson oder eines Unternehmens zuzugreifen, meist mit Hilfe von betrügerischen Webseiten oder E-Mails, die von einem realen Geschäftspartner zu kommen scheinen. Das Wort ist vermutlich in Anlehnung an „phreaking“ entstanden, eine Bezeichnung für die früheren Methoden der „phone freaks“, auf fremde Kosten zu telefonieren.

Erfolge versprechend sind diese Angriffe erst dadurch geworden, dass inzwischen für viele Internetnutzerinnen und -nutzer die Abwicklung von Geldgeschäften im Netz, sei es in der Form von Electronic Banking oder beim Kauf, Verkauf oder der Versteigerung von Waren, alltäglich geworden ist. Sie haben erfahren, wie problemlos und schnell diese Transaktionen abgewickelt werden können, und sie sind es gewohnt, dies über völlig unzureichend abgesicherte Kommunikationswege zu tun. Entsprechend bereitwillig ge-

© Heinrich-Heine-Universität Düsseldorf 2005
 Einbandgestaltung: Wiedemeier & Martin, Düsseldorf
 Titelbild: Schloss Mickeln, Tagungszentrum der Universität
 Redaktionsassistent: Georg Stütgen
 Beratung: Friedrich-K. Unterweg
 Satz: Friedhelm Sowa, L^AT_EX
 Herstellung: WAZ-Druck GmbH & Co. KG, Duisburg
 Gesetzt aus der Adobe Times
 ISBN 3-9808514-3-5

⁴ Vgl. Symantec Corporation (2005).

⁵ Internet Relay Chat.

Signatur keine *false positives* meldet, also keinen falschen Alarm bei harmlosen E-Mails und Dateien auslöst, und schließlich wird sie an die Nutzer übermittelt, die das Regelwerk ihres Virencanners (oft im Rahmen eines kostenpflichtigen Abonnements) in gewissen Zeitabständen aktualisieren. Damit vergehen zwischen der Freisetzung des Virus und seiner wirksamen Abwehr durch den Scanner zumindest mehrere Stunden, oft sogar ein paar Tage, während derer das Virus den Zielrechner ungeschützt vorfindet.

In einer US-amerikanischen Studie² zum Thema Computerkriminalität und -sicherheit wird für das Jahr 2004 festgestellt, dass zwar gezielte Attacken auf IT-Systeme etwa zum Zwecke des Datendiebstahls zurückgegangen sind, dass die Computerviren und Denial-of-Service-Angriffe jedoch eine anhaltende Bedrohung darstellen und den Befragten mit durchschnittlich mehr als 200.000 US\$ pro Jahr die höchsten Schäden verursachen; bei 78 Prozent der Unternehmen traten Virenprobleme auf.

Computerviren und -würmer benötigen zu ihrer Ausbreitung Schwachstellen in der Software. Wie die regelmäßig vom SANS-Institut veröffentlichten Hitlisten der „Top New Vulnerabilities“³ zeigen, werden diese nach wie vor am häufigsten in den verschiedenen Windows-Betriebssystemen entdeckt. Dies mag mit deren Marktdominanz zusammenhängen, die günstige Voraussetzungen für eine Ausbreitung des Schadcodes schafft. Doch kann dieser Aspekt nicht allein ausschlaggebend sein: Bei den Webservern konzentrieren sich die entdeckten Schwachstellen keineswegs auf das am häufigsten eingesetzte Produkt, den Open-Source-Webserver Apache. Vielmehr scheint die Tatsache eine wichtige Rolle zu spielen, dass Microsoft mit Rücksicht auf die Einfachheit der Benutzung und auf Software-Altlasten die Sicherheitsfunktionen der modernen Betriebssysteme (wie beispielsweise die konsequente Trennung von Nutzer- und Administratorberechtigungen) den Normalanwendern nicht nahe bringt. So sind die Windows-Viren und -würmer weiter auf dem Vormarsch: Ihre Anzahl stieg im 2. Halbjahr 2004 um 332 Prozent gegenüber dem Vorjahreszeitraum; in immer kürzeren Abständen setzen die Virenautoren neue Varianten in Umlauf, um die Wirkung von Virenschutzprogrammen zu unterlaufen.

Interessanterweise tauchen im Bericht des SANS Institute auch die Antivirenprodukte von vier namhaften Herstellern auf, die ihrerseits Programmierfehler (*buffer overflows*) enthielten und dringend korrigiert werden mussten, da sie sonst eine Gefahr für diejenigen Windows-PCs darstellten, die sie doch eigentlich vor Angriffen aus dem Netz schützen sollten.

Unter fremder Kontrolle: Bot-Netzwerke

Als „Bot“ wird ein Programm bezeichnet, das versteckt auf einem Computer installiert wird und seine Fernsteuerung ermöglicht. Es kann vom Angreifer gezielt nach einem Einbruch in das System eingerichtet oder durch andere infizierte Rechner automatisch (als „Wurm“) weiterverbreitet werden sein. Anders als die schon seit längerem bekannten Backdoor-Programme (die ebenfalls eine „Hintertür“ in das System öffnen) erlauben es die Bots, eine große Anzahl von Computern gleichzeitig unter Kontrolle zu halten und auf ihnen koordinierte Aktionen durchzuführen. Hierzu gehören die Suche nach weiteren anfälligen, unzureichend geschützten Systemen und deren Eingliederung ins Bot-Netzwerk

² Vgl. Gordon *et al.* (2004) CSI/FBI Computer Crime and Security Survey.

³ Vgl. The SANS Institute (2005).

Inhalt

Vorwort des Rektors	11
Gedenken	15
Rektorat	17
ALFONS LABISCH (Rektor)	
Autonomie der Universität –	
Ein Leitbild für die Heinrich-Heine-Universität Düsseldorf	19
VITTORIA BORSÒ	
Internationalisierung als Aufgabe der Universität	33
RAIMUND SCHIRMEISTER und LILJA MONIKA HIRSCH	
Wissenschaftliche Weiterbildung –	
Chance zur Kooperation mit der Wirtschaft?	51
Medizinische Fakultät	
<i>Dekanat</i>	65
<i>Neu berufene Professorinnen und Professoren</i>	67
WOLFGANG H.M. RAAB (Dekan)	
Die Medizinische Fakultät – Entwicklung der Lehre	77
THOMAS RUZICKA und CORNELIA HÖNER	
Das Biologisch-Medizinische Forschungszentrum	81
DIETER HÄUSSINGER	
Der Forschungsschwerpunkt Hepatologie	87
IRMGARD FÖRSTER, ERNST GLEICHMANN,	
CHARLOTTE ESSER und JEAN KRUTMANN	
Pathogenese und Prävention von umweltbedingten	
Erkrankungen des Immunsystems	101
MARKUS MÜSCHEN	
Illusionäre Botschaften in der	
malignen Entartung humaner B-Lymphozyten	115

Mathematisch-Naturwissenschaftliche Fakultät	
Dekanat.....	127
<i>Neu berufene Professorinnen und Professoren</i>	129
PETER WESTHOFF (Dekan) Die Mathematisch-Naturwissenschaftliche Fakultät – Was hat das Jahr 2004 gebracht?	141
DIETER WILLBOLD Die Rolle des Forschungszentrums Jülich für die Mathematisch-Naturwissenschaftliche und die Medizinische Fakultät der Heinrich-Heine-Universität Düsseldorf	147
DAGMAR BRUSS Verschränkt oder separabel? Moderne Methoden der Quanteninformationstheorie	155
STEPHANIE LÄER Arzneimitteltherapie bei Kindern – Eine Herausforderung besonderer Art für Forschung und Praxis	167
HILDEGARD HAMMER „Vor dem Abitur zur Universitär“ – Studium für Schülerinnen und Schüler an der Heinrich-Heine-Universität Düsseldorf	183
Philosophische Fakultät	
Dekanat.....	195
<i>Neu berufene Professorinnen und Professoren</i>	197
BERND WITTE (Dekan) Zur Lage von Forschung und Lehre an der Philosophischen Fakultät	203
WOLFGANG SCHWENTKER Geschichte schreiben mit Blick auf Max Weber: Wolfgang J. Mommsen	209
DETLEF BRANDES „Besinnungsloser Tummel und maßlose Einschüchterung“: Die Studentendutschen im Jahre 1938	221
ANDREA VON HÜLSEN-ESCH, HANS KÖRNER und JÜRGEN WIENER Kunstgeschichte an der Heinrich-Heine-Universität Düsseldorf – Innovationen und Kooperationen	241
GERHARD SCHURZ Der Mensch – Ein Vernunftwesen? Kognition und Rationalität aus evolutionstheoretischer Sicht	249

JAN VON KNOP und DETLEF LANNERT

Gefahren für die IT-Sicherheit und Maßnahmen zu ihrer Abwehr

Es ist eine für die Heinrich-Heine-Universität Düsseldorf strategische Aufgabe geworden, die Sicherheit und Funktionsfähigkeit des internen Datennetzes sowie der Anbindung an das Internet zu gewährleisten, der sich in besonderem Maße das Universitätsrechenzentrum (URZ) widmet und der es eine zentrale Rolle einräumt. Forschung, Lehre und Verwaltungstätigkeit sind in ihrer heutigen Form kaum noch vorstellbar ohne Nutzung von Datenkommunikation; umso negativer werden die Störungen empfunden, die aus dem Missbrauch von Netzen und netzbasierten Dienstleistungen resultieren. Insbesondere die durch „gehackte“ Arbeitsplatzrechner und die durch Viren- und Werbemails („Spam“) entstehenden Probleme sind vielen Universitätsangehörigen nur allzu vertraut.

Dieser Beitrag gibt einen Überblick über die Entwicklung der Gefährdungssituation und zeigt einige Ansätze auf, wie die zu erwartenden Probleme zu beherrschen sind.

Entwicklung der Gefährdungslage

Nach Erhebungen des Antivirenssoftware-Herstellers Symantec¹ wurden im 2. Halbjahr 2004 wiederum 1.403 neue sicherheitsrelevante Schwachstellen in Betriebssystemen und Anwendungssoftware entdeckt, von denen

- 97 Prozent als gefährlich eingestuft wurden,
- mehr als 70 Prozent „leicht“ für Angriffe auszunutzen waren und
- 80 Prozent über das Internet, also ohne regulären Zugang zum Zielsystem, genutzt werden konnten.

Gegenüber dem vorangegangenen Halbjahr stellt dies eine Steigerung um 13 Prozent dar. Nach wie vor werden die Angriffsmöglichkeiten sehr schnell ausgenutzt: Im Mittel vergehen nur 6,4 Tage zwischen dem Bekanntwerden einer Verwundbarkeit und der Veröffentlichung von so genanntem *exploit code*, also Programmen, die eine Ausnutzung der Schwachstelle ermöglichen.

Die Analyse von Schadenssoftware und die Bereitstellung neuer Signaturen für Virenscanner kann jedoch nicht wesentlich beschleunigt werden: Ein neu auftretendes Computervirus muss zunächst bei seiner Weiterverbreitung erkannt und „eingefangen“ werden, beispielsweise durch einen der von den Virenschützern zu diesem Zweck eigens im Internet eingerichteten „Honeylopf“-Computer. Dabei handelt es sich um scheinbar verwundbare Systeme, die jedes Virus, das sie anzugreifen versucht, an eine Auswertestelle weiterleiten. Bevor die Virenscanner das neue Virus erkennen und abblocken können, muss erst seine Funktionsweise analysiert und eine Signatur erarbeitet werden, anhand derer das Virus möglichst sicher erkannt werden kann. Anschließend ist zu überprüfen, dass die neue

¹ Vgl. Symantec Corporation (2005).

RALPH WEISS	
Medien – Im blinden Fleck öffentlicher Beobachtung und Kritik?	265
REINHOLD GÖRLING	
Medienkulturwissenschaft – Zur Aktualität eines interdisziplinären Faches	279
BERND WITTE	
Deutsch-jüdische Literatur und literarische Moderne. Prolegomena zu einer deutsch-jüdischen Literaturgeschichte	293
Gastbeitrag	
WOLFGANG FRÜHWALD	
Das Geschenk, „nichts erklären zu müssen“: Zur Neugründung eines Instituts für Jüdische Studien	307
Wirtschaftswissenschaftliche Fakultät	
<i>Dekanat</i>	321
<i>Neu berufene Professorinnen und Professoren</i>	323
HEINZ-DIETER SMEETS und H. JÖRG THIEME (Dekan)	
Der Stabilitäts- und Wachstumspakt – Lästiges Übel oder notwendige Schranke?	325
GUIDO FÖRSTER	
Verlustverrechnung im Beteiligungskonzern	341
ALBRECHT F. MICHLE	
Die Effizienz der Fiskalpolitik in den Industrieländern	363
GERD RAINER WAGNER, RÜDIGER HAHN und THOMAS NOWAK	
Das „Montréal-Projekt“ – Wirtschaftswissenschaftliche Kompetenz im internationalen Studienwettbewerb	381
Juristische Fakultät	
<i>Dekanat</i>	393
<i>Neu berufene Professorinnen und Professoren</i>	395
HORST SCHLEHOFER (Dekan)	
Zehn Jahre Juristische Fakultät – Rückblick und Ausblick	397
ULRICH NOACK	
Publizität von Unternehmensdaten durch neue Medien	405
DIRK LOOSCHELDERS	
Grenzüberschreitende Kindesentführungen im Spannungsfeld von Völkerrecht, Europäischem Gemeinschaftsrecht und nationalem Verfassungsrecht	423

RALPH ALEXANDER LORZ Die unmittelbare Anwendbarkeit des Kindeswohlvortrags nach Art. 3 Abs. 1 der UN-Kinderrechtskonvention im nationalen Recht	437
Gesellschaft von Freunden und Förderern der Heinrich-Heine-Universität Düsseldorf e.V.	
OTHMAR KALTHOFF Jahresbericht 2004	459
Forscherguppen der Heinrich-Heine-Universität Düsseldorf	
SEBASTIAN LÖBNER Funktionalbegriffe und Frames – Interdisziplinäre Grundlagenforschung zu Sprache, Kognition und Wissenschaft	463
HANS WERNER MÜLLER, FRANK BOSSE, PATRICK KÜRY, KERSTIN HASENPUSCH-THEIL, NICOLE KLAPKA UND SUSANNE GRESCHAT Die Forschergruppe „Molekulare Neurobiologie“	479
ALFONS SCHNITZLER, LARS TIMMERMANN, BETTINA POLLOK, MARKUS PLONER, MARKUS BUTZ und JOACHIM GROSS Oszillatorische Kommunikation im menschlichen Gehirn	495
MARKUS UHRBERG Natürliche Killerzellen und die Regulation der KIR-Rezeptoren	509
Institute an der Heinrich-Heine-Universität Düsseldorf – Das Deutsche Diabetes-Zentrum	
GUIDO GIANI, DIRK MÜLLER-WIELAND und WERNER A. SCHERBAUM Das Deutsche Diabetes-Zentrum – Forschung und Klinik unter einem Dach	521
WERNER A. SCHERBAUM, CHRISTIAN HERDER und STEPHAN MARTIN Interaktion von Inflammation, Lifestyle und Diabetes: Forschung an der Deutschen Diabetes-Klinik	525
DIRK MÜLLER-WIELAND und JÖRG KOTZKA Typ-2-Diabetes und Metabolisches Syndrom als Folgen einer „entgleisten“ Genregulation: Forschung am Institut für Klinische Biochemie und Pathobiochemie	533
GUIDO GIANI, HELMUT FINNER, WOLFGANG RATHMANN und JOACHIM ROSENBAUER Epidemiologie und Public Health des Diabetes mellitus in Deutschland: Forschung am Institut für Biometrie und Epidemiologie des Deutschen Diabetes-Zentrums	537

Universitätsverwaltung	
JAN GERKEN und HERMANN THOLE Moderne Universitätsplanung	547
Zentrale Einrichtungen der Heinrich-Heine-Universität Düsseldorf	
JAN VON KNOP und DETLEF LANNERT Gefahren für die IT-Sicherheit und Maßnahmen zu ihrer Abwehr	567
MICHAEL WETTERN und JAN VON KNOP Datenschutz im Hochschulbereich	575
IRMGARD SIEBERT und KLAUS PEERENBOOM Ein Projekt zur Optimierung der Selbstausleihe. Zur Kooperation der Universitäts- und Landesbibliothek Düsseldorf mit der 3M Deutschland GmbH	591
SILVIA BOOGHS, MARCUS VAILLANT und MAX PLASSMANN Neue Postkartenserie der Universitäts- und Landesbibliothek Düsseldorf . . .	601
Geschichte der Heinrich-Heine-Universität Düsseldorf	
MAX PLASSMANN Autonomie und ministerielle Steuerung beim Aufbau der neuen Fakultäten der Universität Düsseldorf nach 1965	629
Chronik der Heinrich-Heine-Universität Düsseldorf	
ROLF WILHARDT Jahreschronik 2004.	643
Autorinnen und Autoren	657