inforum

Zentrum für Informationsverarbeitung der Universität Münster
Jahrgang 29, Nr. 1 – April 2005 ISSN 0931-4008

Inhalt

Impressum

infoWWU
ISSN 0931-4008

Westfälische Wilhelms-Universität
Zentrum für Informationsverarbeitung (Universitätsrechenzentrum)
Röntgenstr. 9–13
48149 Münster

E-Mail:	ziv@uni-muenster.de
WWW:	http://www.uni-muenster.de/ZIV/
Redaktion:	E. Sturm (✆ 83-31679, ✉ sturm@uni-muenster.de)
Satz:	K. Hovestadt
Satzssystem:	StarOffice 7
Druck:	Drucktechnische Zentralstelle (Rank Xerox DocuTech 135)

Auflage dieser Ausgabe: 1400

Editorial

E. Sturm

Eine **infoWWU**-Ausgabe steht meistens unter zwei Themen, dem Thema „Sicherheit der Informationsverarbeitung“ und einem weiteren aktuellen. Dieses Mal beschäftigen sich so viele Artikel mit der Sicherheit, dass wir diesen der Übersicht halber ein eigenes Kapitel gewidmet haben: Sie finden „ZIV-Sicherheit“ hinter dem „Botanischen Garten“.

Als zweites aktuelles Thema sehe ich diesmal das Thema „Video-Konferenz“. Nachdem wir in der letzten Ausgabe das Videokonferenzsystem des DFN-Vereins vorgestellt haben, beleuchten wir in diesem **infoWWU** zwei andere Systeme näher, die an unserer Universität benutzt werden können. Diese beiden stehen nicht etwa in Konkurrenz zueinander, sondern ergänzen sich – in Qualität und Preis. Auf diese Weise können wir, was den DFN-Verein betrifft, noch abwarten.

ZIVconf ist ein einfaches System, das ohne Zukauf von Software vom Arbeitsplatz aus genutzt werden kann. Die Bildchen sind klein (siehe mein Fahndungsfoto links) und je mehr Teilnehmer dazustoßen, desto schlechter wird die Qualität. Dafür benötigt man aber keine Einweisung, sondern kann sofort „loslegen“, wenn man nur eine Videokamera und ein Headset (Kopfhörer und Mikrofon) besitzt – einen Browser mit Flash-Plugin haben wohl die meisten auf ihrem PC installiert. Außerdem war das System in der Anschaffung konkurrenzlos billig.

Das andere System benutzt (wie der DFN-Verein) eine Multipoint-Control-Unit (MCU), und man braucht entweder spezielle Software auf dem eigenen PC oder man reserviert den Videokonferenzraum in der Telefonzentrale. Die Qualität ist deutlich besser, vor allem, wenn man ISDN-Leitungen benutzt.

Wenn Sie also in „Videoconferencing“ einsteigen wollen, wäre mein Vorschlag: Testen Sie zunächst Ihre Ausrüstung mit ZIVconf. Wenn Ihnen dann die Qualität nicht ausreicht, lassen Sie sich von ZIV und Dezernat 4 beraten, wie Sie sich verbessern können.

Außerdem sei noch ein anderes Thema hervorgehoben, da drei „Männer der ersten Stunde“ ausgeschieden sind, unsere Kollegen Hans-Werner Kisker, Bernfried Neukäter und Dr. Siegfried Zörkendörfer. Vor allem langjährige „Kunden“ werden sich den Blick zurück nicht entgehen lassen.

ZIV-Aktuell

ZIVconf – Videokonferenz am eigenen PC

E. Sturm

Mit ZIVconf stellt das ZIV ein Videokonferenzsystem zur Verfügung, das an Nutzerfreundlichkeit nicht zu übertreffen ist.

Da wir am Videokonferenzsystem des DFN-Vereins (siehe letztes infoWWU) aus Kostengründen noch nicht teilnehmen wollen, sei hier eine Alternative vorgestellt, die zwar die übliche Hardware (Videokamera und Headset), aber keine weitere Software benötigt.

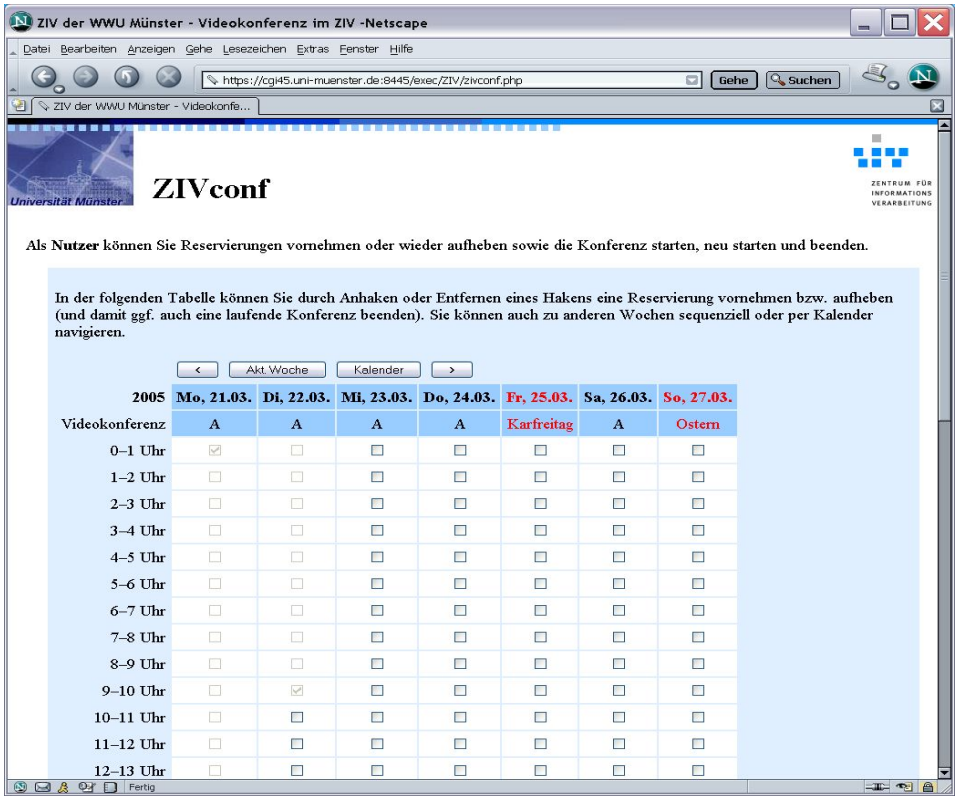
Die zentrale Rolle bei ZIVconf spielt der so genannte FlashComm-Server. Er verteilt die Audio- und Video-Ströme zwischen den einzelnen Teilnehmern. Für 2er-Konferenzen lohnt sich der Aufwand übrigens nicht, da kann man gleich NetMeeting nehmen und braucht nicht einen Server zu belästigen.

Hard-und Software

Im Prinzip sollten jede handelsübliche USB-Kamera und jeder handelsübliche Headset, bestehend aus Kopfhörer und Mikrofon, für ZIVconf geeignet sein. Wenn diese von Ihrem Betriebssystem akzeptiert werden, sollte auch die Videokonferenz laufen. „Keine weitere Software“ ist nicht ganz richtig. Ihr Browser benötigt zur Darstellung der Videokonferenz das so genannte Flash-Plugin. Dieses ist aber bei 90 % aller Browser vorinstalliert, habe ich mir sagen lassen. Anderenfalls bekommt man es bei http://www.macromedia.com/go/getflashplayer. Nach der Installation „merkt“ der Browser, wenn Daten kommen, die das Plugin zu verarbeiten hat.

Die Reservierung

Die Hauptrolle einer ZIVconf-Videokonferenz spielt der Konferenzleiter. Er muss Mitglied der Universität sein (z. B. Professor, Student, Angestellter, Emeritus, aber nicht Gasthörer oder Alumnus, jeweils m/w). Der Konferenzleiter reserviert mit dem über unsere Service-Webseite zu erreichenden Webinterface ZIVconf eine oder mehrere Stunden. Im Augenblick ist die Anzahl auf zwei beschränkt – zusammenhängend oder nicht.



Am Anfang wird wie bei allen Webinterfaces des ZIV die Nutzerkennung und das Passwort abgefragt. Dies sind im Normalfall die Angaben der E-Mail-Adresse (allerdings nicht der vielleicht vereinbarte Aliasname). Dann erscheint nebenstehende Abbildung, die die aktuelle Woche zeigt.

2005	Mo, 21.03.	Di, 22.03.	Mi, 23.03.	Do, 24.03.	Fr, 25.03.	Sa, 26.03.	So, 27.03.
Videokonferenz	A	A	A	A	Karfreitag	A	Ostern
0–1 Uhr	☑	☐	☐	☐	☐	☐	☐
1–2 Uhr	☐	☐	☐	☐	☐	☐	☐
2–3 Uhr	☐	☐	☐	☐	☐	☐	☐
3–4 Uhr	☐	☐	☐	☐	☐	☐	☐
4–5 Uhr	☐	☐	☐	☐	☐	☐	☐
5–6 Uhr	☐	☐	☐	☐	☐	☐	☐
6–7 Uhr	☐	☐	☐	☐	☐	☐	☐
7–8 Uhr	☐	☐	☐	☐	☐	☐	☐
8–9 Uhr	☐	☐	☐	☐	☐	☐	☐
9–10 Uhr	☐	☑	☐	☐	☐	☐	☐
10–11 Uhr	☐	☐	☐	☐	☐	☐	☐
11–12 Uhr	☐	☐	☐	☐	☐	☐	☐
12–13 Uhr	☐	☐	☐	☐	☐	☐	☐

Liegt der gewünschte Termin in einer anderen Woche, so kann man entweder „blättern“ oder über eine Kalenderanzeige den direkten Weg nehmen. Man kann entsprechende Häkchen machen oder auch zurücknehmen und dann auf den Knopf „Übernehmen“ klicken.

Das Programm „übernimmt“ dabei nur die Reservierungen der angezeigten Woche, durch Blättern werden keine Reservierungen geändert!

Nach einer Übernahme zeigt das Programm die Webadresse an, unter der man sich später bei der Videokonferenz anmelden kann. Diese Adresse wird auch per E-Mail an die Adresse des Angemeldeten versandt. Sollte die E-Mail versehentlich gelöscht worden sein: Immer wenn man auf den „Übernehmen“-Knopf klickt, bekommt man eine E-Mail mit den aktuellen Reservierungen zugeschickt – sofern noch welche übrig geblieben sind.

Die Konferenz

Wer darf nun an der reservierten Videokonferenz teilnehmen? Die Antwort ist einfach: jeder, der die eben angesprochene Webadresse kennt. Sie ist hinreichend kryptisch und sieht etwa so aus:

https://www.uni-muenster.de/ZIV/zivconf/a5851c0810416bc67afd94e96bb98a8f.html

Es empfiehlt sich also, die von ZIVconf erhaltene Mail an alle gewünschten Teilnehmer weiterzuleiten. Entscheidend ist der Konferenzleiter, der, wenn die Konferenzzeit begonnen hat, wiederum mit dem Webinterface ZIVconv die Konferenz starten muss. Zu diesem Zweck zeigt der Browser nach Beginn der reservierten Zeit zusätzlich den folgenden Absatz auf der Webseite.

Konferenz

Sie können zur Zeit folgende Konferenz starten:

Videokonferenz A: 2005-03-22 09:00:00 bis 2005-03-22 11:00:00 mit der URL https://www.uni-muenster.de/ZIV/zivconf/a8bec43e2c85a949934d65d7f1d80fbc.html

Zum Starten klicken Sie bitte auf den folgenden Knopf. Dadurch wird dieses Webinterface beendet, die Konferenz gestartet und sofort in diesem Browserfenster angezeigt.

Start

Hinweise:

- Die Konferenz wird nach Ablauf der von Ihnen gebuchten Zeit automatisch gestoppt, falls Sie sie nicht verlängert haben.
- Wenn Sie die Reservierung der laufenden Konferenz streichen, wird die Konferenz innerhalb einer Minute beendet.

Der Konferenzleiter braucht jetzt nur noch auf den „Start“-Knopf zu klicken, das Webinterface beendet sich und zeigt dann im selben Fenster die Konferenzseite (siehe Abb. nächste Seite). In der Mitte sieht man die Frage des Plugins, ob man den Zugriff auf Kamera und Mikrofon erlaube. Tut man das nicht, so kann man später nur am Chat teilnehmen.

Nach dieser Erlaubnis gebe man im oben stehenden Eingabefeld einen Fantasienamen ein und klicke auf das „Login“-Feld. Der Name braucht nur unter den Teilnehmern der Konferenz aussagekräftig zu sein. Er erscheint auch rechts oben im Fenster in der Anwesendenliste (s. Abb. nächste Seite).

Wenn nach und nach alle Teilnehmer eintrudeln, muss man ihre Bildchen auf der Browserfläche verteilen. Zunächst erscheinen nämlich alle in der linken oberen Ecke, ggf. auch übereinander. Das (absichtlich verschwommene) Hintergrundbild hat das Format 1024 x 768, damit genügend Teilnehmer untergebracht werden können. Ist die Konferenz beendet, sollten Sie die Reservierung zurücknehmen – vielleicht kann ein anderer noch den Rest der Stunde ausnutzen.

Einstellungen

Normalerweise braucht man keine weiteren Einstellungen zu tätigen. Voreingestellt ist neben dem Loginfeld in einer Klappliste „DSL“. Hier könnte man auch „Modem“, „LAN“ oder „Custom“ wählen. Je nachdem, wie viel Teilnehmer es gibt, kann man hier die Qualität herauf- oder herabsetzen, „DSL“ scheint ein guter Kompromiss zu sein.

Lässt man den Mauszeiger über dem eigenen Bild schweben, so sieht man drei Schaltmöglichkeiten:

- Beenden der Teilnahme,
- Einfrieren des eigenen Bildes,
- Abschalten des eigenen Mikrofons („Räuspertaste“).

Schwebt der Mauszeiger über dem Bild eines anderen Teilnehmers, so gibt es zwei Schalter:

- Einfrieren des Bildes,
- Abschalten des Tons, wobei dies für jeden Teilnehmer getrennt einstellbar ist.

Weitere Einstellungen sind möglich im Kontextmenü der gesamten Fensterfläche, natürlich unter dem Punkt „Einstellungen“. Hier gibt es vier Tabulatorzungen:

- Zugriffsschutz,
- Lokaler Speicher,
- Mikrofon („Echo reduzieren“ anhaken!),
- Kamera.

Die letzten beiden Punkte kann man auch mit Windows-Mitteln verstellen: „Start → Systemsteuerung → Sounds und Audiogeräte → Audio“ für das Mikrofon, für die Kamera ggf. unter „Scanner und Kameras“, falls Sie nicht spezielle Hardware besitzen.

Der Chat

Wenn die Verbindung zum FlashComm-Server geklappt hat, erscheint unten eine Eingabezeile. Hier können Sie Text eintippen und den anderen Konferenzteilnehmern kundtun – und natürlich deren Antworten lesen.

Diese Zeile ist an sich nur sinnvoll, wenn man den anderen etwas mitteilen möchte, was zu kurz für eine E-Mail und zu lang zum Diktieren ist, etwa eine interessante Webadresse. Man kann in der Chat-Auflistung etwas mit der Maus überstreichen und per Kontextmenü in die Zwischenablage übernehmen.

Unangenehmer ist der Fall, dass jemand schreibt: „Ich höre nichts!“ Dann ist der FlashComm-Server womöglich am Ende der Bandbreite angelangt und lässt den ersten Audio-Strom weg – leider ohne Fehlermeldung an den Nutzer. Vielleicht ist aber auch nur das Mikrofon falsch angeschlossen.

Hintergründiges

Wie erwähnt kann jeder an der Konferenz teilnehmen, der die kryptische Webadresse kennt. Diese Webadresse ist nur zugänglich während der reservierten Zeit. In ihr ist die Anfangszeit der Konferenz (und die Nutzerkennung) verschlüsselt (per MD5, wem das etwas sagt).

Das bedeutet, dass, wenn Sie sich kurz vor Ende der Konferenz überlegen, die Konferenz zu verlängern, dies ohne Problem möglich ist (sofern nicht jemand anders sich die nächste Stunde reserviert hat). Wenn Sie allerdings den Anfang der Konferenz vorverlegen, müssen Sie eine neue Webadresse an die Teilnehmer verschicken.

Es lohnt sich übrigens nicht – dies ist an die Hacker gerichtet – sich die HTML-Datei (oder andere) auf den heimischen PC zu laden – von dort werden keine Anmeldungen akzeptiert!

Bleibt noch das Problem der Bandbreite. Wir besitzen eine Lizenz für 10 Mbit/s. Man kann sich also aussuchen, ob man wenige Teilnehmer mit hoher oder viele Teilnehmer mit niedriger Qualität bedienen will. Natürlich kann man auch jedes Mal das eigene Mikrofon erst dann einschalten, wenn man spricht. Das senkt sowohl den Geräuschpegel, also auch die benötigte Bandbreite!

Solche Tricks können eine an sich überfüllte Konferenz noch lauffähig halten. Sollten Sie also beobachten, dass die letzten Teilnehmer keinen Audiostrom mehr erhalten oder dass überhaupt keine Anmeldung mehr akzeptiert wird, so teilen Sie uns das bitte mit – vielleicht lohnt es sich, etwas Bandbreite hinzuzukaufen.

Wir haben die Beobachtung gemacht, dass das Gelingen der Konferenz in hohem Maße von den Endgeräten abhängt. Ein unbelastetes Notebook mit 600 MHz CPU kann da besser sein als ein Pentium 4 mit vielen laufenden Anwendungen, der sich lieber mit anderen Dingen „beschäftigt“ und dann Audioströme „weglässt“.

Ausbau der Videokonferenz-Infrastruktur im Netz der Universität Münster

L. Elkemann, G. Richter

Die Universität besitzt auch ein Videokonferenzsystem mit höherer Qualität und mehr Möglichkeiten.

Videokonferenzen wurden bereits in der Vergangenheit an der Universität, im Allgemeinen als Punkt-zu-Punkt-Kommunikation, betrieben. Zumeist waren das Konferenzen, die mittels Netmeeting, einer Software, die den Windows-Betriebssystemen beiliegt, realisiert wurden. Mehrpunktkonferenzen, Konferenzen an denen mehrere Teilnehmer teilnehmen können, waren ohne den Einsatz einer MCU, Multipoint-Control-Unit nicht möglich. Mit dem Einbau einer MCU vom Typ MGC 50 des Hersteller Polycom in das Kommunikationsnetz der Uni ist diese Möglichkeit nun gegeben.

Am Standort Orléansring 16 befindet sich ein voll ausgestatteter Videokonferenzraum, der es erlaubt Videokonferenzen mittels einer Videokonferenzanlage von Tandberg des Typs T800 sowohl über das LAN und Internet als auch über ISDN, auch im gemischten Betrieb, durchzuführen. Diverse Zuspielerquellen, wie PC, DVD, Video, usw. werden unterstützt. Beamerprojektion auf eine Leinwand und der zusätzlich mögliche Einsatz eines elektronischen Whiteboards runden das Portfolio ab. Die vorhandene Technik wurde bereits für umfangreiche Konferenzen mit Einrichtungen in Brasilien, USA, China, den GUS-Staaten, Skandinavien und natürlich Deutschland erfolgreich genutzt.

ISDN-Verbindungen, die für eine Videokonferenz genutzt werden können, sind leitungsorientiert. Das heißt, dass die gesamte Bandbreite der insgesamt aufgebauten ISDN-B-Kanäle, also n x 64 kbit/s (n = 1 bis max. 6), für die Videokonferenz zur Verfügung steht. Grundlage hier ist das Protokoll H.320 der ITU-Standardisierung. Gute Bild- und Tonverbindungen werden bereits mit Bandbreiten von 256 Kbit/sec, welches vier so genannten B-Kanälen entspricht, erzielt. Durch die mittlerweile reduzierten Verbindungsentgelte ist diese Art der Videokonferenz nach wie vor sehr attraktiv.

Parallel dazu wird die Möglichkeit der LAN-Konnektivität von den bereits installierten Videokonferenzsystemen Tandberg T800 im Fürstenberghaus und am Orleansring 16 unterstützt. Grundlage hier ist zur Zeit der Standard H.323 der ITU. Aufgrund des am Hochschulstandort Münster in großen Bereichen sehr gut ausgebauten Rechnernetzes sind Videokonferenzen innerhalb des Netzes bereits heute, was den Grad der Verbindungsstabilität und -qualität angeht, gut durchzuführen. Allerdings kann man Videokonferenzen nicht vorbehaltlos in Datennetze einführen, da Datennetze in aller Regel nicht leitungsorientiert, sondern paketorientiert arbeiten; damit ist zunächst keine Reservierung von Ressourcen verbunden, was in der Vergangenheit bekanntermaßen manchmal zu unliebsamen Überraschungen beim Videokonferenzbetrieb führte. Mit der Einführung neuer Router- und Sicherheitstechnologie, wie in einem separatem Artikel in diesem infoWWU beschrieben, wird es aber in Kürze noch besser möglich sein, Verkehrsflüsse und Kommunikationsbeziehungen, gerade hinsichtlich der H.32x-Protokolle, zu differenzieren und zu priorisieren und Videokonferenzanlagen und -teilnehmer zu schützen. Insbesondere die Stateful-Packet-Screening-Funktionen können die dynamische Verwendung von so genannten Ports in den Protokollen geeignet kontrollieren. Priorisierung ist aber auch in den schon vorhandenen Backbone-Komponenten, zum Teil auch in den peripheren Netzkomponenten möglich. Die Aktivierung solcher Funktionen dort benötigt aber wegen des Umfangs der operativen und administrativen Maßnahmen noch etliche Arbeitsschritte, so dass die garantierte Nutzbarkeit des LANs für Videokonferenzen zunächst nur in ausgewiesenen Bereichen voll gewährleistet werden kann. Trotzdem kann man davon ausgehen, dass die bereits eingeleiteten Maßnahmen insgesamt zu einem relativ hohen Maß an Sicherheit und Verfügbarkeit für Videokonferenzanwendungen führen werden.

Im zweiten Quartal dieses Jahres wird die zentrale Multipoint-Control-Unit MGC 50 des Hersteller Polycom, welche im Wesentlichen als Sternverteiler für Mehrfachkonferenzen arbeitet und sich am Standort Orléansring 16 befindet, das Protokoll SIP, Session Initiation Protocol, unterstützen, sodass ein weiterer flexiblerer Grad der Nutzung erreicht wird. SIP ist ein Standard-Protokoll aus der Familie der TCP/IP-Protokolle, das sich immer mehr im Bereich von Videokonferenzen und Telefonie (VoIP, Voice over IP) im Internet durchsetzt.

Die angesprochene Priorisierung von Datenströmen im Netz der Universität lässt sich in externen Netzen, insbesondere dem Internet, nur selten anwenden. Meistens reicht aber schon eine hohe Übertragungsbandbreite auf der gesamten Übertragungsstrecke, so dass das Internet zunächst die erste Wahl darstellt. Ist aber eine durchgängige Übertragungsqualität über das Internet für die Videokonferenzdatenströme zu bestimmten Standorten, wie Brasilien oder China, nicht möglich, ist eine ISDN-Verbindung nach wie vor nicht wegzudenken. Mit dem System an der Universität lässt sich aber ohne Weiteres realisieren, dass im lokalen Netz für die lokalen Teilnehmer das LAN verwendet wird, während die Verbindung nach außen nicht über das Internet, sondern über ISDN geschaltet wird.

Sofern Sie mit einem PC eine Videokonferenz initiieren möchten, ist eine Client-Software erforderlich. Diese Software muss das Protokoll H.323, sofern ein vorhandener LAN-Anschluss genutzt werden soll, bzw. das Protokoll H.320, wenn ein vorhandener ISDN-Anschluss verwendet werden soll, unterstützen. Ab dem zweiten Quartal dieses Jahres kann auch Clientsoftware, welche das Protokoll SIP nutzt, von dem zentralen System unterstützt werden. Clientsoftware ist im Internet als Freeware oder Shareware herunterzuladen. Bei einigen Betriebssystemen ist bereits eine Clientsoftware enthalten, wie z. B. Netmeeting. Sofern Sie jedoch für ihren Desktop oder ihr Notebook Videokonferenzsoftware benötigen, welches an Komfort und Funktionalität über die vorab ge-

nannte Software hinaus geht, sollten Sie Kontakt mit dem ZIV oder der Kommunikations- und Medientechnik des Dezernats 4 aufnehmen.

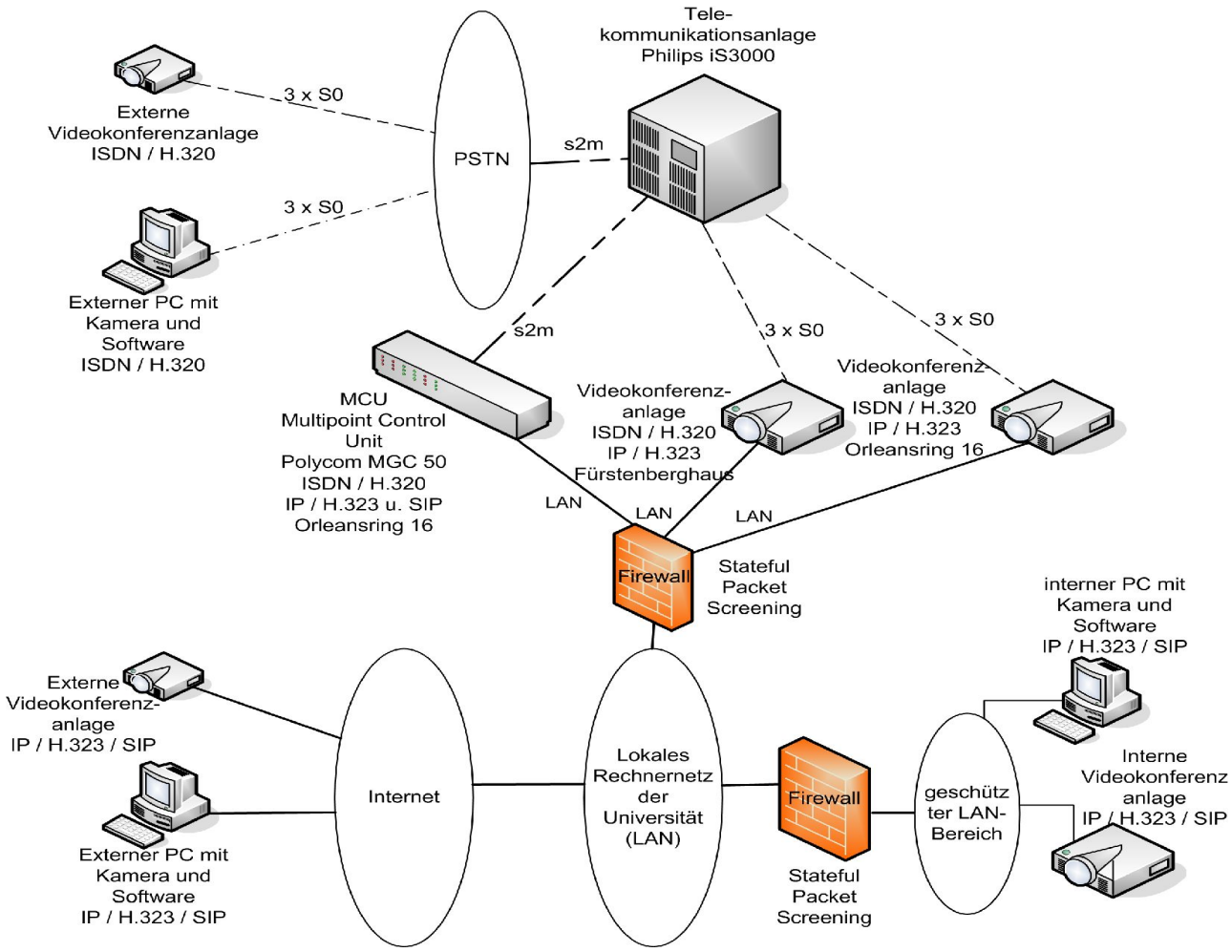
Die MCU MGC 50 des Hersteller Polycom unterstützt aber auch diverse hardwarebasierende Videokonferenzsysteme mit integrierter Kamera, wenn die vorgenannten Protokolle verwendet werden.

Für Videokonferenzen mit einer größeren Zahl von Teilnehmern innerhalb der Universität wird es sich häufig empfehlen, den eingangs erwähnten zentralen Konferenzraum zu buchen, auch bei der Vorbereitung und Durchführung von Videokonferenzen mit an der Universität verteilten Teilnehmerplätzen kann Hilfestellung angeraten sein.

Bezüglich der Beschaffung von hardwarebasierenden Videokonferenzsystemen für Einrichtungen der Universität und deren Einbindung in das Kommunikationsnetz der Universität, weil sich z. B. ein kontinuierlicher Bedarf abzeichnet, kann die Kommunikations- und Medientechnik des Dezernats 4 Hilfestellung leisten.

Sofern Sie den zentralen Konferenzraum benötigen, nehmen Sie bitte Kontakt mit der Hotline der Kommunikations- und Medientechnik des Dezernats 4 auf. Erreichbar ist diese Hotline werktags in der Zeit von 7.00 – 16.00 Uhr unter der Rufnummer 83-31111 oder unter `www.km@uni-muenster.de`. Sofern Sie andere Fragen haben, wenden Sie sich bitte ebenfalls an das Dez. 4.43, Kommunikations- und Medientechnik. Neben dieser Möglichkeit des Supports werden Ihnen zukünftig Selfcare-Mechanismen zur Verfügung gestellt werden.

Die folgende Abbildung zeigt noch einmal die Konfiguration der Universität.



Die Freiheit das Nützliche zu tun

W. Bosse

Wer sieht es nicht als Ideal an, sich beruflich den Dingen widmen zu können, die man sich erwählt – einmal abgesehen von Notwendigkeiten, die aber akzeptiert werden können? Wer es versteht im Zuge der rasanten Entwicklung der Informationsverarbeitung die neuen Herausforderungen frühzeitig anzunehmen, ist stets bestens motiviert.

Da das Rechenzentrum (wie das Zentrum für Informationsverarbeitung damals hieß) es sich von Anfang an zur Aufgabe gemacht hatte, einen breiten Nutzerkreis in der Universität zu unterstützen, konnte unser Kollege Hans-Werner Kisker schon früh einige „spannende" Anwendungen bearbeiten. Während numerische Anwendungen in den Naturwissenschaften eher zum Tagesgeschäft gehörten, war z. B. in den Geisteswissenschaften Pionierarbeit zu leisten. Seine Mitarbeit im Rahmen des DFG-Forschungsauftrags „Ugaritisches Handwörterbuch" begann im Sommer 1967, also bereits während seiner Studienzeit, und bestand in der Entwicklung eines Programmsystems zur Erstellung einer Bibliographie, wobei das Editieren ugaritischer Texte mit ihren besonderen Schriftzeichen eine Herausforderung darstellte.

Diesem Tätigkeitsfeld, das damals unter die schlichte Sammelbezeichnung „Nichtnumerische Datenverarbeitung" fiel, blieb er mit der Ende 1971 erfolgten Einstellung als Diplom-Mathematiker im Rechenzentrum zunächst treu. Ergänzend war er nun auch an Aufgaben des SFB 7 „Mittelalterforschung" beteiligt, die das automatische Auffinden von Personengruppen betrafen, und unterstützte Projekte des SFB 164 „Vergleichende geschichtliche Städteforschung". Aufgrund seiner praktischen Erfahrungen mit der Verwaltung diverser Datenbestände entschloss er sich, ein allgemeines Programmsystem zur laufenden Bearbeitung von Daten zu entwickeln. Diese Software kam unter der Bezeichnung DMP („Datenverwaltungsprogramm") in mehreren Fachbibliotheken der Universität und natürlich auch im Rechenzentrum zum Einsatz.

Ausgehend von Arbeiten zum Prozessrechnereinsatz in der Chirurgischen Klinik erweiterte er dann auf dem Gebiet der *Real-Time*-Anwendungen seine Kenntnisse. Er betreute den Einsatz des 1980 vom Rechenzentrum beschafften Prozessrechners und gab erste Einführungen in dessen Unix-Betriebssystem. Unter dem Namen STAU entwickelte er sogar ein spezielles „Studenten-Ausbildungssystem", um den Prozessrechner für Programmierkurse flexibel nutzen zu können.

Die Anfang der 80er Jahre beginnende Verbreitung von Mikrorechnern (Personal Computer, PC) und ihrer lokalen Vernetzung brachte weitere neue Herausforderungen, die besonders den System- und Hardware-Bereich betrafen. Durch ein Studium der Informatik, das Hans-Werner Kisker ergänzend und „ganz nebenbei" an der Fernuniversität Hagen absolviert hatte, verfügte er über einen Fundus an systematischem Fachwissen und konnte mit umfangreicher Sachkenntnis und Erfahrung in dieser Zeit viele tragfähige Ideen zur Positionierung des Rechenzentrums beisteuern. Vor allem waren wegweisende Entscheidungen zum Aufbau des Rechnernetzes in der Universität vorzubereiten und Konzepte für die PC-Auswahl, -Beschaffung und -Unterstützung zu entwickeln. Die Realisierung nahm besonders mit dem vom Bund 1984 initiierten Förderprogramm CIP (Computer-Investitionsprogramm) für den Bereich studentischer Rechnerarbeitsplätze „Fahrt" auf und wurde danach auch auf die Wissenschaftler-Arbeitsplätze ausgeweitet (WAP).

Unter Berücksichtigung dieser wichtigen neuen Entwicklungen entstand im Rechenzentrum die neue Abteilung *Rechnernetze, Mikrorechner und Prozessdatenverarbeitung*, deren Leitung ihm 1985 übertragen wurde. Fortan bestanden seine wichtigen Tätigkeitsfelder einerseits in allen Belangen der PC-Hardware und -Software, was auch Vorkehrungen zur Wartung und Reparatur einschloss. Andererseits waren im Bereich der Rechnernetze ebenso Auswahl und Beschaffung der Netzkomponenten sowie Ausbau, Betrieb und Weiterentwicklung des Netzes vorzunehmen, wobei keine „lokalen Netzinseln" entstehen durften, sondern leistungsfähige Verbindungen zwischen den Standorten und nicht zuletzt zum Rechenzentrum vorzusehen waren.

Als die dramatische Ausweitung dieser Aufgabenfelder zwangsläufig zur Einrichtung einer eigenen Rechnernetz-Abteilung führte, übernahm er die Abteilungsleitung für den Arbeitsbereich *PC-Systeme*. Diese Entscheidung war nicht allein darin begründet, dass er ein hervorragender Kenner dieser Rechnerwelt war, sondern sie eröffnete ihm gleichzeitig auch wieder Möglichkeiten, über die Systemfragen hinaus neue Anwendungen

aufzugreifen, wobei insbesondere Entwicklungen im Multimedia-Umfeld sein Interesse fanden. Hervorzuheben ist dazu, dass er neben dem Aufbau der Multimedia-Arbeitsplätze im Zentrum für Informationsverarbeitung auch ein Multimedia-Praktikum mit dem Schwerpunkt „Bildgewinnung und deren Präsentation“ konzipierte, das schon mehrmals durchgeführt wurde und bei den Teilnehmern großen Anklang fand.

Über all die Jahre haben wir Hans-Werner Kisker als einen fachlich kompetenten, kooperativen und stets ausgeglichenen Kollegen geschätzt. Aufgrund gesundheitlicher Einschränkungen war er leider in den letzten Jahren (im Rahmen von Altersteilzeit) nur noch halbtags tätig und wurde Ende Februar 2005 vorzeitig pensioniert. Für seine geleistete Arbeit und die vertrauensvolle gute Zusammenarbeit danken wir herzlich und wünschen ihm für den nun beginnenden neuen Lebensabschnitt alles Gute und weiterhin Motivation und Möglichkeiten das Nützliche zu tun.

Ein ganz anderer 68er

W. Bosse

Die 68er-Generation hat ihren eigenen Ruf. Dass aber in der Informationsverarbeitung jemand zum 68er wurde, kann völlig andere Gründe haben.

In diesem Jahr ist unser Kollege Bernfried Neukäter als erster von mehreren langjährig im Zentrum für Informationsverarbeitung tätigen wissenschaftlichen Mitarbeitern Ende Januar 2005 in den Ruhestand getreten. Zwar lässt ihn sein bisheriges Tätigkeitsfeld noch nicht ganz los, doch nun ist die Zeit, ihm unseren herzlichen Dank für die geleistete Arbeit und die beständig gute Zusammenarbeit zu sagen und dies mit den besten Wünschen für seinen nun beginnenden neuen Lebensabschnitt zu verbinden.

Als der Rechner Zuse Z23 des Rechenzentrums der Universität Mitte der 60er Jahre im Gebäude Schlossplatz 5 in Betrieb war, verbrachte Bernfried Neukäter bereits viele Stunden damit, diesen zu programmieren und mit Daten zu füttern. Das Medium der Wahl war dabei der Lochstreifen, der sich auch als bestens geeignet erwies, Programmschleifen durch Zusammenkleben eines Stücks, auf dem der Programmcode stand, zu einem Ring „elegant“ zu realisieren. Anschaulicher ist das Programmieren eigentlich nie geworden. Außerdem war es damals für den Anwender ein „Muss“, sich gute Kenntnisse der Hardware und des Betriebssystems anzueignen.

Nach Abschluss seines Studiums der Mathematik mit dem Diplom war er 1967 zunächst für den Anwendungsbereich tätig und entwickelte im Anorganisch-Chemischen Institut Programme zur Kristallstrukturanalyse. In enger Zusammenarbeit mit dem Rechenzentrum war er auch in Programmierfragen und zur Nutzung der Rechenanlage beratend tätig. Außerdem befasste er sich von Anfang an intensiv mit speziellen Problemen der Informatik (obwohl es dieses Fach noch gar nicht gab!). Wichtige Themen waren dabei Datenorganisation, Betriebssysteme und Compiler. Nach Programmierkursen in Assembler für Anfänger und Fortgeschrittene bot er im Sommersemester 1971 bereits eine „Einführung in die Informationsverarbeitung“ an und war mit seiner Themenwahl sehr weitsichtig – 25 Jahre später wurde das Rechenzentrum, in dessen Dienste er 1972 eintrat, dann endlich in „Zentrum für Informationsverarbeitung“ umbenannt.

Aufgrund seiner umfassenden Kenntnisse der Rechnerstrukturen, Betriebssysteme und Sprachübersetzer war er von nun an im Arbeitsbereich *Systemsoftware* tätig. Insbesondere für die großen Zentralrechner (Mainframes) entwickelte und pflegte er umfangreiche Komponenten der Job-Eingabe-Systeme, betreute Datenfernverarbeitungskomponenten und widmete sich den Aufgaben in Verbindung mit immer komplexer werdenden Betriebssystemen für den Dialog- und Stapelbetrieb. Da er die gesamte Entwicklung der Datenverarbeitung an der Universität Münster miterlebt und mitgestaltet hat, können natürlich hier nicht alle jeweils zu ihrer Zeit wichtigen Systemkomponenten erwähnt werden, die seine Arbeit bestimmt haben. Besonders hervorgehoben werden sollen aber die IBM-Betriebssysteme MVS und VM/CMS sowie das Amdahl-Unix UTS. Vor 18 Jahren wurde er mit der Abteilungsleitung betraut. Aufgrund der zunehmenden Verbreitung von PC- und Unix-Systemen und der damit einhergehenden Aufgabenvermehrung erfolgte später dann für ihn eine Fokussierung auf den zentralen Betrieb und Spezialsysteme. Schon früh gehörte er auch zu den Kennern und Befürwortern von Linux.

Im Bereich der Anwendungen blieb er ebenfalls stets interessiert und griff neue Herausforderungen gerne auf, wobei seine intimen Systemkenntnisse von großem Vorteil waren. So entwickelte er sich schon frühzeitig zum XML-Experten und gab sein Wissen und seine Erfahrungen auch in zahlreichen Lehrveranstaltungen weiter. Außerdem unterstützte er kenntnisreich und mit viel Elan die Einführung des Content-Management-Systems für die Universität und realisierte in einem Pilotprojekt den Webauftritt für das Haus der Niederlande.

Über all die Jahre haben wir Bernfried Neukäter als einen besonders fachkundigen und besonnenen Kollegen geschätzt, der sein breites Fachwissen stets *up to date* hält und sich durch gewissenhafte und durchdachte Lösungen auszeichnet. Und als „ein ganz anderer 68er" bleibt er in besonderer Erinnerung. Denn er gehört zu den begnadeten Menschen, die wirklich die zur Definition der Programmiersprache ALGOL 68 verwendete neue zweistufige van-Wijngaarden-Grammatik verstehen und konsequent anwenden konnten. Das zeigte sich 1968 in den intensiven Arbeitsgesprächen, die wir im Rechenzentrum über den Entwurf dieser umfassenden ‚algorithmischen' Programmiersprache führten. Danach war es für uns ganz natürlich, die vom Rechenzentrum im Februar 1969 veranstaltete Tagung unter das Thema »MUEHSAL 68« (Münstersches Hochschul-Seminar über ALGOL 68) zu stellen, auf der sich über 200 Fachleute aus mehreren europäischen Ländern eine ganze Woche ausführlich mit den Facetten der im Dezember 1968 von der *IFIP Working Group 2.1 on ALGOL* abschließend definierten Programmiersprache ALGOL 68 befassten und einen ersten Erfahrungsaustausch pflegten.

Beständigkeit im schnellen Wandel

W. Bosse

Die Geschichte der Datenverarbeitung ist zwar relativ kurz, bewirkt aber aufgrund des unaufhaltsamen technischen Fortschritts einen schnellen Wandel, durch den ständig das heute Aktuelle schon morgen zum „alten Eisen" wird. Wohl dem, dessen Arbeitsfeld so beschaffen ist, dass er dieses Werkzeug methodisch nutzen kann.

Als nun dienstältester Kollege ist Dr. Siegfried Zörkendörfer nach mehr als 39 Jahren in den wohlverdienten Ruhestand getreten. Er stieß im Januar 1967 als wissenschaftlicher Mitarbeiter zu den „Männern der ersten Stunde", die damals im Gebäude Schlossplatz 5 ihren Dienst leisteten. Alle heute im Zentrum für Informationsverarbeitung (dem ehemaligen Rechenzentrum) Tätigen hat er kommen sehen und sich auch nicht durch Verlockungen der Altersteilzeit oder dergleichen verleiten lassen, vorzeitig unser Haus zu verlassen. „Mit mir können Sie rechnen" – diesen doppeldeutigen Satz hat er uns in Verbindung mit der Angabe seiner langjährigen Beschäftigungszeit, die am 28. Februar 2005 endete, noch am Arbeitsplatz zurückgelassen.

Als Mathematiker war er von Anfang an im *Anwendungsbereich* tätig. Das hatte den Vorteil, dass er zwar den schnellen Wandel in der Datenverarbeitung durch die sich verändernden Werkzeuge (Hardware und Software) erlebte, jedoch im Wesentlichen die anzuwendenden bewährten Methoden und Algorithmen beibehalten konnte (die nach Bedarf natürlich auch verbessert wurden). Entsprechend beriet er die Nutzer in der Auswahl numerischer Methoden und der Nutzung vorhandener Programmbibliotheken. Während dies vornehmlich die Naturwissenschaften betraf, zogen Wissenschaftler und Studierende zahlreicher anderer Fächer (vor allem Sozialwissenschaften, Medizin, Psychologie, Wirtschaftswissenschaften) Nutzen aus seinem Beratungsangebot zur Statistik und dem Einsatz der vorhandenen Programmsysteme zur statistischen Datenanalyse.

Seine anwendungsorientierte und auf enge Zusammenarbeit mit den Nutzern bedachte Arbeitsausrichtung lässt sich exemplarisch an zwei Fragestellungen verdeutlichen, mit denen er sich schon früh befasste: einerseits in Verbindung mit der Augenklinik die Berechnung von Netzhautbildgrößen und Kontaktlinsenüberkorrektionen und andererseits im Rahmen des SFB 7 „Mittelalterforschung" statistische Auswertungen für das automatische Auffinden von Personengruppen.

In der Lehre behandelte Siegfried Zörkendörfer als Schwerpunkt regelmäßig das Thema der statistischen Datenanalyse, wobei er methodisch fundierte Anleitungen zum fachkundigen Einsatz der mächtigen Programmsysteme SPSS bzw. SAS gab. Aus diesen Lehrveranstaltungen entstanden (gemeinsam mit D. Steinhausen) auch erfolgreiche Lehrbücher zur „Informationsbearbeitung und Datenanalyse mit dem Programmsystem SAS" und über „Statistische Datenanalyse mit dem Programmsystem SPSS…" in meh-

reren Auflagen. Außerdem sind zahlreiche Programmierkurse zu Fortran, Pascal und PL/I sowie Veranstaltungen zur „Einführung in die EDV“ zu nennen.

Gerade die Vermittlung von Grundlagen der Datenverarbeitung war auch Gegenstand der Fortbildungskurse, die das Rechenzentrum im Auftrag des Innenministeriums NRW seit den 70er Jahren für Landesbedienstete regelmäßig durchführte und an denen er stets mit großem Engagement mitwirkte. Außerdem war er an gemeinsam mit dem Landesinstitut für Curriculumentwicklung und Lehrerfortbildung durchgeführten Fortbildungsveranstaltungen für Gymnasial- und Realschullehrer beteiligt.

Im Rahmen der ihm obliegenden Aufgaben zur Software-Bereitstellung arbeitete er sich mit besonderer Gründlichkeit in zahlreiche neue Produkte oder Versionen ein und prüfte sie auf Herz und Nieren. Dank seines außergewöhnlichen „Gespürs“ gelang es ihm beim Testen immer wieder, verborgene Schwachstellen und Fehler ausfindig zu machen, sodass hilfreiche Maßnahmen für die Nutzer oft frühzeitig angestoßen werden konnten. Den Erfahrungsaustausch mit anderen Hochschulen pflegte er in seiner Funktion als stellvertretender Leiter der Abteilung *Anwendungssysteme* durch regelmäßige Teilnahme an den Besprechungen der Anwenderberater in NRW.

Fast vier Jahrzehnte war Siegfried Zörkendörfer ein fachlich kompetenter, gewissenhafter und angenehmer Kollege, der stets „das Wohl des Ganzen“ im Auge hatte und Generationen von Nutzern freundlich und hilfsbereit unterstützte. Mit unserem herzlichen Dank für die geleistete Arbeit und die langjährige gute Zusammenarbeit verbinden wir die besten Wünsche für seinen neuen Lebensabschnitt.

MIAMI – der **Dokumentenserver der Universität**

U. Seewald

Gelehrt und gelernt wird heute nicht mehr nur aus Büchern – und so ist auch an der Westfälischen Wilhelms-Universität längst das digitale Zeitalter angebrochen. Mit MIAMI, dem „**M**ünsterschen **I**nformations- und **A**rchivsystem für **M**ultimediale **I**nhalte“, steht den Angehörigen der Universität ein Publikations- und Dokumentenserver zur Verfügung, mit dem digitale und multimediale Objekte aus der Hochschule publiziert, bereitgestellt und archiviert werden können. Damit ebnet die Universitäts- und Landesbibliothek Münster (ULB) in Zusammenarbeit mit dem Zentrum für Informationsverarbeitung (ZIV) bereits seit November 2002 Wissenschaftlern und Studierenden den Weg für flexible, zeit- und ortsungebundene Arbeitsbedingungen.

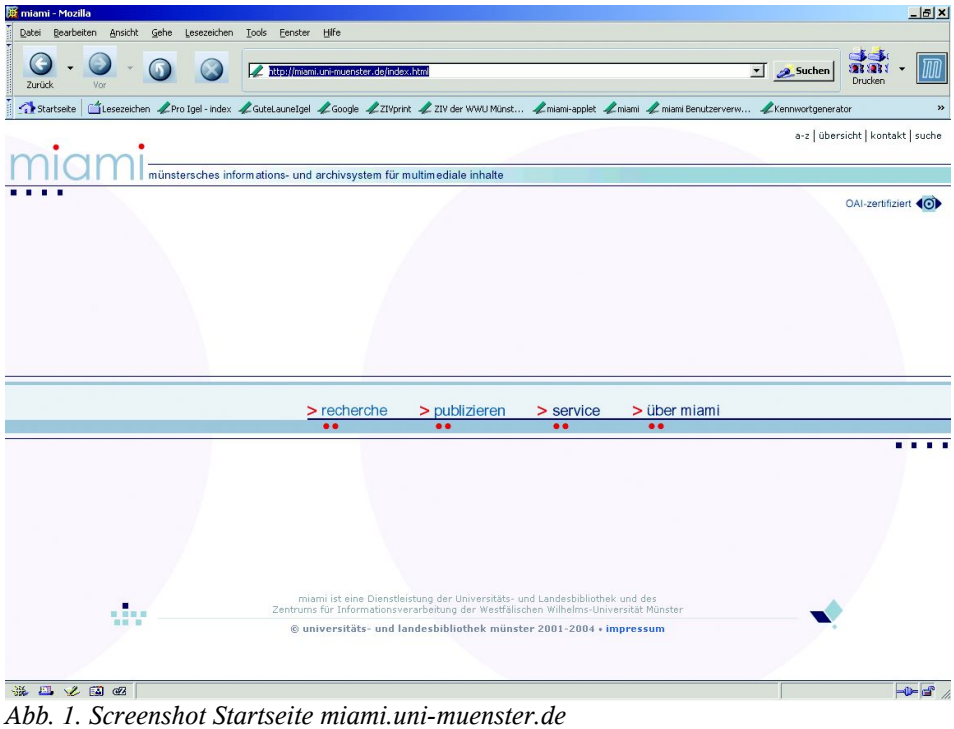


Abb. 1. Screenshot Startseite miami.uni-muenster.de

In MIAMI werden die digitalen Dokumente archiviert und formal durch Metadaten erschlossen. Schon mehr als 750 digitale Dissertationen der Universität wurden bereits durch die ULB mit MIAMI publiziert, für die Promovenden eine attraktive Möglichkeit, ihrer Veröffentlichungspflicht schnell und kostenlos nachzukommen. Auch Digitalisate wertvoller

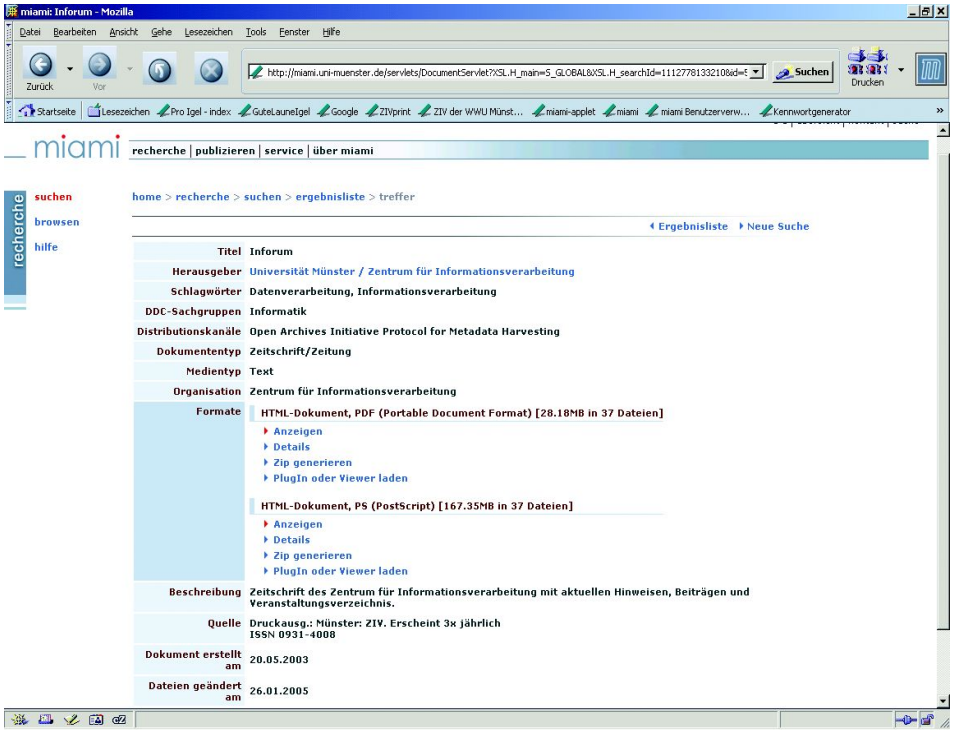


Abb. 2. Screenshot Dokumentbeschreibung infoFORUM

historischer Bestände der ULB sind eingestellt. Von Einrichtungen und Instituten der Universität herausgegebene Online-Zeitschriften werden ebenfalls mit MIAMI publiziert.

Wissenschaftliche Mitarbeiterinnen und Mitarbeiter der Universität können Dokumente und Objekte selbstständig in MIAMI einstellen und pflegen, z. B. ihre Forschungsergebnisse multimedial aufbereitet weltweit über Datennetze verbreiten. Von einfachen Texten bis hin zu interaktiven Materialien sind Dokumente unterschiedlichster Art über MIAMI dauerhaft verfügbar. Auch für aktuelles Lehr- und Lernmaterial steht der Dokumentenserver bereit. Je nach Wunsch der Lehrenden kann man den Zugriff auf Materialien einschränken, beispielsweise für Seminar- oder Kongressteilnehmer mit einem Passwortschutz versehen.

Wissenschaftlerinnen und Wissenschaftler, Studierende und Interessierte können MIAMI für die Recherche nutzen und direkt auf Volltexte und multimediale Inhalte zugreifen. Durch die Erschließung der Dokumente mit Metadaten und die leicht bedienbare MIAMI-Weboberfläche ist eine komfortable Recherche nach digitalen Dokumenten möglich.

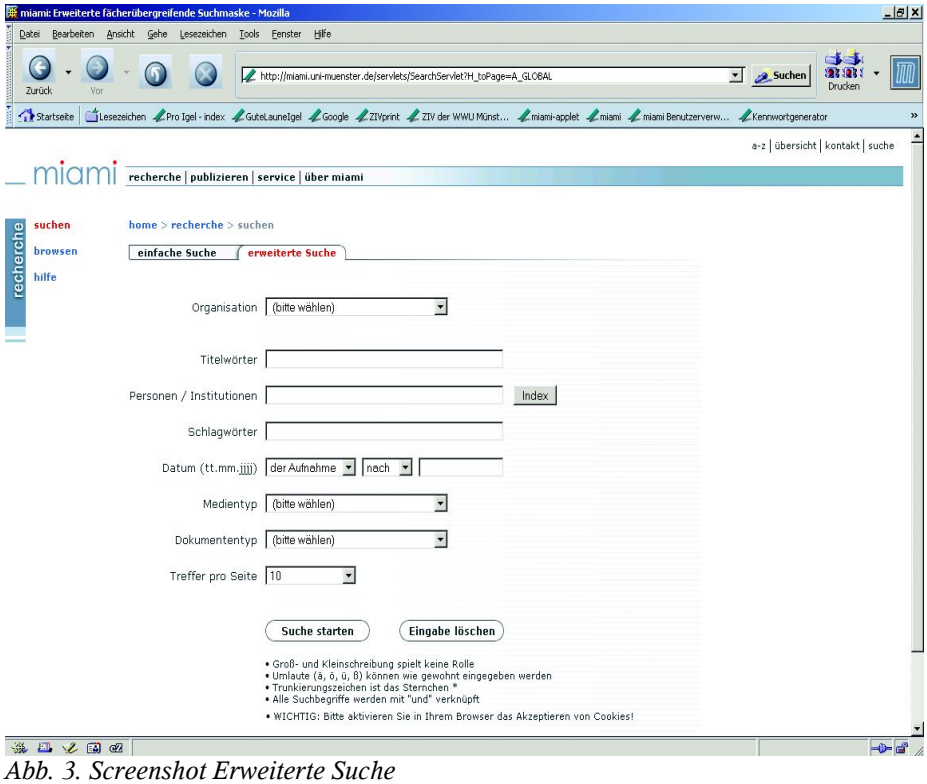


Abb. 3. Screenshot Erweiterte Suche

Die Vorteile von MIAMI liegen auf der Hand: schnelle Veröffentlichung wissenschaftlicher Erkenntnisse, weltweite Verfügbarkeit über das Internet, mehrfache Nutzung eines Dokuments zur gleichen Zeit sowie die Integrierbarkeit verschiedener Medienformate.

Anlaufstelle für alle Interessenten ist der „ServicePunkt Digitale Dienste“ in der ULB. Informationen und Hilfestellung zum Publizieren und Recherchieren findet man auch auf der MIAMI-Website

http://miami.uni-muenster.de

Inhalte verwalten für den Webauftritt

B. Neukäter

Ein Web Content Management System (WCMS, CMS) unterstützt den Anbieter von Inhalten im Web dabei, Inhalte zu erfassen, zu strukturieren, aufzubewahren und Webseiten zu erzeugen – kurz: Inhalte zu verwalten. Die WWU hat sich nach sorgfältiger Vorbereitung und in Abstimmung mit anderen Hochschulen in NRW für Imperia als CMS entschieden. Gleichzeitig wurde der Webauftritt der Universität professionell gestaltet und es wurden Richtlinien für eine einheitliche Struktur der Webseiten der Universität erarbeitet.

Die Einführung von Imperia als CMS der Universität war nicht ohne Probleme. Es waren umfangreiche Erweiterungen an dem System zu programmieren, um es an die heterogene Struktur der Universität anzupassen und die gewünschte Funktionalität zu erreichen.

Imperia läuft auf Servern unter dem freien Betriebssystem GNU/Linux. Die in der Programmiersprache Perl geschriebenen Programme von Imperia stehen als Quelltexte zur Verfügung. Nur so war es möglich, die erforderlichen Anpassungen und Erweiterungen vorzunehmen.

Die Webseiten der WWU werden der Allgemeinheit oder einem bestimmten Anwenderkreis in der Hypertext Markup Language (HTML), der lingua franca des Web, zugänglich gemacht.

Die Inhalte, die von einem CMS verwaltet werden müssen, sind – neben den Webseiten selbst – die Komponenten, aus denen die Webseiten bestehen, oder auf die verwiesen wird:

- Textbestandteile,
- Grafiken im GIF-, PNG- oder JPEG-Format,
- Audio- und Video-Dateien,
- Texte in speziellen Formaten (z. B. PDF),
- Beschreibungen der Darstellung (CSS),
- Skript-Dateien.

Die Webseiten werden aus diesen Bestandteilen mittels Imperia erzeugt und veröffentlicht. Die Textbestandteile, aus denen Imperia die Webseiten erzeugt, werden in einer relationalen Datenbank (PostgreSQL) aufbewahrt. Die übrigen Bestandteile (Grafiken usw.) sind Dateien des Dateisystems.

Imperia ist ein Inhaltsverwaltungssystem. Es verwaltet die für den Webauftritt benötigten Inhalte. Folgende Aktivitäten werden unterstützt:

- Erfassung der Inhalte,
- Strukturierung einer einzelnen Webseite und der Gesamtveröffentlichung,
- Strukturierung einer Mediendatenbank,
- Zugriffsregelungen,
- Arbeitsablaufplanung,
- Protokollierung der Arbeitsvorgänge,
- Vorschau eines entstehenden Dokuments,
- Veröffentlichung eines Dokuments,
- Erzeugung der Webseite auf dem Entwicklungssystem,
- Transfer der Webseite auf ein Zielsystem,
- Sichere Aufbewahrung verschiedener Versionen eines Dokuments,
- Kontrollierte Löschung eines Dokuments und der dazu gehörigen Bestandteile

Die Erfassung der Inhalte

Um einer großen Zahl von Anbietern die Möglichkeit zu geben, Dokumente im Web zu veröffentlichen, muss ein CMS die Eingabe und Zusammenstellung der Texte und sonstiger multimedialer Elemente erleichtern. Bei Imperia werden die Inhalte über Web-Formulare erfasst. Kenntnisse der HTML sind in der Regel nicht erforderlich. Andererseits ist Imperia flexibel genug, um in speziellen Fällen auch die Eingabe von HTML-Texten zuzulassen.

Grafiken können eingebunden werden, indem man sie per Mausklick aus einer Mediendatenbank auswählt. Dabei kann die Größe verändert werden.

Viele Anwender sind mit der Textverarbeitung auf dem PC vertraut. Daher hat das ZIV die Form der Eingabe den üblichen Textverarbeitungssystemen angeglichen. Grundlage dafür ist ein frei verfügbares Programmsystem namens HTMLAREA. Das in JavaScript geschriebene System wurde so verändert, dass es unter Imperia einsetzbar ist und den Gestaltungsrichtlinien der Universität entspricht. So werden z. B. Verweise (links) mit einem kleinen Pfeil gekennzeichnet oder Tabellen entsprechend der Stilvorgabe gestaltet. Auch das Einfügen von Grafiken und PDF-Dateien aus der Mediendatenbank wird ermöglicht.

Durch diese Anpassung wurde erreicht, dass der Erfasser von Inhalten leicht angelernt werden kann und sich nicht mit den komplexen Strukturen der HTML beschäftigen muss.

Die Strukturierung einer Webseite

Die Gestaltungsrichtlinien der Universität sehen vor, dass im oberen Teil jeder Webseite neben der Grafik des Anbieters und dem Logo der Universität die Hauptnavigation zu finden ist. Die Hauptnavigation verweist auf wichtige Unterbereiche des Anbieters. Die Navigation für jeden Unterbereich ist im linken Seitenbereich zu finden. Der mittlere Bereich enthält den eigentlichen Inhalt, während der rechte Seitenbereich eine Suchschnittstelle und weitere Verweise enthalten kann.

Die Erzeugung einer Webseite wird über eine Vorlage (template) gesteuert. Eine Vorlage sieht auf den ersten Blick aus wie eine HTML-Seite. Sie enthält jedoch spezielle Sprachelemente. Variable Bestandteile werden durch Texte ersetzt, die aus anderen Quellen stammen oder während der Erfassung eingegeben werden.

Man kann eine Vorlage auch als Programm betrachten, das einerseits die Erfassung der Inhalte steuert und andererseits bestimmt, wie die Webseite gestaltet wird. Wie in einer Programmiersprache gibt es Konstrukte zur bedingten Ausführung in Abhängigkeit von variablen Inhalten oder Zuständen und Möglichkeiten der Wiederholung vorgegebener Abläufe.

Einzelne Bestandteile der Vorlage können auch über Perl-Programme erzeugt werden. Diese Möglichkeit wird zur automatischen Erzeugung der Navigation im linken Seitenbereich benutzt. Ein im ZIV entwickeltes Programm erzeugt den entsprechenden HTML-Text.

Zur Verwaltung der Navigationseinträge musste ebenfalls ein Programm entwickelt werden, das es dem Anwender gestattet, die Navigationstexte und die Reihenfolge der Navigationseinträge zu bestimmen. Darüber hinaus kann er Dokumente aus der Navigation ausschließen sowie externe Verweise, Zwischenräume und Überschriften einfügen.

Eine weitere Entwicklung des ZIV ermöglicht die Gestaltung des rechten Seitenbereichs gemeinsam für mehrere Webseiten. Hier werden Überschriften (Kategorien) und Verweise eingefügt und eine Suchschnittstelle konfiguriert.

Die Struktur der Gesamtveröffentlichung

Die Struktur der Gesamtveröffentlichung ist eng verbunden mit der Struktur der Universität. Über Haupt- und Seitennavigation kann jede Einrichtung ihre Veröffentlichung nach Themen gliedern. Diese Struktur einer Veröffentlichung wird in Imperia abgebildet

auf Rubriken. Die Rubriken haben eine Baumstruktur mit Hauptrubrik (Stamm) und Unterrubriken (Äste). Die Dokumente sind dann gleichsam die Blätter des Baumes.

Jeder Einrichtung der Universität kann eine Hauptrubrik zugeordnet werden, die sie selbständig verwaltet.

Die Rubrikstruktur dient als Grundlage der Navigation. Für jeden Eintrag in der Hauptnavigation definiert man eine Unterrubrik der Hauptrubrik, die wiederum weiter untergliedert werden kann. Verweise auf die Dokumente dieser Rubrik werden in die Navigation an der linken Seite aufgenommen. Hat diese Rubrik selbst wieder Unterrubriken, so werden deren Dokumente in der Regel in einer zweiten Stufe – etwas weiter eingerückt – dargestellt. Eine Ausnahme ist das Dokument, das man als Leitseite der Unterubrik kennzeichnet. Der Navigationseintrag für dieses Dokument wird in die erste Stufe übernommen, in einer Reihe mit den Einträgen für die Dokumente der darüber liegenden Rubrik.

Zu jeder Rubrik kann der Anwender ein Verzeichnis angeben, das die erzeugten Dokumente aufnimmt. Mehrere Rubriken können sich ein Verzeichnis teilen. Das Verzeichnis wird relativ zu einem mit dem ZIV vereinbarten Basispfad definiert. Dadurch wird sichergestellt, dass nicht zwei von verschiedenen Einrichtungen erzeugte Dokumente die gleiche Position im Dateibaum einnehmen.

Neben dem Verzeichnis wird jeder Rubrik noch ein Dateiname, ein Arbeitsablauf (workflow), eine Metadatei (metafile) und eine Vorlage (template) zugeordnet. Der in der Rubrik angegebene Dateiname ist in der Regel unwichtig, da der Name der Datei erst beim Anlegen eines Dokuments festgelegt werden muss. Arbeitsablauf, Metadatei und Vorlage sollten im Normalfall nicht geändert werden. Es wäre für eine so heterogene Organisation wie die Universität sehr aufwändig, für alle Beteiligten unterschiedliche Arbeitsabläufe, Metadateien und Vorlagen zentral zu verwalten. Das ZIV hat aus diesem Grunde durch eine Erweiterung von Imperia die Möglichkeit geschaffen, jeder Rubrik einen Satz von Parametern zuzuordnen, über die jede Einrichtung bestimmen kann, wie ihre Webseiten im Rahmen der gemeinsamen Struktur gestaltet werden sollen. So wie ihre Rubriken verwaltet jede Einrichtung ihre Rubrikparameter selbständig.

Eine Unterrubrik erbt die Rubrikparameter der übergeordneten Rubrik, eigene Rubrikparameter gleichen Namens überschreiben die geerbten Werte.

Die Mediendatenbank

Die Mediendatenbank ist von Imperia in vier Bereiche unterteilt: Grafiken (images), Videos, Audio-Dateien und sonstiger Inhalt (content). In jedem dieser Bereiche kann vom ZIV für jede Einrichtung ein Verzeichnis zur Verfügung gestellt werden. Der Anwender kann analog zu seinen Rubriken Unterverzeichnisse einrichten. Der Anwender transferiert die Inhalte menügesteuert als Dateien in diese Verzeichnisse.

Entwicklungssystem und Zielsysteme

Jede erzeugte Webseite findet sich nach der Veröffentlichung zunächst auf dem Entwicklungssystem wieder. Die Webadresse hat die Form

`https://imperia.uni-muenster.de`<basispfad>/<verzeichnis>`/`<dateiname>

wobei <basispfad> für den Basispfad steht, <verzeichnis> für das in der Rubrik angegebene Verzeichnis und <dateiname> für den Namen des Dokuments. Ein Beispiel wäre:

```
https://imperia.uni-muenster.de/ZIV/Beratung/index.html
```

mit dem Basispfad `/ZIV/`, dem Verzeichnis `Beratung` und dem Dateinamen `index.html`. Danach folgt die „Freischaltung“. Sie bewirkt eine Übertragung der Webseite auf das Zielsystem der Rubrik. Auf dem Standardzielsystem der Universität sähe die Webadresse etwa so aus:

`http://www.uni-muenster.de`<basispfad><verzeichnis>/<dateiname>

Zugriffsregelungen

Die Rechte sind in Imperia an Rollen gebunden. Einem Anwender können mehrere Rollen zugeordnet werden. Er kann gleichzeitig mehrere Rollen annehmen. Man kann zwischen zwei Arten von Rollen unterscheiden: Werkzeugrollen und Zuständigkeitsrollen. Über Werkzeugrollen werden die verfügbaren Menüpunkte zugeordnet. Sie bestimmen, welche Programme der Anwender ausführen darf. Zuständigkeitsrollen entscheiden über Zugriffsrechte auf Rubriken, Parameter, Dokumente, Grafiken usw.

Das ZIV vergibt pro Anwender mindestens eine Werkzeugrolle und eine Zuständigkeitsrolle.

Werkzeugrollen sind:

u6cmsred
Diese Rolle erlaubt einem „Redakteur“, Rubriken und Dokumente zu bearbeiten.

u6cmsmdb
Es werden Menüpunkte bereitgestellt, die den Zugriff auf die Mediendatenbank erlauben.

u6cmshtm
Den Kennern von HTML wird die Eingabe von HTML ermöglicht.

u6cmssys
Für Systemadministratoren werden Menüpunkte zur Bearbeitung von Metadateien und Vorlagen angeboten.

Für Zuständigkeitsrollen gibt es die Namenskonvention f6iiinnn, wobei f das Fachbereichskürzel bedeutet, iii das Informationsanbieterkürzel und nnn eine laufende Nummer.

Imperia verwaltet für jeden Anwender ein Kennwort, mit dem er sich bei dem System anmeldet. Wenn der Anwender sein Standardpasswort über die Webseite des ZIV ändert, so wird dieses Kennwort von Imperia übernommen.

Arbeitsabläufe

Im Prinzip sind in Imperia verschiedene Arbeitsabläufe denkbar, die den Rubriken zugeordnet sind. Im Normalfall ist es jedoch ausreichend, den vom ZIV bereitgestellten Ablauf zu verwenden.

Wenn ein neues Dokument erstellt werden soll, muss zunächst eine Rubrik ausgewählt werden. Danach wird ein so genannter Metaschritt durchlaufen, in dem Information über das Dokument wie Dateiname und Titel eingegeben wird. Es folgt der eigentliche Bearbeitungsschritt (edit), in dem der Inhalt erfasst wird, gesteuert durch die ausgewählte oder vorgegebene Vorlage. Der nächste Schritt ist das Publizieren. Jetzt wird entschieden, ob das Dokument in eine Webseite verwandelt und veröffentlicht werden soll.

In jedem Stadium des Arbeitsablaufs kann eine Vorschau des entstehenden Dokuments angezeigt werden. Es ist auch möglich, einen begonnenen Bearbeitungsschritt zu einem späteren Zeitpunkt fortzusetzen oder zu einem früheren Schritt zurückzukehren.

Über Rubrikparameter kann man veranlassen, dass einzelne Schritte nicht ausgeführt werden. So kann man z. B. den Publikationsschritt unterdrücken, um den Ablauf zu verkürzen. Dieser Schritt ist jedoch ratsam, wenn nach Beendigung des Bearbeitungsschritts eine andere Person über die Veröffentlichung entscheidet.

Nach dem Beenden des Arbeitsablaufs wird eine Webseite auf dem Entwicklungssystem erzeugt, die anschließend freigeschaltet und damit auf ein Zielsystem übertragen werden kann. Der Zeitpunkt der Freischaltung kann im Voraus festgelegt werden, ebenso wie der Zeitpunkt, zu welchem die Webseite vom Zielsystem entfernt werden soll.

Der Anwender, der seine Webseite auf dem Entwicklungssystem oder dem Zielsystem betrachtet, kann diese per Mausklick wieder in den Arbeitsablauf befördern. Dazu muss er vorher über den Menüpunkt „Persönliche Einstellungen“ den Zusatz „One-Click-

Edit“ für seinen Browser installieren. Ältere Versionen eines Dokuments werden über den Menüpunkt „Archiv“ in der Vorschau angeschaut und wieder in den Arbeitsablauf geschleust.

Wenn nur ein das Seitenlayout betreffender Parameter geändert wurde oder ein neuer Navigationseintrag eingefügt werden soll, so braucht der eigentliche Arbeitsablauf nicht gestartet zu werden, sondern es reicht, wenn die Webseite „aufgefrischt“ wird. Das bedeutet, dass die Webseite mit den neuen Parametern, der neuen Navigation und den schon vorhandenen Inhalten noch einmal erzeugt wird.

Rubrikparameter

Obwohl jeder Rubrik eigene Parameter zugeordnet werden können, sind die meisten Parameter mit der Hauptrubrik verknüpft und werden an die Unterrubriken vererbt. Lediglich in den Fällen, in denen sich die Parameter unterscheiden, werden sie Unterrubriken zugeordnet.

Rubrikparameter dienen unterschiedlichen Zwecken:

- Systemsteuerung und Pfade
- Gestaltung der Webseite (Layout)
- Gemeinsame Texte
- Navigation
- Steuerung des Metaschritts
- Steuerung des Arbeitsablaufs

Ein typischer Parameter der ersten Gruppe ist der schon besprochenen Parameter basispfad, der vom Anwender nicht geändert werden kann. Gleiches gilt für den Parameter zielsystem, der festlegt, auf welchen Webserver die Webseite bei der Freischaltung übertragen wird. Über pfad_mdb wird der relative Pfad innerhalb der Mediendatenbank angegeben.

Beispiele für Gestaltungsparameter sind:

bereich_a_dateiname
Dateiname der Grafik im Bereich A (oben links),

bereich_a_text
Alternativtext der Grafik im Bereich A,

bereich_a_uri
URI (Webadresse) für die Grafik im Bereich A.

Manche Bestandteile der Seite können als HTML-Bausteine eingefügt werden. Ein Beispiel ist bereich_d_nav_baustein für einen Bestandteil, der oberhalb der Navigation eingefügt werden kann.

Gemeinsame Texte sind z. B. Anschriften und Telefonnummern, die auf allen Seiten einer Rubrik erscheinen sollen.

Die Rubrik, deren Dokumente im linken Seitenbereich der Navigation erscheinen, bestimmt der Parameter nav_rubrik. Auch die Texte und Webadressen der Hauptnavigation werden über Rubrikparameter definiert.

Rubrikparameter, deren Name mit eingabe_ beginnen, steuern die Eingabe im Metaschritt. So bedeutet eingabe_schlagwoerter, dass im Metaschritt Schlagwörter eingegeben werden können, die der Webseite als Metainformation für Suchmaschinen mitgegeben werden.

Soll der Publikationsschritt nicht ausgeführt werden, so setzt man den Parameter kein_publ_schritt auf 1. Das ist ein Beispiel für die Steuerung des Arbeitsablaufs. Dieser Artikel konnte nur einen Überblick geben. Weitere Einzelheiten und praktische Anleitungen sind in der angeführten Literatur zu finden.

Literatur:

Kaspar, W.: Zum Internet-Auftritt unserer Universität,
infoWWW , Sonderausgabe - Dezember 2004

Kaspar, W.: Beschreibung der Rubrikparameter

Neukäter, B.: Publizieren im Internet,
infoWWW , Sonderausgabe - Dezember 2004

Schaten, E.: Imperia 7 Handbuch für die WWU

Weitere Literaturhinweise über die Webseite des ZIV:

Service -> Dokumentationen -> System-Dokumentationen -> Imperia-Dokumentation

Entwicklung der TSM-Server-Infrastruktur

R. Mersch

Die Installation einer SAN-Infrastruktur im Rahmen der HBFG-Beschaffung Ende 2004 sowie die Möglichkeit der gemeinsamen Nutzung unseres Kassetten-Archiv-Systems durch mehrere TSM-Server („Tape Library Sharing“) erlaubt es uns, mit recht geringen zusätzlichen Mitteln ein Netz von TSM-Servern aufzubauen.

Der primäre Backup-, Archiv- und Migrations-Server TSM01 (Aliasname BACKUP) hat eine Größe erreicht, bei der eine Aufteilung des Dienstes auf mehrere Server dringend geboten ist. Gründe dafür gibt es mehrere:

- Das Erreichen der Leistungsgrenzen der Maschine, einer schon etwas in die Jahre gekommenen IBM RS/6000 F80, ist absehbar. Immerhin nimmt dieser Server derzeit pro Monat ca. 110 TB Daten entgegen. Da gleichzeitig alte Backups verfallen, resultiert dies in einem monatlichen Wachstum in Höhe von einem TB bei den lagernden Daten.
- Die Größe der TSM-internen Datenbank ist mit über 100 GB grenzwertig. Zum einen wird in der Fachwelt von massiven Performance-Einbrüchen bei derartig großen TSM-Datenbanken berichtet, zum zweiten würde bei einer – hoffentlich niemals auftretenden – Datenbank-Inkonsistenz für die Bereinigung eine Außerbetriebnahme des Servers für etliche Tage erforderlich werden.

Die Ende 2004 durchgeführte Erweiterung unseres Kassetten-Archivsystems IBM 3494 um 7 Bandlaufwerke mit Fibre-Channel(FC)-Interface bietet nun die Möglichkeit, dieses hochwertige System von einem Netz von TSM-Servern aus zu nutzen. Auch kapazitätsmäßig bietet das Archivsystem derzeit hierfür reichlich Reserven. Die neuen TSM-Server müssen dazu lediglich über ein FC-Interface verfügen, das sie mit dem SAN (Storage Area Network) verbindet, in dem sich auch die neuen Bandlaufwerke befinden. Die Steuerung des Kassetten-Archivsystems, also letztlich des Roboters, der die Bänder in die Laufwerke und wieder zurück in die Regale stellt, bleibt beim TSM-Server BACKUP. Dieser koordiniert auch die Nutzung der Bandlaufwerke, so dass sie den TSM-Servern dynamisch geordnet werden können. Alle anderen TSM-Server müssen sich also an BACKUP wenden, wenn sie ein Bandlaufwerk benötigen und ein Band eingelegt haben wollen. Dieses „Tape Library Sharing“ genannte Feature ist seit geraumer Zeit in der TSM-Server-Software vorhanden.

Wurden unsere TSM-Server bisher unter AIX betrieben, so wird wegen der geringeren Hardware-Kosten künftig Linux als Plattform angestrebt. Erste Erfahrungen mit einem Linux-basierten TSM-Server werden derzeit gesammelt. Er heißt TSM03 und hat SLES9 als Betriebssystem. Leider fehlten in diesem System bisher noch die Treiber für unsere neuen Bandlaufwerke, so dass wir das Tape Library Sharing noch nicht ausprobieren konnten. Seit April sind diese Treiber aber verfügbar. Nach einer kurzen Testphase werden wir dann neue TSM-Clients auf TSM03 registrieren und eventuell auch ausgewählte Clients von TSM01 nach TSM03 migrieren.

IPv6-Pilotbetrieb in der Universität Münster

Chr. Schild

IPv6 ist ein neues Protokoll für das Internet, das zunächst parallel zum aktuell verwendeten IP-Protokoll (Ipv4) verwendet werden kann.

Das neue Internet-Protokoll (IP Version 6) wird seit vielen Jahren vom Zentrum für Informationsverarbeitung im Rahmen des Drittmittelprojektes Projektes JOIN (`http://www.join.uni-muenster.de`) gefördert und erforscht. In Zukunft soll IPv6 IPv4 vollständig ersetzen, weil viele mit IPv4 verbundene Probleme durch IPv6 gelöst werden.

Auch im Universitätsnetzwerk ist IPv6 in einigen Teilbereichen bereits jetzt verfügbar und viele Dienste (FTP, Web, Mail, News, Time, usw.) sind über spezielle Server via IPv6 erreichbar. Der Standort Münster, der bis vor kurzem noch Kernnetzknoten des 6WiN – dem IPv6-Netz des DFN – war, ist mittlerweile als regulärer DFN-Kunde dort angeschlossen.

Die Nutzung und die Verfügbarkeit von IPv6 soll nun in Zukunft in der Universität Münster ausgeweitet werden. Statt wie bisher die Konnektivität über IPv6 nur in einigen ausgewählten Subnetzen zu aktivieren, soll IPv6 einem breiteren Nutzerkreis zur Verfügung gestellt werden. Zu diesem Zweck wird die Infrastruktur des Kernnetzes erweitert und um IPv6-Funktionalität ergänzt werden.

Es ist geplant, in diesem Jahr einen Pilotbetrieb mit interessierten Nutzern zu starten, der dann mit der Zeit in einen Produktionsbetrieb übergeht. Ob IPv6 in Ihrem Subnetz-Bereich aktiviert werden kann, ist je nach Einzelfall zu prüfen. In Fällen, wo nicht im gesamten Subnetz IPv6-Konnektivität aktiviert werden soll, besteht die Möglichkeit, einzelne Endgeräte mit dem im ZIV bereits vorhandenen sogenannten IPv6-Tunnelbroker an das IPv6-Internet anzuschließen. Eine Nutzung in Bereichen erhöhter Sicherheit schließt sich zu Beginn aus, da netzwerkseitige Sicherheitsmechanismen oft IP- oder Netzwerktopologie-basiert arbeiten, die mit IPv6 zur Zeit noch nicht 1 zu 1 portiert werden können. Der Pilotdienst soll ab der zweiten Jahreshälfte zur Verfügung stehen, eventuell schon früher. Interessierte Nutzer mögen sich bis dahin an das JOIN-Team (`join@uni-muenster.de`) wenden.

Betriebs-Parameter von Netz-Anschlussdosen in NIC_online

M. Kamp

Einige wichtige netzseitige Betriebs-Parameter von Netz-Anschlussdosen können jetzt unter NIC_online eingesehen werden.

Bisher war für Betreiber von Datenendgeräten im Netz nicht zu erkennen, mit welchen Betriebs-Parametern eine Netz-Anschlussdose genutzt werden kann. In Zweifelsfällen half nur ein Anruf beim Netz-Operations-Center (NOC, Tel. 31599), um die Information zu erhalten. Inzwischen werden aus den zugehörigen Netzkomponenten (Switches) regelmäßig alle drei bis vier Tage wichtige Parameter der Anschluss-Ports ausgelesen und in der Netz-Datenbank des ZIV gespeichert. Derzeit werden über 1000 Netzkomponenten regelmäßig überwacht, die zusammen ca. 30.000 aktive Ports besitzen. Hierbei werden etwa 500.000 Informationen abgefragt.

Einige der wichtigsten Informationen werden inzwischen im Pilotbetrieb unter NIC_online (`www.nic.uni-muenster.de`) angezeigt. Dies gelingt allerdings nur, wenn zum jeweiligen Rechner auch eine Netz-Anschlussdose dokumentiert wurde und diese sich in unserer Dokumentation bis zu einer zentralen Netzkomponente zurückverfolgen lässt. Für die meisten modernen Netzkomponenten sind die Voraussetzungen inzwischen gegeben, bei veralteter Repeatertechnik oder bei AUI-Anschlüssen ist diese Auskunft aber nicht möglich.

Angezeigt werden der administrative Zustand des Anschlusses (eingeschaltet oder ausgeschaltet), die Übertragungsgeschwindigkeit (10MBit/s, 100Mbit/s, usw.) und der Duplex-Modus (halbduplex, vollduplex, usw.) sowie der jeweilige Zeitpunkt, an dem die Daten ermittelt wurden.

Für die Zukunft ist an dieser Stelle geplant, dass Nutzer diese Betriebsparameter in einem vereinbarten Rahmen selbst umstellen können, was sicher zu einer Vereinfachung

der Administration sowohl für die Nutzer, als auch für den NOC-Dienst des ZIV führen wird.

Auch die Information, zu welchem Netz-Bereich ein Anschluss gehört, ist prinzipiell möglich, hier wird aber derzeit noch an einem Sicherheitsmodell gearbeitet, das diese Information nur den jeweils befugten Administratoren darstellt.

Zivcluster: Häufig gestellte Fragen

M. Leweling

Nach nunmehr zwei Jahren erfolgreichem Betrieb des Zivclusters ist es an der Zeit, Bilanz zu ziehen. Und zwar in Form einer Sammlung häufig gestellter Fragen, die von Benutzern in dieser Zeit in meine Mailbox eingeworfen wurden.

Die folgende Sammlung häufig gestellter Fragen zum Thema Zivcluster ist vermutlich weder wirklich erschöpfend noch repräsentativ. Die Problembereiche, mit denen man im Cluster-Alltag zu tun hat, sind so vielfältig, dass schon Fragen, die nur zweimal gestellt werden, das Kriterium der Häufigkeit erfüllen. Manche Fragen sind verallgemeinert worden, andere wiederum sind gewollt sehr spezifisch formuliert. Da die Sammlung inzwischen doch sehr umfangreich geworden ist, wird an dieser Stelle nur der erste Teil veröffentlicht; eine Fortsetzung folgt dann in den nächsten infoWUM-Ausgaben. Natürlich beginnt die Liste mit

1. Fragen zum Benutzeraccount

F: Könnten Sie für die Arbeitsgruppe x einen neuen Account für den Benutzer y anlegen mit folgenden Zugangsdaten (fremder Name und Kennung folgen)?

A: Zunächst einmal ist Voraussetzung, dass der Benutzer schon eine vom ZIV vergebene zentrale Kennung besitzt. Ist dies der Fall, sollte der Benutzer in jedem Fall selbst für seine Anmeldung über das Webformular (`https://user.uni-muenster.de/exec/zivuseradd.php`) sorgen, indem er dort seine Kennung und sein zentrales Passwort eingibt. Eine manuelle Einrichtung durch den Administrator sollte vermieden werden; der Grund hierfür ergibt sich aus der folgenden Frage:

F: Ehrlich gesagt wusste ich gar nicht, dass ich überhaupt als Nutzer am zivcluster angemeldet bin. Daher meine Bitte: Würden Sie mich bitte als Nutzer vom zivcluster löschen?

A: Selbstverständlich sollten Benutzer, die den Cluster nicht mehr nutzen wollen, eine kurze Mitteilung an den Administrator schicken. Der Plattenplatz ist knapp und wird von anderen Benutzern dringend benötigt. Ebenso sollte regelmäßiges Aufräumen durch den Benutzer eine Selbstverständlichkeit sein. Ein automatisiertes Löschen veralteter Dateien in Benutzer-Homeverzeichnissen findet nämlich nicht statt.

F: Ich habe mein Standard-ZIV-Passwort geändert, reicht das?

A: Momentan noch nicht. Die Benutzerverwaltung auf dem Zivcluster ist von der zentralen Benutzerverwaltung abgekoppelt. Zur Passwortänderung auf dem Zivcluster muss auf der Kopfstation head0102 das Kommando „passwd“ verwendet werden. Aus Sicherheitsgründen ist es sinnvoll, auf dem Cluster ein anderes als das zentrale Passwort zu verwenden und ebenso regelmäßig zu ändern.

F: Als NRW-Verbundnutzer habe ich mich auf Ihrem Webformular angemeldet. Das Formular „schluckt“ zwar die eingebenen Daten, gibt jedoch keinerlei Kommentar über Erfolg oder Misserfolg, daher weiß ich leider nicht, ob ich mich korrekt angemeldet habe oder nicht, jedenfalls ist ein Einloggen auf `zivcluster.uni-muenster.de` über ssh nicht möglich. Können Sie mir hier weiterhelfen?

A: Bei erfolgreicher Anmeldung bekommt man seine numerische User-ID (UID) und Gruppen-ID (GID) angezeigt, bei Misserfolg erscheint wieder das leere Formular. Für NRW Verbundnutzer schlägt die Anmeldung häufig fehl, wenn die entsprechende DCE-Zelle nicht funktioniert und auf die zentralen Kennungsdaten nicht automatisch zugegriffen werden kann. In solchen Fällen richte ich die Benutzerkennung manuell ein und setze das Anfangspasswort für die Verbundnutzung als Passwort für den Cluster ein. Dieses sollte natürlich umgehend vom Benutzer auf dem Cluster geändert werden.

F: Ich habe letzte Woche versucht, mir eine Nutzerkennung für den Linux-HPC-Cluster über den Link „Web-Formular“ auf der entsprechenden Webpage einzurichten. Leider habe ich bis jetzt keine E-Mail (o. Ä.) zur Bestätigung oder ein Passwort erhalten. Ich bin mir nicht sicher, ob die Anmeldung über jenes Web-Formular funktioniert hat, daher bitte ich Sie, dies zu überprüfen und mir eine Nachricht über meinen Anmeldestatus zu senden.

A: Erfolg oder Misserfolg bei der Anmeldung erkennt man schon wie in der Antwort zur letzten Frage. Man erhält auch kein neues Passwort, sondern das zentrale Passwort wird nach Eingabe in das Formular auf den Cluster übertragen. Ansonsten kann man eine erfolgreiche Anmeldung daran erkennen, dass man sich mit dem zentralen Passwort mittels ssh (Secure Shell) auf dem Rechner `zivcluster` einloggen kann. Eine Bestätigung per E-Mail ist somit nicht notwendig und auch nicht vorgesehen. Falls das zentrale Passwort vergessen wurde, kann man sich am Serviceschalter im Gebäude Einsteinstr. 60 ein neues Passwort setzen lassen und die Anmeldung über das Web-Formular wiederholen.

F: Ich habe mein lokales Passwort auf dem Zivcluster vergessen. Was nun?

A: In diesem Fall setze ich zunächst einmal das zentrale Anfangspasswort auf dem Cluster ein. Das Schreiben vom ZIV haben Sie hoffentlich aufbewahrt ...

2. Fragen zu Nutzungsmöglichkeiten und zur Installation

F: Auf dem Zivcluster müssen wir Standardprogramme mit sehr anspruchsvollen Problemgrößen rechnen. Leider haben wir aber Probleme mit dem Arbeitsspeicher auf dem Zivcluster. Anscheinend stehen uns als Default nur 900 MB zur Verfügung. Wir benötigen aber ca. 2 GB. Wir würden uns daher freuen, wenn Sie dieses Limit für unseren Account höhersetzen könnten.

A: Die Knoten auf dem Cluster haben nur 1 GB Hauptspeicher. Etwa 150 MB davonwerden vom System selbst benötigt und stehen für Benutzer-Prozesse ebenfalls nicht zur Verfügung. Exzessives Swapping hingegen führt das Konzept des Hochleistungsrechnens ad absurdum und führt außerdem zu instabilen Systemen bis hin zu Abstürzen. Daher ist der Adressraum für jeden Benutzerprozess auf 850 MB limitiert. Die Speicherbänke der Rechenknoten sind voll belegt, daher kommt auch eine Aufrüstung des Hauptspeichers mit diesem Cluster nicht in Frage, zumal die Speichermodule praktisch nirgendwo sonst wiederverwertet werden können. Bei manchen parallelen Programmen kann man durch Verwendung von mehr Rechenknoten den Speicherbedarf pro Knoten reduzieren. Leider funktioniert das nicht immer.

F: Kann es eigentlich sein, dass Benutzer xy so viel Rechenzeit auf unserem Cluster verbraucht, und das als Gast von einer anderen Uni? Haben wir eigentlich zuviel Rechenzeit oder was?

A: Da der Cluster etwa zu einem Drittel aus Mitteln des NRW-Verbunds bezahlt worden ist, steht Benutzern aus anderen Unis des Landes NRW auch insgesamt ein Drittel der Rechenzeit zu. Dieser Anteil ist bisher jedenfalls noch nicht voll ausgeschöpft worden, auch wenn er vielleicht in einer Momentaufnahme einmal überschritten worden ist.

F: Ich möchte ein eigenes Programmpaket auf dem Cluster installieren, darf ich das?

A: Dafür ist der Cluster ja gedacht. Wenn es sich allerdings um ein Standard-Programmpaket handelt, welches für einen größeren Benutzerkreis von Interesse ist, sollte eine zentrale Installation einer Installation im eigenen Homeverzeichnis vorgezogen werden. Und insbesondere wenn andere Methoden zur Kommunikation als die vorinstallierten (MPICH-GM, MPICH-P4) verwendet werden sollen, muss der Benutzer dafür Sorge tragen, dass nur die vom Batch-System zugewiesenen Rechenknoten verwendet werden und Jobs anderer Benutzer dadurch nicht gestört werden. Auch für die Einhaltung von Lizenzbedingungen ist dann natürlich der Benutzer selbst verantwortlich.

F: Zur grafischen Auswertung meiner Daten benötige ich das Programm xy. Kannst Du dieses Programm auch auf dem Zivcluster installieren?

A: Sofern sich der Aufwand dafür vertreten lässt. RPM-Pakete, die für die Linux-Distribution vorliegen, stellen kein Problem dar. Programme, die einen Kompiliermarathon nach sich ziehen, weil sie eine Unmenge von Bibliotheken benötigen, die der Distributor nicht anbietet oder nur in inkompatiblen Versionen, sind eher schlechte Kandidaten. Anders sieht es aus, wenn das Programmpaket für die Berechnungen selbst erforderlich ist (Beispiele: APBS, NAMD, ScaLAPACK, ...). Die grafische Aufbereitung von Daten sollte ohnehin eher auf normalen Arbeitsplatzrechnern erfolgen, da hierfür meist kein paralleler Rechenbedarf besteht.

F: Kann man nicht mal schnell eine neue Compiler-Version installieren?

A: Nicht, wenn die neue Compiler-Version eine neue Betriebssystemversion erfordert. Bei den Systemvoraussetzungen achte man unter anderem auf die Kompatibilität zur bestehenden GNU C Library (glibc). Ein Update des Betriebssystems erfordert ein Neukompilieren nahezu aller zuvor angepassten Bibliotheken und Programmpakete (MPICH, Gaussian, ...) und dementsprechend langfristige Planung.

F: Kann ich meine Programme und Skripte auf einem Windows-System schreiben und dann einfach auf den Cluster kopieren? Mir gefällt mein Editor hier einfach besser.

A: Beim Kopieren mittels Secure Copy von einem Windows-System bleiben die MS-DOS-Steuerzeichen für Zeilenumbrüche erhalten. Diese bringen das Batch-System durcheinander, in der Form, dass ausführbare Programme innerhalb eines normal aussehenden PBS-Skriptes nicht gefunden werden. Dem Programmnamen hängt dann nämlich noch ein unsichtbares Steuerzeichen an. Falls man dies als Fehlerursache für angeblich nicht auffindbare Programme vermutet, sind die Befehle „file“ und „recode“ hilfreich. Angenommen, das Job-Skript job.pbs wurde mit einem Windows-Editor erstellt und auf den Cluster kopiert, dann lässt sich der Fehler vermeiden durch:

```
[lewelin@head0102 lewelin]$ file job.pbs
job.pbs: ASCII English text, with CRLF line terminators
[lewelin@head0102 lewelin]$ recode ibmpc..latin1 job.pbs
[lewelin@head0102 lewelin]$ file job.pbs
job.pbs: ASCII English text
```

Anschließend kann das Skript problemlos mit `qsub job.pbs` abgeschickt werden. In der nächsten Ausgabe werden Fragen zum Batch-System (PBS) beantwortet. Fortsetzung folgt.

Webcam im Botanischen Garten

D. Frieler

Das Botanische Institut hat in Kooperation mit dem Dez. 4.43 (Kommunikations- und Medientechnik) und dem ZIV Anfang März im Botanischem Garten eine Webcam (zu deutsch: Netzkamera) aufgestellt und in Betrieb genommen. Die Bilder sollen zur Erweiterung des Internetauftritts des Botanischen Gartens dienen. Es sollen zu unterschiedlichen Tageszeiten verschiedene Ansichten gezeigt werden. Die Ansichten sind so gewählt, dass der Datenschutz gewahrt bleibt.

Es handelt sich um eine Kamera der Firma Axis mit Netzanschluss und integriertem Webserver. Sie ist motorgetrieben 360° schwenkbar

Abb. 1. Die Web-Cam

und 90° neigbar. Montiert ist sie in einem wettergeschütztem Gehäuse mit Rundumsicht und eingebauter Klimatechnik/Heizung.

Das ZIV hat ein Glasfaserkabel vom Verteilerraum im Hauptgebäude des Instituts bis in das Kameragehäuse verlegt und dort zusätzlich einen Medienkonverter installiert.

Die Bilder werden in Kürze auf den Web-Seiten des Gartens (http://www.uni-muenster.de/BotanischerGarten) zu finden sein.

Abb. 2. Das Schloss, aufgenommen von der Webcam

Abb. 3. Der See, aufgenommen von der Webcam

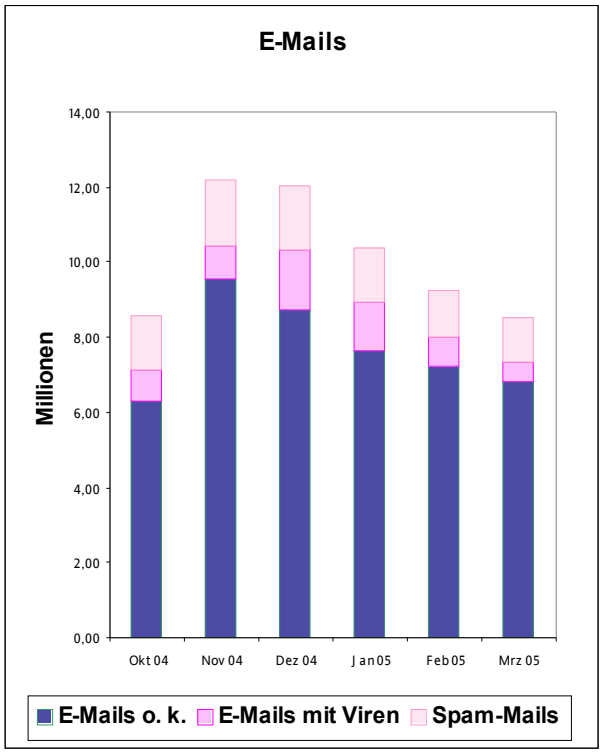
ZIV-Sicherheit

Sicherheit der Informationsverarbeitung – das endlose Thema

W. Bosse, W. Held, W. Kaspar, S. Ost, G. Richter

Universitäten dürfen nicht wie Betriebe oder Ämter weitgehend und rigoros vom Internet abgesperrt werden, denn Forschung und Lehre brauchen offene Verbindungen mit der Welt. Andererseits gibt es Bereiche, in denen dringender Schutzbedarf besteht, wenn z. B. Forschungsergebnisse vor ihrer Veröffentlichung, Prüfungsdaten, Personaldaten oder medizinische Daten zu verarbeiten und zu speichern sind.

Aber auch für derart differenzierte Schutz-Bedürfnisse lassen sich Sicherungen einrichten, sie erfordern jedoch vielfältige Maßnahmen in den Rechnernetzen, am Arbeitsplatzrechner und auf Servern. Dazu gehören auch organisatorische Maßnahmen und das notwendige Bewusstsein und Wissen bei den Nutzern der Informationsverarbeitung.



Hacker kennen natürlich die relative Offenheit der Universitäten und nutzen dies. Wir haben im letzten Halbjahr zentral im ZIV monatlich bis zu 12 Mio. ein- und ausgehende E-Mails bearbeitet und dabei bis zu 5 Mio., **also rund 40 %,** entdeckt, die wir als **virenverseucht bzw. spamverdächtig** erkannt und entsprechend behandelt haben. Summiert über alle 6 Monate waren 25 % virenverseucht oder spamverdächtig. Ergänzend muss man auf dem eigenen PC weitere Abwehrmaßnahmen gegen Viren und Spam einsetzen (s. u. folgende Goldene Regeln), denn zentral ist leider nicht alles erkennbar. Darüber hinaus mussten wir im Jahre 2004 monatlich ca. 125 Angriffe auf Rechner in der Universität oder von diesen ausgehend behandeln (Steigerung 60 % gegenüber 2003), welche die Arbeit anderer stören oder weitergehende Schäden anrichten. 110 bis 115, **also etwa 90 %,** dieser Angriffe gehen (oft ohne Wissen des Besitzers) von „gehackten“ häuslichen (!) Arbeitsplatzsystemen aus, der Rest (also 10 bis 15) lässt sich auf schlecht gepflegte Server und Arbeitsplatzrechner in den Fachbereichen unserer Universität und im Universitätsklinikum zurückführen. Häufig sind Windows-Systeme das Ziel dieser Angriffe, aber auch Unix-Systeme können betroffen sein:

Ein Linux-System unserer Universität verteilte in einer Nacht 4 – 5 Mio. Spam-Mails und in der Folge gingen 40.000 Beschwerden per E-Mail ein. Dies ist nicht mehr beiläufig abzuhandeln!

Oftmals beobachten wir einen **grob fahrlässigen** Umgang mit Passwörtern. Passwörter werden nicht nur schlecht, d. h. leicht erkennbar, gewählt. Es ist vielmehr **unfassbar**, dass es immer noch unbedarfte Mitarbeiter gibt, die andere auffordern, ihnen ihr Passwort zu nennen, obwohl dies in keinem Fall notwendig ist. Vielmehr hat jeder dafür zu sorgen, dass keine andere Person Kenntnis von Benutzerpasswörtern erlangt.

Schon heute kann man, wenn man mit Sorgfalt auf allen Arbeitsplatzrechnern und Servern vorgeht, die Sicherheit deutlich weiter verbessern. Es müsste doch jedem Verantwortlichen in Universität und Universitätsklinikum zu denken geben, dass auf den über 400 Servern, hunderte Rechner in CIP-Pools oder der noch größeren Zahl von Arbeitsplatzrechnern, die von IV-Versorgungseinheiten oder vom ZIV gepflegt werden, praktisch keine Angriffe zum Ziel kommen und von diesen auch keine Angriffe ausgehen.

Das Rektorat hat nach Beschlüssen der zuständigen Gremien längst den Rahmen festgelegt, in denen sich Nutzer mit ihren Rechnern bewegen müssen, wenn sie Zugang zum Rechnernetz von außerhalb oder innerhalb der Universität haben wollen. Manche Mitglieder der Universität nehmen das leider immer noch nicht ernst genug, obwohl der zu-

sätzlich zu leistende Aufwand und die Störung bei der Arbeit zur Beseitigung der Folgen unerträglich hoch sind.

Das ZIV hat jetzt, nachdem die Technik entsprechend fortgeschritten ist, für viel Geld eine Reihe von Komponenten beschafft, mit denen die Sicherheit weiter verbessert werden wird: In naher Zukunft werden z. B. Rechner, von denen Angriffe ausgehen, **automatisch solange blockiert** werden, bis die Ursachen behoben sind. In einem weiteren Schritt werden solche Rechner, deren Software-Konfigurationen nicht einen bestimmten Pflegezustand aufweisen, überhaupt nur noch einen sehr begrenzten Zugang erhalten, unabhängig davon, ob sie gerade stören oder nicht.

Doch schon jetzt muss mit wenig Aufwand für den Einzelnen mehr für die Sicherheit getan werden: Die folgenden *Goldenen Regeln*[1] sind beim Einsatz von Arbeitsplatzsystemen und Servern dringend zu beachten:

1. Das Betriebssystem ist aktuell zu halten, d. h. Updates sind zeitnah einzuspielen.
2. Virenscanner[2] sind zwingend zu verwenden und aktuell zu halten. Spam-Markierer oder -Löscher sollten zusätzlich eingesetzt werden (z. B. Deleatur aus dem ZIV oder Produkte anderer Hersteller)
3. Eine „Personal Firewall“[2] soll eingesetzt werden.
4. Sichere Passwörter müssen laut der Benutzungsordnung des ZIV und der IVVen, veröffentlicht in den Amtlichen Bekanntmachungen (Ausgabe 2000/9 vom 15.08.2000) oder unter `http://www.uni-muenster.de/Rektorat/buni/ab00905.htm`, verwendet und regelmäßig geändert werden. Hinweise zur angemessenen Wahl eines sicheren Passwortes finden Sie im folgenden Artikel. Die einzuhaltenden Randbedingungen werden automatisch überprüft.
5. Sicherheitskritische Anwendungsprogramme müssen richtig und gewissenhaft konfiguriert und aktuell gehalten werden.
6. Nicht benötigte Dienste sollten deaktiviert werden, dies gilt insbesondere für Arbeitsplatzrechner nachts und an Wochenenden.
7. E-Mails sollten nur geöffnet werden, wenn sie zuvor auf Viren untersucht wurden. Mit perMail werden Anhänge vor dem Öffnen automatisch auf vorhandene Viren untersucht. Zweifelhafte E-Mails dürfen nicht bearbeitet oder beantwortet werden. Anhänge einer E-Mail öffnet man nur, wenn der Absender bekannt ist und die Betreff-Zeile sinnvoll erscheint. Diese Aufmerksamkeit ist dringend notwendig, weil Viren sich manchmal in wenigen Minuten verbreiten, so dass die Virenscanner sie bei ihrem Auftreten noch nicht berücksichtigen können.
8. Regelmäßig müssen Datensicherungen durchgeführt werden. Das ZIV bietet dazu einen leistungsfähigen und komfortablen Service an, beschrieben unter `http://www.uni-muenster.de/ZIV/Content_HinweiseSicherung.html`.
9. Persönliche Aufmerksamkeit ist stets erforderlich. Unregelmäßigkeiten und merkwürdige Abläufe sollten stets an den zuständigen Administrator und die IVV bzw. an die CERT-Stelle des ZIV (E-Mail: `ziv@uni-muenster.de`) gemeldet werden.

1 Diese Regeln sind vom Rechenzentrum der Universität Duisburg-Essen formuliert und für hiesige Zwecke angepasst worden.

2 Die Universität hat Virenscanner- und Personal-Firewall-Software beschafft, die von allen Mitgliedern der Universität auch für häusliche Arbeitsplatzsysteme kostenfrei genutzt werden kann. Das ZIV und einige IVVen bieten zu den Punkten 1 bis 3 der Goldenen Regeln entsprechende Dienste und Unterstützungen.

Zum Umgang mit und zur Bildung von Passwörtern

St. Ost, R. Perske

In der Benutzungsordnung des ZIV und der IVVen findet man in § 3 (2) 4.) bis 6.), folgende Festlegungen

(http://www.uni-muenster.de/Rektorat/abuni/ab00905.htm):

(2) Die Nutzer sind verpflichtet,

...

4.) ausschließlich mit den Benutzerkennungen zu arbeiten, deren Nutzung ihnen im Rahmen der Zulassung zugewiesen wurde;

5.) dafür Sorge zu tragen, dass keine anderen Personen Kenntnis von den Benutzerpasswörtern erlangen, sowie Vorkehrungen zu treffen, damit unberechtigten Personen der Zugang zu den DV-Ressourcen des IV-Systems der WWU verwehrt wird;

6.) dazu gehört auch der Schutz des Zugangs durch ein geheimzuhaltendes und geeignetes, d. h. nicht einfach zu erratendes Passwort, das möglichst regelmäßig geändert werden sollte; fremde Benutzerkennungen und Passwörter weder zu ermitteln noch zu nutzen;

Im Einzelnen empfehlen wir dazu:

1. Ändern Sie Ihr Passwort möglichst alle 4 Wochen, spätestens alle 6 Monate!
2. Bilden Sie das Passwort nach folgenden Regeln:
   a) Verwenden Sie kein Wort aus irgendeinem Wörterbuch einer beliebigen Sprache.
   b) Das Passwort sollte mindestens 8 Zeichen und (aus technischen Gründen) höchstens 16 Zeichen lang sein.
   c) Es sollte aus mindestens 6 verschiedenen Zeichen bestehen.
   d) Es sollte mindestens einen Kleinbuchstaben enthalten.
   e) Es sollte mindestens einen Großbuchstaben oder eine Ziffer oder ein Satzzeichen enthalten.
   f) Falls nur ein Großbuchstabe (aber keine Ziffer und kein Satzzeichen) verwendet wird, dann darf der Großbuchstabe nicht das erste Zeichen sein.
   g) In Passwörtern sollten (aus technischen Gründen) nur druckbare 7-Bit-ASCII-Zeichen verwendet werden, das heißt alle auf der üblichen deutschen Tastatur aufgedruckten Zeichen **mit nachfolgenden Ausnahmen**:

      Leerzeichen

      Tabulator-Zeichen

      ä ö ü ß Ä Ö Ü

      ° = Umschalt ^ (oben links auf der Tastatur)

      § = Umschalt 3

      ² = AltGr 2

      ³ = AltGr 3

      µ = AltGr M

      € = Euro-Zeichen = AltGr E

      ´ Acute-Akzent-Zeichen ` (oben rechts auf der Tastatur, unterscheidet sich vom Apostroph = Umschalt ')

Die Einhaltung dieser Regeln 2.b) bis 2.g) wird bei Änderungen des zentralen Standardpassworts und des Netzzugangspassworts automatisch überprüft und erzwungen.

Security-Audit an der Universität Münster

G. Richter

Wie sicher ist die IV an WWU und UKM?

Die Universität wird in diesem Jahr erstmals ein Security-Audit (security: Sicherheit, Sicherung, Schutz; audit: Prüfung, Revision) für den Bereich der Informationsverarbeitung (IV) durchführen, an dem alle Einrichtungen teilnehmen sollen.

Sicherheit in der IV ist Allerweltsthema. Es beginnt bei der individuellen Betroffenheit und reicht bis zu rechtlichen und wirtschaftlichen Weichenstellungen mit weit reichenden Konsequenzen – es beginnt bei den von Viren heimgesuchten Heim-PC-Nutzern, die einfach ihre Plagegeister los werden müssen, aber betrifft schließlich Wirtschaftsunternehmen, die durch gesetzliche Regelungen (Sarbanes-Oxley Act, Basel II oder KonTraG) verstärkt gezwungen sind, mit großem Aufwand die Sicherheit ihrer IT-Infrastrukturen (IT: Informationstechnologie) und IV-Prozesse im Rahmen eines Risiko-Managements nachzuweisen, um überhaupt noch im nationalen und globalen Markt agieren zu können.

Auch für die Universität und das Universitätsklinikum ist die Fragestellung nach dem Stand der IV-Sicherheit natürlich von großer Bedeutung, in mancher Hinsicht auch existentiell. Nicht nur der Schutz von persönlichen Daten ist zu gewährleisten, um ein Beispiel zu nennen, wo unabweisbare rechtliche Rahmenbedingungen gesetzt sind. Sichere Informationsverarbeitung ist allein schon vor dem Hintergrund der Sicherung von Forschung und Lehre, der Krankenversorgung usw., allgemein für die Sicherung aller IT-gestützten Produktions- und Geschäftsprozesse notwendig und schließlich muss der Aufwand für die Beseitigung von direkten Schäden durch Sicherheitsvorfälle und den häufig noch viel größeren Folgeschäden auf ein tolerables Maß begrenzt werden. Unmittelbar Verantwortliche für die IV-Versorgung kennen die Problematik aus der täglichen praktischen Erfahrung – eine Vielzahl von Ursachen, von der mangelnden Ausbildung manches Systembetreibers bis zur ungenügenden Infrastruktur, kann in der Summe zeitweise an die Grenzen des leistbaren Arbeitsaufwandes für die Beseitigung allein der unmittelbaren Schäden führen. Die Leitungen von Universität und Universitätsklinikum und der untergeordneten Einrichtungen müssen aber schließlich dafür Sorge tragen, dass eine angemessene IV unter Beachtung wirtschaftlicher Aspekte, also rationell durchgeführt wird. Ein effektives Risiko-Management ist auch hier zwingend; die demnächst feststehenden Ergebnisse der kürzlich durchgeführten Prüfung des Landesrechnungshofes werden auch in diesem Punkt mit Spannung erwartet.

Die Universität Münster hat aber, so kann man aufgrund von Vergleichen feststellen, bereits viel in die Wege geleitet, um Sicherheit fest in der IV zu verankern. Sowohl das organisatorische Umfeld einer verteilten, aber wohl strukturierten IV-Landschaft als auch wichtige Bereiche der sonstigen Infrastrukturen bieten bereits heute gute Voraussetzungen. Verwiesen sei beispielsweise auf die Regelungen vom 8.6.2004 zur/zum „Technisch Verantwortlichen (für vernetzte IV-Systeme)“, womit ein schon in der Praxis bewährtes Instrument Eingang in die Universitätsordnung gefunden hat, so dass die Umsetzung und Überwachung von Sicherheitsmaßnahmen vor Ort gesichert werden kann. Auch die Strukturierung in IV-Versorgungsbereiche mit ihren IV-Versorgungseinheiten trägt durch eine anwendernahe Einflussnahmemöglichkeit zur Sicherheit der IV am Arbeitsplatz bei. Verwiesen sei auch auf Regelung und Beschluss vom 11.3. bzw. 6.5.2004, in denen IT-Nutzer unter Androhung von Sanktionen für den Fall der Missachtung verpflichtet werden, Standardvorkehrungen (Virusschutz, Personal Firewall, Betriebssystem-Updates) zur IV-Sicherheit zu treffen. Begleitet wird diese Maßgabe aber durch eine kostenlose Bereitstellung entsprechender Lizenzen für jeden Universitätsangehörigen, also auch für Studierende, so dass die Beachtung der Vorgaben meistens ohne Probleme möglich sein dürfte. Einige IV-Versorgungseinheiten können schon jetzt durch „Policy-Orchestrierung“, also durch eine servergesteuerte Konfiguration der

IT-Arbeitsplätze entsprechend sichere Betriebsbedingungen vorgeben oder zumindest unterstützen.

Nicht unerwähnt bleiben dürfen viele durch das Rektorat unterstützte Einzelmaßnahmen für die IT-Infrastruktur, z. B. zur Sicherung der Verfügbarkeit von IV-Diensten durch die Ausstattung von Server-Standorten mit Klimatisierungs- und Strom-Notversorgungseinrichtungen. Last not least, auch für das Datenübertragungsnetz wurden in der Vergangenheit und werden aktuell umfangreiche Maßnahmen getroffen, um das Risikopotential zu reduzieren. Beispiel sind die Redundanzen im Netz-Backbone, die dort in den meisten Bereichen Ersatzübertragungswege bei Leitungsausfällen automatisch zuschalten, so für die Verbindung zum Wissenschaftsnetz G-WiN und Internet oder für die Versorgung des Schloss- und Altstadtbereiches (durch einen Ersatzweg über die Scharnhorststraße und den Klinikenbereich). Aktuelle Maßnahmen zur Einbettung von „Stateful Packet Screens“ („Firewalls“) und Intrusion-Prevention-Funktionen werden in einem eigenen Beitrag in diesem infoDUV beschrieben.

Sicherheit definiert sich dadurch, dass Risiken in dem Maße eingedämmt worden sind, dass die verbleibenden Restrisiken vertretbar sind und ein angemessenes Verhältnis von Aufwand für die Sicherheitsmaßnahmen zu deren Nutzen gewährleistet ist. Dementsprechend empfiehlt es sich, grundsätzlich zunächst eine Risikoanalyse durchzuführen, den Nutzen und Aufwand bei Schutzmaßnahmen zu ermitteln, um schließlich nach einer Prioritätendefinition die als notwendig erachteten Maßnahmen durchzuführen; es müssen also verschiedene Faktoren bewertet werden. Das Verfahren insgesamt ist dabei nicht als einmaliger Prozess zu verstehen, sondern als nachhaltige zyklische Vorgehensweise, beginnend bei Planung (mit einer Bestimmung der Sicherheitsziele) über die Umsetzung und Kontrolle bis zur Anpassung. Mit der Einrichtung eines durchgängigen Security-Audit-Verfahrens an der Universität Münster und seiner erstmaligen Durchführung werden zwei wichtige Bestandteile in dieser Prozesskette des Informationssicherheitsmanagements (ISM) etabliert, die Feststellung des Schutzbedarfs und die Feststellung getroffener Sicherheitsvorkehrungen. Daraus abgeleitet werden kann der erreichte Stand der IV-Sicherheit bzw. können noch bestehende Defizite sichtbar gemacht werden. Das Security-Audit kann damit als Steuerungsinstrument benutzt werden – es ist Nachweis für getroffene Maßnahmen und Erreichtes, erlaubt die Überprüfung der Zielvorgabeneinhaltung („Compliance“) und ist Planungsgrundlage für noch einzuleitende Maßnahmen. Dies gilt nicht nur für die obersten Gremien der Universität, sondern auch für alle Verästelungen unserer IV-Struktur.

Das Security-Audit-Verfahren für die Universität Münster ist angelegt als Online-Verfahren, das unter Verwendung der Netzdatenbank im ZIV durch die für die IT-Endgeräte im Netz zuständigen Technisch Verantwortlichen bedient wird. Es wird also keine Befragung mit speziellem Personal mit Fragebögen durchgeführt, wie dies häufig sonst geschieht. Nachteil hier ist sicherlich, dass die Fragestellungen i. A. nicht persönlich erläutert werden können – es gibt aber umfangreiche Online-Hilfen –, und die Qualität der Ergebnisse ist möglicherweise etwas geringer, aber der Aufwand für zusätzliches Personal oder externe Dienstleister kann somit in Grenzen gehalten werden. Auch ist der entscheidende Vorteil in der gewünschten Nachhaltigkeit zu sehen: Die Durchführung kann nach Bedarf wiederholt werden, wobei soweit als möglich auf die Antworten früherer Ermittlungen zurückgegriffen werden kann. Jedenfalls steht erstmals ein Instrument zur Verfügung, mit dem systematisch und durchgängig eine Revision der IV-Sicherheit durchgeführt werden kann.

Das erste Security-Audit nach dem geschilderten Verfahren beginnt in den nächsten Tagen mit einigen Pilotanwendern. Nach sich dann möglicherweise ergebenden Korrekturen, voraussichtlich Anfang Mai, steht das Verfahren allen Einrichtungen von Universität und Universitätsklinikum zur Verfügung; ein genauerer Stichtag für die Erhebung wird noch bekannt gegeben werden. Aufgefordert zur Teilnahme sind alle IV-Versorgungsbereiche, jedoch besteht zzt. keine verbindliche Verpflichtung dazu. Der IV-Lenkungsausschuss und die IV-Kommission unterstützen das mit diesem Verfahren verfolgte Ziel und den Weg aber ausdrücklich.

In der jetzigen Form des Fragenkataloges liegt der Schwerpunkt des Security-Audits auf der IT-Endgeräteseite, Fragen zum Umfeld (Raumsicherheit u. Ä.) werden nur bei höherem Schutzbedarf gestellt. Der Fragenkatalog lehnt sich an die Vorgehensweise des Bundesamtes für Sicherheit in der Informationstechnik (BSI) an, jedoch wurde an einigen Stellen der Umfang deutlich reduziert und an die Verhältnisse in der Universität angepasst, um die Akzeptanz zu verbessern. Man darf aber trotz aller Verkürzungen, die natürlich auch zu Lasten der Genauigkeit und Vollständigkeit gehen mögen, nicht den verbleibenden Aufwand unterschätzen. In das Online-Verfahren sind jedoch etliche Mechanismen eingebaut, die zur Bedienungsvereinfachung dienen. So können immer wiederkehrende Antwortmuster individuell durch die Technisch Verantwortlichen definiert und zugeordnet werden, so dass Wiederholungen auf ein Mindestmaß verringert sein dürften. Der folgende Artikel in diesem infoWWW erläutert die Details genauer und gibt auch sonst einen genaueren Einblick in die Fragestellungen.

Hilfestellungen zum Security-Audit gibt das Netz-Informations-Center (NIC) unter ✆31 598 und NIC@uni-muenster.de und hier insbesondere auch Frau Labahn, die den folgenden Artikel verfasst hat und in großem Umfang an der Gestaltung des Online-Verfahrens beteiligt ist (✆ 31 625 und labahn@uni-muenster.de).

ISIDOR – Online-Security-Audit an der Universität Münster

M. Labahn

ISIDOR – Informationssicherheit ist die oberste Regel.

Die IT-Gremien der Universität Münster haben die Durchführung eines Security-Audits befürwortet, das ZIV hat dazu ein entsprechendes interaktives Programm entwickelt und wird das Security-Audit-Verfahren nun unter dem Namen ISIDOR einführen.

Da das IV-Umfeld an der Universität nicht unmittelbar mit dem von Industriebetrieben, sonstigen Unternehmen oder Behörden zu vergleichen ist, konnte nicht auf kommerzielle Produkte zurückgegriffen werden. Vielmehr wurde ein eigenes Programm vom ZIV entwickelt, um diesen Besonderheiten der Universität gerecht zu werden. Außerdem sind viele Informationen bzgl. des Netzes der Universität (z. B. geräteseitige Netzanschlüsse, Datenendgeräte und deren Standorte) in der bestehenden Netzdatenbank LANbase bereits vorgehalten und es bot sich an, das Security-Audit auf den vorhandenen Informationen aufzusetzen.

Im Folgenden wird das Security-Audit näher vorgestellt.

Umfeld

Die Westf. Wilhelms-Universität Münster und das Universitätsklinikum haben zurzeit ca. 18.600 Endgeräte (Arbeitsplatzrechner, Server, usw., ohne Systeme des ZIV), die an das Netz angeschlossen sind. Dazu kommen noch einige 10.000 Rechner von Studierenden und Bediensteten, die von zu Hause aus auf das Netz zugreifen. Dabei lässt sich die Informationsverarbeitung in diesem Netz nicht mit der in anderen Institutionen oder Industriebetrieben vergleichen; die Systeme sind in höchstem Maße heterogen, es handelt sich um ein gewachsenes, zergliedertes Netz mit einzelnen mehr oder weniger abgeschlossenen, selbstständigen Segmenten. Insgesamt unterteilt sich die Universität in ca. 450 mehr oder weniger eigenständige Einrichtungen. Die einzelnen Einrichtungen befinden sich nicht an einem zentralen Standort, sondern sind auf insgesamt 250 Gebäude der Universität über die gesamte Stadt verstreut, wodurch größere Strecken durch Verkabelung zu überwinden sind. Dadurch sind die Integrität und Vertraulichkeit der Daten gefährdet und entsprechende Maßnahmen z. B. bzgl. der Abhörsicherheit vorzunehmen. Außerdem besteht die Gefahr, dass durch Bauarbeiten Verkabelungen beschädigt werden und somit die Verfügbarkeit von Daten und Diensten beeinträchtigt wird. Um einen Zugriff auf das Universitätsnetz auch standortunabhängig anbieten zu können, z. B. bei Veranstaltungen, Vorlesungen usw., werden die über Funk-LAN erreichbaren Gebiete immer weiter ausgebaut. Dieses Angebot bringt jedoch eine Einbuße an Sicherheit bzgl. der Vertraulichkeit der Daten mit sich, auf die mit entsprechenden Verschlüsselungsverfahren reagiert werden muss.

Das Datenmaterial innerhalb der Universität unterliegt unter Umständen strengsten Vertraulichkeitsanforderungen. Forschungsergebnisse, die mit hohem finanziellem und persönlichem Aufwand erstellt wurden, Patientendaten, Prüfungskataloge oder -ergebnisse verdeutlichen die Bedeutung der Integrität und Vertraulichkeit des Datenmaterials. Niemand mag sich die Folgen ausmalen, wenn aufgrund einer Datenmanipulation die Einträge für Medikation oder Bestrahlungszeit eines Patienten in der Datenbank nicht korrekt sind. Um das Datenmaterial zu schützen, ist es im industriellen Umfeld möglich, Zugriffe auf das Netz weitgehend zu unterbinden. Für eine Universität besteht jedoch teilweise in viel größerem Maße die Notwendigkeit, im Rahmen der Informationsvermittlung Zugriffe von außen zu ermöglichen. Dabei wird der Zugang zum Netz sehr unterschiedlichen Personengruppen gewährt und auch die Zeiten der Nutzung lassen sich nicht an bestimmte Geschäftszeiten koppeln, d. h. Daten und Dienste müssen u. U. 24 Stunden am Tag zur Verfügung stehen. Durch die genannten Beispiele und Erläuterungen wird deutlich, dass ein Universitätsnetz besonderen Gefährdungen ausgesetzt ist, denen entsprechend begegnet werden muss.

Gefährdungspotential

Datenendgeräte und Daten sind vielen Gefährdungen ausgesetzt, die sich nach BSI (Bundesamt für Sicherheit in der Informationstechnik) in folgende Kategorien untergliedern lassen:

Höhere Gewalt

Hierunter sind alle Gefährdungen zu verstehen, die unvorhersehbar sind und nicht direkt beeinflusst werden können. Aktuelles Beispiel ist die gerade vorbeigezogene Grippewelle, die eine Vielzahl von Mitarbeitern vorübergehend aus dem Arbeitsalltag herausgezogen hat. Aber auch Witterungsverhältnisse, wie Blitzeinschlag, starker Sturm oder Regen, die die Infrastruktur des Netzes beschädigen können, zählen zu den Gefährdungen durch höhere Gewalt.

Organisatorische Mängel

Zu den organisatorischen Mängeln zählen fehlende Regelungen, die klare Zuständigkeiten und Vorgehensweisen definieren. So kann es zu unangemessenen Ausfällen kommen, wenn z. B. Ersatzteile nicht beschafft, notwendige Bestellungen nicht aufgegeben oder Reparaturen nicht ausgeführt werden. In diese Kategorie fällt auch die Vergabe von Berechtigungen: Wer darf z. B. auf welche Daten zugreifen und diese bearbeiten. Eine allgemeine Freigabe könnte gravierende Folgen haben. Ein weiteres Beispiel ist die Regelung zur Lagerung von Datenträgern. Die besten Sicherheitskopien sind wertlos, wenn die Datenträger nicht an einem vereinbarten Ort gelagert werden und bei Bedarf auffindbar sind.

Menschliche Fehlhandlungen

Dieser Bereich zählt zu den größten Gefährdungen. Dabei handelt es sich in den meisten Fällen nicht um absichtlichen Schaden, der angerichtet wird, sondern die Nutzerinnen und Nutzer handeln nach bestem Wissen und Gewissen. Zum Beispiel fiel in einem Rechenzentrum immer zur gleichen Tageszeit ein bestimmter Server aus. Die gesamte Hard- und Software wurde überprüft, aber kein Fehler konnte gefunden werden – bis schließlich herauskam, dass die Raumpflegerin den Stecker aus der Steckdose zog, um den Staubsauger anzuschließen. Oder: Passworte dienen der Sicherheit und bieten einen guten Schutz, wenn sie entsprechend der Sicherheitsrichtlinien gewählt werden. Wenn aber das Passwort offen auf dem Schreibtisch liegt, erfüllt es nicht seinen Zweck.

Technisches Versagen

Auch die Technik ist nicht unfehlbar. Wenn es zu Ausfällen oder Fehlfunktionen der Geräte kommt, ist damit auch eine Gefährdung verbunden und es kann z. B. zu Störungen der Verfügbarkeit der Daten und Dienste kommen. Hierzu ist z. B. ein Ausfall der Stromversorgung zu rechnen, der von Seiten der Anbieter oder durch einen Defekt der Leitungen verursacht worden sein kann. Aber auch Softwarefehler in IV-Systemen sind dazuzurechnen, die den laufenden Betrieb stören können.

Vorsätzliche Handlungen

Hierunter werden gezielte Handlungen verstanden, die dazu dienen, unbefugt in Systeme einzudringen, diese zu zerstören oder zu stehlen, z. B. Denial-of-Service-Attacken, die darauf abzielen, Funktionen von Internetrechnern zum Ausfall zu bringen. Der Angreifer Überlastet z. B. gezielt einen Mail-Empfänger und bringt ihn damit zum Absturz. In diesem Zusammenhang sind auch Viren, Würmer usw. zu nennen. Allein im Dezember letzten Jahres wurden 800.000 virenverseuchte Mails auf den Mail-Servern des ZIV registriert. Jedoch auch Einbrüche in Räume, um teure Geräte zu entwenden oder zu zerstören, gehören zu dieser Gefährdungsgruppe.

Bei der Auflistung handelt es sich nur um eine Grobeinteilung, die Beispiele sind nur einzelne unter unendlich vielen Gefährdungen. Es soll lediglich verdeutlicht werden, wie viele verschiedene Gesichter die Gefährdungen haben können. Es wird nicht möglich sein, sich vor allen Gefährdungen zu schützen aber es ist wichtig und wird in Zukunft noch wichtiger werden, wirksame Vorkehrungen zu treffen, um die IV sicherer zu machen.

Zielsetzung

Das Ziel des Security-Audits ist die Feststellung des Schutzbedarfs aller untersuchten IT-Systeme, der vorhandenen Sicherheitsvorkehrungen und der Sicherheitsdefizite mit dem übergeordneten Ziel, Grundlagen für die Einführung weitergehender Sicherheitsmaßnahmen zu ermitteln und letztendlich eine Anhebung des IV-Sicherheitsniveaus zu bewirken.

Als Nebeneffekt wird erwartet, dass den Nutzerinnen und Nutzern zu den einzelnen Themenbereichen Informationen zur Sicherheitstechnik vermittelt werden können. Beim Durchlesen der Antworten wird deutlich, welche Möglichkeiten der Absicherung bestehen und welchem Sicherheitsstand der Ist-Zustand entspricht.

Außerdem werden die Nutzerinnen und Nutzer für sicherheitsrelevante Aspekte sensibilisiert. Über die Darstellung der Konsequenzen, die eine Verletzung der Integrität, Vertraulichkeit oder Verfügbarkeit der Daten und Dienste nach sich ziehen würde, wird ihnen die Notwendigkeit von Sicherheitsvorkehrungen vor Augen geführt und an Beispielen verdeutlicht.

Vorgehensweise

Das Security-Audit wird mittels Web-Seiten, die Fragenkataloge aufzeigen, durchgeführt. Zu jeder Frage werden fünf Antworten zur Auswahl angeboten. Die Nutzerin oder der Nutzer wählt die Antwort, die am ehesten den Ist-Zustand beschreibt. Die Antworten werden in einer Datenbank vorgehalten, damit langfristige Entwicklungen bzgl. der IV-Sicherheit zu verfolgen sind.

Ermittlung des Schutzbedarfs

Für jedes Datenendgerät wird zunächst der Schutzbedarf ermittelt, d. h. die Wertigkeit und Wichtigkeit der Daten und Dienste, die über das Datenendgerät erreichbar sind, werden festgestellt. Dabei wird unterschieden zwischen Integrität und Vertraulichkeit der Daten und Verfügbarkeit der Daten und Dienste.

Im Einzelnen bedeutet das, dass von der Nutzerin oder dem Nutzer das Ausmaß der Folgeschäden anzugeben ist, das eine Verletzung der Integrität oder Vertraulichkeit der Daten zur Folge hätte oder das sich ergäbe, wenn Daten und Dienste nicht zur Verfügung stünden. Es werden zu jeder Frage fünf Antwortmöglichkeiten zur Auswahl angeboten, in denen die Konsequenzen stichwortartig dargestellt sind und von denen die am ehesten zutreffende ausgewählt werden kann.

Der Fragenkatalog zur Ermittlung des Schutzbedarfs gliedert sich in folgende sechs Abschnitte (nach BSI):

- Verstoß gegen Gesetze und Vorschriften/Verträge
- Beeinträchtigung des informationellen Selbstbestimmungsrechts

- Beeinträchtigung der persönlichen Unversehrtheit
- Negative Außenwirkung
- Finanzielle Auswirkungen
- Beeinträchtigung der Aufgabenerfüllung

Nach der Auswertung der Antworten steht für das Datenendgerät der Schutzbedarf hinsichtlich der Aspekte Vertraulichkeit und Integrität der Daten als auch hinsichtlich der Verfügbarkeit der Daten und Dienste fest. Insgesamt wurden folgende fünf Schutzbedarfskategorien festgelegt:

Schutzbedarfskategorie: „Keine“
(0%, keine Folgeschäden)
Schäden haben keine Beeinträchtigung der Institution zur Folge.

Schutzbedarfskategorie: „Niedrig“
(25%, geringe Folgeschäden)
Schäden haben nur eine unwesentliche Beeinträchtigung der Institution zur Folge.

Schutzbedarfskategorie: „Mittel“
(50%, mittlere Folgeschäden)
Schäden haben Beeinträchtigungen der Institution zur Folge.

Schutzbedarfskategorie: „Hoch“
(75%, hohe Folgeschäden)
Im Schadensfall tritt Handlungsunfähigkeit wichtiger Bereiche der Institution ein; Schäden haben erhebliche Beeinträchtigungen der Institution selbst oder betroffener Dritter zur Folge.

Schutzbedarfskategorie: „Sehr hoch“
(100%, sehr große Folgeschäden)
Der Ausfall der IV führt zum totalen Zusammenbruch der Institution oder hat schwerwiegende Folgen für breite gesellschaftliche oder wirtschaftliche Bereiche. Es besteht Gefahr für Leib und Leben von Personen.

Ermittlung der Sicherheitsvorkehrungen

In Abhängigkeit vom ermittelten Schutzbedarf für Integrität/Vertraulichkeit der Daten bzw. für Verfügbarkeit der Daten und Dienste werden nun automatisch Fragenkataloge zusammengestellt, die die Sicherheitsvorkehrungen bei dem Datenendgerät und dessen Umfeld ermitteln.

Im Einzelnen handelt es sich dabei um Fragenkataloge zu

- dem Datenendgerät,
- dem geräteseitigen Netzanschluss (z. B. Netzadapter),
- dem netzseitigen Anschluss (z. B. Anschlussdose),
- der zugeordneten Netzzone und
- dem Raum, in dem sich das Datenendgerät befindet.

Je höher der Schutzbedarf eines Datenendgerätes ist, umso ausführlicher werden Fragen gestellt, um den Status der Sicherheitsvorkehrungen festzustellen.

Zu jeder Frage werden fünf Antwortmöglichkeiten in Stichworten dargestellt, von denen die am ehesten den Ist-Zustand beschreibende von der Nutzerin oder dem Nutzer ausgewählt werden kann. Jede Antwort entspricht einem bestimmten Sicherheitsniveau. Aus der Gesamtheit der Antworten wird für jeden einzelnen der o. g. Fragenkataloge ein Index für den Stand der Sicherheitsvorkehrungen berechnet. Wie beim Schutzbedarf wird auch hier unterschieden zwischen Maßnahmen zur Sicherung der Integrität und Vertraulichkeit der Daten und Maßnahmen zur Sicherung der Verfügbarkeit der Daten und Dienste, um später zielgerichteter entsprechende weitergehende Sicherheitsmaßnahmen einleiten zu können. Bei dem Datenendgerät, dem geräteseitigen und netzseitigen An-

schluss, der Netzzone und dem Raum gibt es damit eine Beurteilung, welchem von den im Folgenden aufgeführten Zustände die jeweiligen Sicherheitsmaßnahmen entsprechen:

- Es wurden keine Sicherheitsvorkehrungen getroffen (0%),
- Es wurden geringe Sicherheitsvorkehrungen getroffen (25%),
- Es wurden wichtige Sicherheitsvorkehrungen getroffen (50%),
- Es wurden weit reichende Sicherheitsvorkehrungen getroffen (75%) oder
- Es wurden umfassende, durchgreifende Sicherheitsvorkehrungen getroffen (100%).

Der Status der Sicherheitsvorkehrungen wird jeweils für Integrität und Vertraulichkeit der Daten und Verfügbarkeit der Daten und Dienste ermittelt.

Hilfen zur Bearbeitungserleichterung

Die Bearbeitung der Fragenkataloge des Security-Audits kann je nach ermitteltem Schutzbedarf größeren Arbeitsaufwand bedeuten. Da viele Datenendgeräte sowohl weit gehend gleichartigen Schutzbedarf haben als auch weit gehend gleichartigen Sicherheitsvorkehrungen unterliegen, gibt es Hilfsfunktionen, um eine einfachere und schnellere Bearbeitung der Fragenkataloge zu ermöglichen.

Kopierfunktion

Als Beispiel soll hier der CIP-Pool genannt werden. Es existieren mehrere Datenendgeräte, die sowohl von der Ausstattung als auch von der Funktion gleichwertig sind. Damit die Fragenkataloge nicht für jedes Datenendgerät einzeln beantwortet werden müssen, besteht die Möglichkeit, bereits bearbeitete Fragenkataloge für andere Datenendgeräte zu kopieren.

Antwortmuster

Ähnlich wie bei der Kopierfunktion können bei der Nutzung von Antwortmustern Fragenkataloge automatisch bearbeitet werden. Bei dieser Funktion werden bestimmte Antwortmuster definiert und stehen daraufhin zur Verfügung, um in die Fragenkataloge ausgewählter Datenendgeräte oder zu deren Umfeldern kopiert zu werden.

Graphische Darstellung und statistische Auswertungen

Zur Ermittlung, ob die Sicherheitsvorkehrungen bei einem Datenendgerät und dessen Umfeld ausreichend sind, wird der Schutzbedarf des Datenendgerätes dem Status der Sicherheitsvorkehrungen für das Datenendgerät und dessen Umfeld gegenübergestellt. Liegt der Status der Sicherheitsvorkehrungen oberhalb des Schutzbedarfs, so sind ausreichende Sicherheitsmaßnahmen getroffen worden, um das Datenendgerät und die Daten und Dienste zu schützen. Ist der Status der Sicherheitsvorkehrungen geringer als der ermittelte Schutzbedarf des Datenendgerätes, so besteht Handlungsbedarf; die Sicherheitsvorkehrungen sollten ausgeweitet werden, um das Datenendgerät ausreichend zu schützen.

Das erste Security-Audit-Verfahren liefert somit eine erste grobe „pauschale“ Bewertung, die für eine erste Sichtung ausreichend erscheint, eine genauere Analyse ist aber notwendig, da einzelne Aspekte trotz eines pauschal positiven Vergleichs ungenügend sein können.

Die Ergebnisse der bearbeiteten Fragenkataloge werden direkt nach dem Datenbankeintrag graphisch dargestellt. Es wird aufgezeigt, wie hoch der Schutzbedarf des Datenendgerätes ist, wie hoch der Status der Sicherheitsvorkehrungen ist und ob die getroffenen Sicherheitsvorkehrungen pauschal betrachtet ausreichend sind.

Um übersichtliche Ergebnisse zu Gruppen von Datenendgeräten zu erhalten, werden zusätzlich verschiedene statistische Auswertungen vorgenommen. So ist es möglich, einen Überblick über den Schutzbedarf und die Sicherheitsvorkehrungen der Datenendgeräte und deren Umfelder eines Institutes oder eines gesamten IV-Versorgungsbereiches zu erhalten.

Fortlaufende Bestandsaufnahme

Die Sicherheit der IV ist kein statischer Faktor, sondern unterliegt einer ständigen Veränderung. Alle mit der IV zusammenhängenden Komponenten werden immer komplexer und damit häufig auch immer anfälliger. Außerdem verbessern auch Angreifer permanent ihr Wissen und erarbeiten sich neue Methoden, um z. B. in IV-Systeme einzudringen. Es ist daher unumgänglich, ein Security-Audit laufend zu aktualisieren, um den neuesten Stand zu erfassen, denn was gestern noch aktuell war, ist bei der rasanten Entwicklungsgeschwindigkeit der EDV heute schon häufig veraltet. In diesem Sinne ist das vorgestellte Online-Security-Audit-Verfahren auf Nachhaltigkeit ausgelegt, indem neue Fragenversionen erstellt werden können, um die Fragenkataloge zu aktualisieren und der jeweiligen Entwicklung anzupassen. Dabei bleiben ältere Fragenversionen bestehen, um Tendenzen aufzeigen zu können.

Organisation

Die Abwicklung des Security-Audits erfolgt über NIC_online. Die Ergebnisse werden in der Netzdatenbank LANbase vorgehalten und setzen auf den bereits bestehenden Datenbankinhalten auf. Das Security-Audit richtet sich zunächst an die Technisch Verantwortlichen. Die Bearbeitung der Fragenkataloge kann jedoch an befugte Dritte, die von den Technisch Verantwortlichen benannt werden, delegiert werden. Zurzeit laufen Tests im eigenen Haus und mit Pilotnutzern außerhalb. In Abhängigkeit von den Ergebnissen dieser Testphase wird das Security-Audit voraussichtlich Anfang Mai 2005 angeboten werden. Die erste Durchführungsphase sollte am 31. Juli 2005 abgeschlossen sein.

Fazit

Diese oben beschriebene Vorgehensweise ist auf Dauer sicherlich nicht in allen Fällen ausreichend und muss in Zukunft verfeinert werden; für das erste Security-Audit-Verfahren an der Universität liefern diese Ergebnisse aber erstmals Indikatoren, die für die weitere Vorgehensweise richtungsweisenden Charakter, z. B. für die Prioritätensetzung, haben können.

Auf den ersten Blick mag die Einführung eines Security-Audits ausschließlich als eine zusätzliche Belastung zu den täglichen Anforderungen am Arbeitsplatz der IV-Verantwortlichen und ihrer Beauftragten (Technisch Verantwortliche für vernetzte IV-Systeme, Mitarbeiter der IV-Versorgungseinheiten) erscheinen. Langfristig jedoch stellt die ständige Überprüfung des Sicherheitsniveaus eine Notwendigkeit dar, die nicht zu umgehen ist. Die Verhinderung möglicher Schäden hat erste Priorität. Die Auswirkungen eines Eindringens von Seiten Unbefugter in ein IV-System könnten größten Schaden nach sich ziehen. Würde vertrauliches Datenmaterial bekannt, so wäre dem Ansehen der Universität geschadet und wie bereits oben angeführt kann ein unbefugtes Eindringen in das IV-System u.U. lebensbedrohliche Gefährdungen nach sich ziehen.

Übrigens, wenn Sie wissen wollen, warum das Audit-Verfahren Isidor heißt, fragen Sie doch die Suchmaschine Ihrer Wahl!

Netzseitige IT-Sicherheitsmaßnahmen des ZIV
Strukturierung, Virtuelle Firewalls, Intrusion-Prevention und VPN

G. Richter

Netzseitige Maßnahmen zur IV-Sicherheit 2004/2005

Das Zentrum für Informationsverarbeitung hat im Auftrag der Universität und des Universitätsklinikums Münster seine Bemühungen intensiviert, durch netzseitige Maßnahmen die Gefährdung der Informationsverarbeitung, ihrer Verarbeitungsprozesse, IT-Systeme und Daten zu verringern und damit die direkten und indirekten Aufwendungen für eingetretene Schäden zu reduzieren. Insbesondere wurden zum Ende des Jahres 2004 nach längerer Vorbereitungszeit Beschaffungen durchgeführt, die möglichst zügig 2005 umgesetzt werden sollen. Konzeptionell sind diese Maßnahmen selbstverständlich nur ein Teil der Gesamtmaßnahmen – Maßnahmen auf den IT-Endgeräten selbst, organisa-

torischen Maßnahmen, Ausbildungsmaßnahmen usw. wird in der Gesamtheit ein noch größeres Gewicht zugeordnet. Netzseitige Maßnahmen erlauben jedoch in wichtigen Fällen und gezielt für wichtige Bereiche, das Gefährdungspotential auch dann zu begrenzen, wenn lokale, organisatorische und sonstige Maßnahmen nicht ausreichend umgesetzt werden konnten. In bestimmten Fällen können auch nur netzseitige Maßnahmen Schutz bieten, z. B. zur Abwehr bestimmter Denial-of-Service-Angriffe.

Grundstrukturen für netzseitige Sicherheitsmaßnahmen

Grundgedanke des Systems der netzseitigen Sicherheitsmaßnahmen ist die „Einbettung von Sicherheitsfunktionen in ein strukturiertes Netz". Grundelemente sind hierbei

- ein **strukturiertes Netz mit Netzzonen**, die den Kommunikations- und Sicherheitsbedürfnissen der Teilnehmersysteme mit ihren Anwendungen und Daten entsprechen. Diese Strukturierung ist mitunter ein wechselseitiger Prozess: Zur Optimierung der Sicherheit bei gleichzeitig möglichst geringer Beschränkung der erforderlichen Kommunikationsmöglichkeiten muss zum einen
  - Einfluss auf die Verteilung der Anwendungen und Daten auf IT-Systeme (Server, Proxies, Clients) genommen werden und zum anderen muss
  - eine Verteilung der IT-Systeme auf geeignet zu definierende Netzzonen (Subnetze, VLANs, usw.), welchen zonenspezifische Sicherheitsfunktionen (z. B. Paketfilter, Firewalls) zugeordnet sind, durchgeführt werden.
- **Hierarchisierung der Netzzonen:** Erlaubt übergeordnete Netzzonen, auch mehrstufig, zu bilden. Gesamtheiten von Netzzonen können so entsprechend den Bedürfnissen ganzheitlich gegenüber anderen übergeordneten Netzzonen sicherheitstechnisch definiert und betrieben werden. Eine solche Strukturierung entspricht den vorhandenen IV-Strukturen, die häufig auch vielstufig ausgeprägt sind.
- die **Einbettung von Sicherheitsfunktionen in das Netz**: Es sollte längst ohne Frage Allgemeingut sein, dass „die Firewall" im Sinne eines „Border Defense Gateway am Netz-Perimeter" für größere Netzen als alleinige netzseitige Maßnahmen ziemlich unzureichend ist. Vielmehr sind alle netzseitigen Sicherheitsmaßnahmen möglichst überall dort im Netz, wo eine sicherheitstechnische Abgrenzung eines informationsverarbeitenden Bereiches gegenüber anderen Bereichen erwünscht scheint, zu integrieren. Damit werden Verbände von Netzzonen aufgebaut, die nicht nur nach außen geschützt sind, sondern denen auch für überschaubare Bereiche innerhalb eines Zonenverbundes gleichermaßen Sicherheitsfunktionen bereitgestellt werden können.

Die Herausforderung an die IV- und Netzplaner besteht nun darin, unter Maßgabe der technischen Möglichkeiten und der verfügbaren finanziellen und personellen Ressourcen eine optimierte Struktur aus Netzzonen mit Sicherheitsfunktionen an Übergängen aufzubauen.

Sicherheitsfunktionen im Netz

Netzseitig können hier folgende Sicherheitsfunktionen eingesetzt werden:

- **Stateless-Packet-Screening**, insbesondere auf den Layer-3-Switches (Routern), kontrolliert die Konnektivität im Wesentlichen auf der Basis von Kommunikationsquellen und -zielen (IP-Adressen und logische Interfaces von Routern) sowie bestimmter höherer Protokollmerkmale (Anwendungsprotokolltypen, d. h. z. B. TCP-/UDP-Ports, und einige weitere Protokollelemente). Diese Methode bietet sich kostengünstig und hochperformant überall dort an, wo die mit Zugangskontrolllisten in Routern (ACLs, Access Control Lists) erreichbare Grundsicherheit ausreichend ist oder wo hoher Durchsatz als vorrangig betrachtet werden muss. Hier kann in Zusammenhang mit besonderen Zonen, in denen Applikation-Gateways mit Sicherheitsfunktionen (Application-Proxies, auch Terminal-Server, Web- und FTP-Server mit Sicherheitsfunktionen, usw.) installiert werden, bereits eine sehr hohe Sicherheit erreicht werden, ohne dass besondere Kosten anfallen würden, da moderne Router meistens dazu geeignet sind und ohnehin Bestandteil der Netze sind. Ein Einsatz sol-

cher Funktionen ist technisch praktisch immer möglich, erfordert allerdings auch einen Verwaltungsaufwand, der nicht zu unterschätzen ist.

- **Firewalls** im Sinne eines **Stateful-Packet-Screening** unter Berücksichtigung portagiler Protokolle (wie z. B. FTP, SIP, H.323). Die Möglichkeiten sind hier sicherheitstechnisch den Möglichkeiten der Router deutlich überlegen, da die Blockierung unerwünschter Konnektivität sitzungsbezogen (Flow-basiert) ist. Auch sind die Möglichkeiten des Reportings wesentlich umfangreicher und detaillierter. Hier kann wie bei den Stateless-Paket-Filtern eine noch weitergehende Sicherheitsqualität im Zusammenhang mit besonderen Zonen für Applikations-Gateways (quasi DMZs, „Demilitarisierte Zonen“) erreicht werden. Nachteil solcher Firewalls sind die vergleichsweise geringen Durchsatzmöglichkeiten, die weit hinter den Möglichkeiten von Routern zurückbleiben. Deshalb können solche Systeme nur dann eingesetzt werden, wenn die Durchsatzbeschränkungen unkritisch sind oder wenn die Erhöhung der Sicherheit gegenüber den ACL-basierten Funktionen Vorrang hat vor der Performance. Gleichzeitig muss der Kostenaufwand betrachtet werden; leistungsfähige Firewalls beruhen stets auf spezieller und damit vergleichsweise teurer Hardware und Software. Dies gilt insbesondere für monolithische Firewall-Systeme, die gleichzeitig auch Applikation-Gateways und zum Teil auch VPN- und Intrusion-Prevention-Funktionen (s. u.) integrieren.

- **Application-Gateways** oder Application-Proxies können auf der Ebene von Anwendungsprotokollen und unter Berücksichtigung der Inhalte für besondere Sicherheitsfunktionalitäten sorgen (z. B. Mail-Relays bzw. SMTP-Gateways mit Virenschutzfunktionen oder entsprechende Systeme für HTTP, d. h. Web-Proxies, FTP usw.; auch Terminal-Server können hier eine ausgezeichnete Funktion als Übergangsmöglichkeit in fremde Netzbereiche einnehmen). Solche Funktionalitäten sind in der Regel durch die Verantwortlichen bereitzustellen, die auch sonst für den Bereich der IV-Anwendungen verantwortlich sind (z. B. Systemadministratoren) und können nicht im Sinne eigentlicher netzseitiger Sicherheitsmaßnahmen betrachtet werden. Netzseitig ist hier jedoch für die Abstimmung und entsprechende Bereitstellung von Netzzonen („DMZ“) zu sorgen.

- **Intrusion-Detection- und -Prevention**-Systeme (IPS) analysieren Datenströme und können Dateneinheiten oder Flows aufgrund bestimmter maliziöser Datenmuster (Signaturen), Verhaltensanomalien oder Kombinationen beider Merkmale automatisch erkennen und blockieren. Damit können Angriffe abgewehrt werden, die zum Teil über hostbasierte Abwehrmöglichkeiten hinausgehen; die Abwehr kann häufig frühzeitiger erfolgen, d. h. insbesondere bevor weite Infrastrukturbereiche in Mitleidenschaft gezogen wurden. Sogenannte Zero-Day-Attacken, also bisher unbekannte Angriffstypen, können oft erkannt und abgewehrt werden. Auch können Denial-of-Service(DoS)-Angriffe, die von den betroffenen Systemen kaum selbst beherrscht werden können, abgewehrt werden.

- Sicherer Zugang zu Netzzonen durch verschlüsselte Tunnel mit Hilfe der **VPN-Technologie** ermöglicht den kontrollierten Zugang (authentifiziert, unter Autorisierungsüberwachung) zu Ressourcen auch in geschützten Bereichen.

Virtualisierung als Voraussetzung

Eine bedarfsweise Einbettung der genannten Sicherheitsfunktionen in ein unter Sicherheitsgesichtspunkten strukturiertes Netz unterliegt stets drei wichtigen Gesichtspunkten, die mitunter untrennbar miteinander verbunden sind:

- der technologischen Machbarkeit,
- der Finanzierbarkeit und
- der Administrierbarkeit.

Die technologische Machbarkeit und die Finanzierbarkeit würden sehr schnell an ihre Grenzen stoßen, wenn Netzstrukturen und funktionale Instanzen 1:1 physisch auf das Netzinventar abgebildet werden müssten. Eine hierarchische Netzstruktur mit einer Viel-

zahl den einzelnen Netzzonen zugeordneter Geräte (Switches, Routern, Firewalls, IPS usw.) ist kaum vorstellbar und auch wohl nur in wenigen Fällen jemals durchgängig realisiert worden. Selbst Kabelwege müssten in solchen Szenarien im schlimmsten Fall gesondert für die einzelnen Netzzonen errichtet werden. Die Administration einer Vielzahl von Firewalls in einem solchen Netz, das auch noch anforderungsgerecht betrieben werden soll, ist für Netzverantwortliche ein Schreckensszenario.

Ein Weg aus diesem Dilemma ist Virtualisierung:

- Durch **Virtuelle LANs** (VLANs), eine bewährte Layer-2-Netztechnologie[1], können Netzzonen gebildet werden, ohne dass dabei jedes Mal Kabelwege speziell geschaffen werden müssten. Die Zusammenfassung von Arbeitsplätzen in einer gemeinsamen Netzzone gelingt so auch über größere Entfernungen hinweg, gebäudeübergreifend und weitgehend beliebig für jeden einzelnen Arbeitsplatz.
- Durch **Virtualisierung von Routern**, eine relativ junge Layer-3-Technologie[2], können flexibel auch relativ komplexe Netztopologien aufgebaut werden, die den jeweiligen sicherheitstechnischen Strukturierungsanforderungen entsprechen, ohne dass gleich bei neuen Zonenstrukturen neue (physische) Router beschafft werden müssten. Vielmehr kann heute ein einzelner physischer Switch ohne besondere weitere Kosten in mehrere „virtuelle Router“ aufgeteilt werden. Im Zusammenhang mit der VLAN-Technologie kann im Grundsatz so jede beliebige Topologie mit den gewünschten hierarchischen Sicherheitszonen aufgebaut werden. Ein Seiteneffekt dieses Ansatzes ist neben der Kostenersparnis, insbesondere durch bessere Ausnutzung von Geräten, eine Konzentration auf weniger Geräte und damit verbesserte Möglichkeiten der Betriebsführung.
- Ebenfalls recht neu sind die Möglichkeiten der **Virtualisierung von Firewalls** und der **Virtualisierung von Intrusion-Prevention-Systemen**. Entsprechend kann eine größere Zahl an Instanzen solcher Sicherheitselemente auf der Basis einer geringen Anzahl leistungsfähiger Geräte an beliebiger Stelle in das Netz „eingebettet“ werden.
- VPN-Technologie (in engerem Sinne) erlaubt seit langem die Ausdehnung einer Netzzone (meistens als „Intranet“ deklariert) über so genannte Tunnel auf externe Netze (Sites) oder Arbeitsplätze (Clients). Einschränkungen gibt es bei sehr vielen Produkten hinsichtlich der Möglichkeit, mit einem VPN-System den Zugang zu verschiedenen Ziel-Netzzonen unter Beachtung der Sicherheit zu ermöglichen. Die Unterstützung von VPN-Clients und -Sites im Rahmen des vorgestellten Zonenkonzeptes macht es notwendig, dass VPN-Systeme VLANs unter spezieller Berücksichtigung des Routings unterstützen, so dass **virtuelle multiple VPN-Zugangsmöglichkeiten** entstehen. Entsprechende Produkte sind heute erhältlich, wobei aber kaum ein Produkt allen Wünschen gerecht wird. Besonderes Augenmerk muss hier auf die Sicherheit angeschlossener Clients gerichtet werden, so dass die durch VPN erreichten Netzzonen nicht über unsichere Clients mit neuen Sicherheitsrisiken belastet werden.

Zentrale und dezentrale Administrationsfähigkeit

In dem vorgestellten Konzept wird die Rolle zentraler und dezentraler IV-Strukturen abgebildet, wobei das Netz als einheitliche Infrastruktur für alle durch das Zentrum für Informationsverarbeitung bereitgestellt wird und in dieser Form Grundvoraussetzung für die korrekte Funktion des Zonenkonzeptes ist. Netzseitig eingebettete Sicherheitsfunktionen sind unter diesem Gesichtspunkt zunächst kritisch zu betrachten,

- da netzseitig und damit zentral Funktionen bereitgestellt werden, die in engstem Zusammenhang mit den spezifischen Regelungen der dezentralen IV bis hin zu kleinsten Teilbereichen zu sehen sind.

1 Layer-2-Technologie beinhaltet die Technologie Lokaler Rechnernetze (LANs, z. B. Ethernet) und die Technologie, die zur unmittelbaren Kopplung von LANs dient (Switches mit sog. Bridging-Funktion).

2 Layer-3-Technologie sorgt für die Weiterleitung und Vermittlung (Routing) von Informationen über die Grenzen verschiedener Layer-2-Netze (z. B. LANs) hinweg, lokal und global, von Endgerät zu Endgerät.

- Andererseits können in das Netz eingebettete Sicherheitsfunktionen so massiv in die Ende-zu-Ende-Kommunikation eingreifen, dass die Netzbetriebsführung als zentrale Aufgabe mit flächendeckendem Charakter illusorisch würde, wenn eine uneingeschränkte dezentrale Administration der eingebetteten Sicherheitsfunktionen ermöglicht würde.

Einige Firewall- und Intrusion-Prevention-Produkte kommen heute dieser Problemstellung entgegen:

- **Mandantenfähigkeit** erlaubt selbstständige Konfiguration der Sicherheitsfunktionen und des spezifischen Reporting für die zugeordneten virtuellen Ressourcen **durch die jeweiligen Netzzonenverantwortlichen**.
- Rahmenkonfigurationsmöglichkeiten und andere **Generalfunktionen für die Netzverantwortlichen** erlauben dagegen die Vorgabe von Muster-, Standard- und Mindestkonfigurationen zur Unterstützung der Zonenverantwortlichen und die Gewährleistung der Netzmindestfunktionalitäten sowie eine allgemeine Reporting- und Eingriffsmöglichkeit.

Für die besprochenen Netzbasisfunktionen Virtuelle LANs und Virtuelle Router mit den Stateless-Packet-Screening-Funktionen ist Mandantenfähigkeit nicht als Teil eines Produktes erhältlich. Hier muss die **Self-Care-Funktionalität der Netzdatenbank** des Zentrums für Informationsverarbeitung im Rahmen einer Netzzonenverwaltung ausgebaut und mit Geräte-Steuerungsmechanismen verbunden werden; dies ist eine der vorrangigen Entwicklungsnotwendigkeiten 2005.

Vergleichbares gilt für die Administration der Client-VPN-Zugangsmöglichkeiten. Hier ist eine Anpassung des zzt. vorhandenen **Identitätsmanagements (Nutzerdatenbank) für personenbezogene Authentifizierung und Autorisierung** beim netzzonenspezifischen Zugang notwendig.

Maßnahmenkatalog 2005

Anfang 2005 sind folgende Systeme wie beschrieben vorhanden:

- Mehrere so genannte Switching-Engines für Backbone-Router, so dass virtuelle Routing-Instanzen möglich sind. Durchsatz 400 Mio. Pakete/s, 720 GBit/s.
- Redundantes virtuelles Firewall-System mit 5,5 GBit/s Durchsatz.
- Redundantes virtuelles Intrusion-Prevention-System mit 2 GBit/s Durchsatz.
- Redundantes virtuelles VPN-System (3DES-Verschlüsselung) mit 1,9 GBit/s Durchsatz.

Die 2005 durchzuführenden Maßnahmen werden entsprechend sein

- eine intensivierte Umsetzung des heute schon in Teilen von Universität (z. B. Universitätsverwaltung) und Universitätsklinikum (z. B. IT-Zentrum) etablierten Zonenkonzeptes,
- die Einführung von Firewall-Instanzen für übergeordnete Netzzonen (z. B. IV-Versorgungsbereiche) und auch wichtige bzw. dringliche untergeordnete Netzzonen,
- die Einführung von Intrusion-Prevention-Instanzen zunächst für große übergeordnete Netzzonen wie z. B. Gesamtuniversität, Universitätsklinikum, WLAN- und andere Remote-Access-Bereiche,
- die „sanfte“ Ablösung der bisherigen PPTP basierten VPN-Zugänge und die Integration in die, soweit schon vorhandenen, Netzzonen.

Bei höherem Durchsatzbedarf können die Beschaffungen auch unter Kostengesichtspunkten verhältnismäßig leicht erweitert werden, da die Systeme bis auf das Intrusion-Prevention-System auf Modultechnik basieren.

Begleitet werden müssen diese Maßnahmen durch die schon erwähnten

- Entwicklungsarbeiten im Bereich der Nutzer- und der Netzdatenbanken und die
- Ausbildung auch der Netzzonenverantwortlichen für die Anwendung und Verwaltung der eingebetteten Sicherheitsinstanzen.
- Entsprechend den Erfahrungen müssen voraussichtlich Reporting-Mechanismen genauer bewertet und zusammen geführt werden.

Nicht abschließend gelöst ist zzt. die Frage nach der Client-Sicherheit bei VPN-Tunneln, die 2005 einer weiter gehenden Lösung zugeführt werden soll. Es gilt aber als sicher, dass die an der Universität Münster umfangreich eingesetzten Client-Sicherheitsprodukte durch den Hersteller der VPN-Systeme grundsätzlich unterstützt werden; VPN-Tunnel können dabei nur zu Clients aufgebaut werden können, auf denen bestimmte Sicherheitsmaßnahmen durchgeführt worden sind. Die Zielplanung des Herstellers sieht vor, dass diese Funktionalität auf dem bei uns eingesetzten Produkt Mitte 2005 zur Verfügung stehen soll.

Weiteres

Nicht Gegenstand der Betrachtung hier waren netzseitige Sicherheitsmaßnahmen, die der unmittelbaren Erhöhung der Verfügbarkeit der IV-Systeme und des Netzes selbst dienen und als Dauerthema mit den Aspekten Redundanz und Geräteerneuerung allein schon ein sehr belastendes Arbeitsfeld sind.

Ein weiteres wichtiges Arbeitsfeld sind Fragen des Zugriffsschutzes für LAN und WLAN, die mit standardisierten Methoden (z. B. IEEE 802.1x) und unter Berücksichtigung des Zonenkonzeptes (z. B. mit dynamischer VLAN-Zuordnung bei Verbindungsaufnahme) beantwortet werden sollen. Auch hier wurden Beschaffungen im vierten Quartal 2004 durchgeführt (Edge-Switches, WLAN-Access-Points für IEEE 802.11i), die entsprechende Möglichkeiten bieten.

Insgesamt dürfte die Client-Sicherheit durch Viren-Scanner, Personal-Firewall, Host-Intrusion-Prevention unter Verwendung eines Policy-Enforcement in Kopplung mit Netzkomponenten eine wichtige Rolle spielen.

Begleitend soll das für das zweite Quartal 2005 geplante erste Security-Audit-Verfahren genauere Kenntnisse über Schutzbedarf, Sicherheitsanforderungen und Defizite in den Sicherheitsvorkehrungen bringen und unter anderem Hilfestellung bei der Netzstrukturierung geben.

Es soll noch einmal betont werden, dass in dem oben dargestellten Konzept die Content-basierten Sicherheitsfunktionen weitestgehend in entsprechenden Applikation-Gateways bzw. -Proxies realisiert und durch die Anwendungsverantwortlichen und Serverbetreiber, dezentral und zentral nach Bedarf, betreut werden sollen. Entsprechende Funktionalitäten sind im Grundsatz beispielsweise schon in den zentralen Mail-Servern realisiert, Terminal-Server werden in der Universitätsverwaltung und im UKM mit Sicherheitsfunktionalität eingesetzt. Das ZIV hat weiter gehende Evaluationen, z. B. für HTTP-Gateways mit Sicherheitsfunktionen begonnen und wird dies aktiv weiter betreiben, aber auch die dezentralen Einrichtungen können hier mitwirken.

Zum Abschluss

IV-Sicherheit ist eine kooperative Aufgabe: Ohne die Einbeziehung und aktive Einbringung aller Beteiligten – Nutzer, technisch und leitende Verantwortliche in den Einrichtungen, zentrale und dezentrale IV-Versorgungseinrichtungen – kann Sicherheit in der Informationsverarbeitung nicht ausreichend gelingen. Dieser Leitgedanke gilt auch vor dem Hintergrund der eingeleiteten netzseitigen Maßnahmen:

- Der Aufbau eines unter Sicherheitsgesichtspunkten strukturierten Netzes setzt voraus, dass sich die vor Ort zuständigen Personen in diesen Prozess aktiv und konstruktiv, ja sogar kreativ und schließlich konsequent einbringen, um im Widerstreit unterschiedlicher Interessen und Ziele der Nutzer, z. B. hinsichtlich Flexibilität des Arbeitsplatzes und der wirtschaftlichen und sicheren IV-Versorgung aller, diesen umfangreichen Prozess erfolgreich voran zu bringen und nachhaltig weiter zu führen.

- Gleiches gilt für die Ausgestaltung der Sicherheitsfunktionen, z. B. für die Definition der Zugangssteuerungsregeln, die in entspreche Zugangskontrolllisten (z. B. ACLs, s. o.) umzusetzen sind.
- Die vorgestellte Mandantenfähigkeit einiger Sicherheitskomponenten und die beabsichtigten Self-Care-Mechanismen für die Netzdatenbank sind zunächst nur Instrumente, die erst durch die aktive Nutzung durch die zuständigen „Mandanten“ zum Leben erweckt werden.
- Auch das begleitende Security-Audit-Verfahren, das als Online-Instrument eine unmittelbare Erfassung durch die für IT-Endgeräte zuständigen Personen ermöglicht, ist nicht denkbar ohne den Einsatz der zuständigen Personen.

Das ZIV will die hier notwendigen Prozesse unterstützen und so einfach wie möglich gestalten. Es wird jederzeit beraten und notwendige Projekte gemeinsam mit den IV-Verantwortlichen durchführen. Der Arbeitsaufwand seitens des ZIV ist dabei so, dass große Teile der Abteilung Kommunikationssysteme damit gebunden sind, ganz unabhängig von dem Aufwand für Systemintegration und -betrieb. Es verbleibt aber unabwendbar ein nicht unerheblicher Arbeitsaufwand auf Seiten der übrigen Beteiligten.

Mit dem „Instrument“ der/des Technisch Verantwortlichen für vernetzte IV-Systeme, wie sie/er in einer Regelung der Universität vom 8.6.2004 definiert ist und schon seit langer Zeit faktisch existiert, müsste die Umsetzung gelingen. Technisch Verantwortliche haben die notwendige Nähe zu den IV-Nutzern vor Ort, den Leitern ihrer Einrichtung und zu den IV-Versorgungseinheiten. Auf den Schultern dieser Technisch Verantwortlichen wird also ein großer Teil der Arbeitslast getragen werden müssen. Leitungen und Arbeitsgruppen der IV-Versorgungseinheiten können und sollten koordinierend und unterstützend wirken.

Dass es sich lohnt an der Umsetzung des Netzzonenkonzeptes mitzuarbeiten, kann man an schon durchgeführten Projekten erkennen. In der Universitätsverwaltung ist die Zahl der Sicherheitsvorfälle nach Einführung einer stringenten Zonenstruktur und Zugangssteuerung auf wenige Fälle gesunken, die auf andere Wege als über das Netz zurückzuführen waren. Auch in Teilen des Universitätsklinikums, in denen die Konzeption umgesetzt wurde, konnte mit diesem Ansatz die Sicherheit erhöht werden. Mit der Einführung neuer Sicherheitsfunktionen im Jahre 2005, wie oben dargestellt, dürfte der Aufwand noch besser gerechtfertigt sein und die Motivation hoffentlich verstärkt werden können.

ZIV-Lehre

Veranstaltungen in der Vorlesungszeit (Sommersemester 2005) für Hörer aller Fachbereiche

Beratung zum Lehrangebot durch Herrn W. Bosse jeweils Di, Do 11-12, ✆ 83-31561

Für alle Veranstaltungen ist eine frühzeitige Online-Anmeldung erforderlich. Für den Dialog sollte dabei vorzugsweise auf die dort angebotene verschlüsselte (abhörsichere) Datenübertragung umgeschaltet werden. Anmeldungen zu den Veranstaltungen sind ab 1. März 2005 möglich.

260109	Programmieren in Java Mittwoch 13-15 Uhr Hörsaal: M4, Einsteinstr. 64, Beginn: 20.04.2005	Mersch, R.
260113	Dynamische Webseiten mit PHP und MySQL Donnerstag 9-11 Uhr Hörsaal: M4, Einsteinstr. 64, Beginn: 21.04.2005	Sturm, E.
260128	Statistische Datenanalyse mit dem Programmsystem SPSS Donnerstag 11-13 Uhr Hörsaal: ZIV-Pool 3, Einsteinstr. 60, Beginn: 21.04.2005	Nienhaus, R.
260132	Kolloquium des Zentrums für Informationsverarbeitung Freitag 14-16 Uhr Hörsaal: Raum 206, Röntgenstr. 9-13	Held, W.

Kommentare zu den Veranstaltungen

260109 Programmieren in Java

Java ist eine objektorientierte Programmiersprache, die inzwischen weltweit große Verbreitung gefunden hat und sich weiterhin dynamisch entwickelt. Sie basiert auf dem Konzept einer virtuellen Maschine, die es ermöglicht, Anwendungen für unterschiedliche Plattformen ohne Neuübersetzung zu entwickeln, und verfügt über eine sehr umfangreiche Klassenbibliothek, die ständig erweitert wird. Grundkenntnisse in Java sind für die Softwareentwicklung in vielen Bereichen unbedingt erforderlich.

Die Vorlesung bietet eine Einführung in die objektorientierte Programmierung anhand von Java. Sie ist auch für Hörer/innen ohne Vorkenntnisse im Programmieren geeignet.

260113 Dynamische Webseiten mit PHP und MySQL

Diese Veranstaltung kann als Fortsetzung von „Erstellen von dynamischen Webseiten mit PHP“ angesehen werden. Kenntnisse von HTML und CSS sowie Grundkenntnisse von PHP werden vorausgesetzt. Großen Raum wird die Vorstellung der Datenbank MySQL einnehmen, weitere Themen sind Sitzungsverwaltung, Up- und Download sowie XML.

260128 Statistische Datenanalyse mit dem Programmsystem SPSS

Das statistische Programmsystem SPSS (Statistical Package for the Social Sciences) wird in dieser Veranstaltung in der neuesten deutschsprachigen Version unter Windows vorgestellt und erprobt. Mit diesem System stehen bequem aufzurufende Programme zu den gebräuchlichen univariaten und multivariaten statistischen Verfahren sowie zur Datenaufbereitung zur Verfügung. SPSS wird z. B. zur Auswertung von Fragebögen eingesetzt.

In dieser Veranstaltung wird das programmtechnische Rüstzeug zur Durchführung derartiger Auswertungen vermittelt. Solide Grundkenntnisse bezüglich der anzusprechenden statistischen Verfahren sowie Kenntnisse der Anwendungsmöglichkeiten dieser Verfahren im jeweiligen Fachgebiet sind erwünscht und bei den praktischen Übungen von großem Nutzen.

260132 Kolloquium des Zentrums für Informationsverarbeitung

Im Rahmen des Kolloquiums werden Vorträge über aktuelle Themen der Informationsverarbeitung gehalten. Vortragstermine werden im WWW und durch Aushang bekanntgegeben.

ZIV-Regularia

Fingerprints

R. Perske

Unter dieser Rubrik erscheinen regelmäßig die aktuellen kryptographischen Prüfsummen der öffentlichen Schlüssel, die von der WWUCA und vom ZIV verwendet werden.

Bei E-Mails, WWW-Servern und an vielen anderen Stellen wird zunehmend mit Verschlüsselung und elektronischen Unterschriften gearbeitet. Dabei besitzt mindestens einer der Kommunikationspartner (beispielsweise der WWW-Server) einen öffentlichen Schlüssel, der vom anderen Partner (beispielsweise Ihrem WWW-Browser) zum Verschlüsseln oder zum Überprüfen einer elektronischen Unterschrift benutzt wird.

Um zu verhindern, dass Ihnen falsche öffentliche Schlüssel untergeschoben werden, sollten Sie überprüfen, ob der jeweilige Schlüssel tatsächlich zur angegebenen Person bzw. zum angegebenen Server gehört. Zu diesem Zweck sind die Schlüssel häufig mit Zertifikaten versehen, das sind elektronische Beglaubigungen, ausgestellt von sog. Zertifizierungsstellen, in denen die Eigentümerschaft bestätigt wird.

Im Bereich des deutschen Wissenschaftsnetzes erstellen die DFN-PCA als übergeordnete Zertifizierungsinstanz und die WWUCA als Zertifizierungsstelle der Universität Münster solche Zertifikate, siehe http://www.dfn-pca.de und http://www.uni-muenster.de/WWUCA/. Seit Januar 2004 zertifiziert die WWUCA auch RSAv4- und DSS/DH-Schlüssel, die mit Gnu PG, PGP 8 u. Ä. erzeugt wurden.

DFN-PCA und WWUCA unterstützen zwei verschiedene Verschlüsselungs- und Zertifizierungssysteme: Die PGP-Familie (Pretty Good Privacy), zu der auch GnuPG (Gnu Privacy Guard) gehört, wird meistens bei E-Mail eingesetzt. Die X.509-Familie wird beispielsweise bei abhörsicheren WWW-Servern, bei S/MIME und bei Object Signing verwendet.

Zum Überprüfen der von DFN-PCA und WWUCA ausgestellten Zertifikate benötigen Sie deren öffentliche Schlüssel. Diese finden Sie auf `http://www.unimuenster.de/WWUCA/zertifikate.html` (X.509 und PGP) oder auch an anderen Stellen wie beispielsweise der perMail-Titelseite http://permail.uni-muenster.de (nur X.509), der ZIVprint-Einstiegsseite `http://www.unimmuenster.de/ZIV/zivprint.html` (nur X.509) oder der ZIV-Mitarbeiterliste `http://www.uni-muenster.de/ZIV/Mitarbeiter/` (nur PGP).

Die Fingerabdrücke (Fingerprints) dieser Schlüssel sind nachfolgend abgedruckt, damit Sie beim Aktivieren der Schlüssel auf Ihrem Rechner kontrollieren können, dass Sie tatsächlich die echten Zertifizierungsschlüssel erhalten haben.

PGP-Kommunikationsschlüssel

Da die Zertifizierungsschlüssel ausschließlich zum Zertifizieren verwendet werden, gibt es gesonderte Kommunikationsschlüssel, die Sie bitte verwenden, wenn Sie eine verschlüsselte E-Mail an die jeweilige Zertifizierungsstelle schreiben möchten:

DFN-PCA (2005), ENCRYPTION Key <dfnpca@dfn-pca.de>
DFN-PCA (2005), ENCRYPTION Key <dfnpca@dfn-cert.de>
KeyID: 13813809, Schlüssellänge 2048 Bits, Erstellungsdatum: 2004/11/26
Key fingerprint = 53 C2 37 D6 15 5B CF 88 F3 7D 3F F5 E2 E4 E5 1D

PGP-Zertifizierungsschlüssel der WWUCA

KeyID 38B7A481: Zertifizierungsstelle Universitaet Muenster 2004-2005
2048 Bits, Fingerprint: 973E 0725 040B 1745 F272 180D 08C2 C15A
KeyID BC811EB1: Zertifizierungsstelle Universitaet Muenster 2002-2003
2048 Bits, Fingerprint: 2864 01BC F0EF D5BA D9A0 866C 4379 4C1D
KeyID 313C02F5: Zertifizierungsstelle Universitaet Muenster 2000-2001
2048 Bits, Fingerprint: 3762 F5E0 C278 7697 530F 2DF2 F3B3 27F5
KeyID EF750F1D: Rainer Perske +49(251)83-31582 Certification Key
2048 Bits, Fingerprint: 2F38 6EF8 DC2E D85E 5B35 DB49 8AE4 52AF

PGP-Zertifizierungsschlüssel der DFN-PCA

KeyID FDCB1C33: DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2004-2005)
<http://www.dfn-pca.de/>
2048 Bits, Fingerprint: 96B0 AD7F B8DC 0018 DCA0 7053 1C3B 4DA5
KeyID F2D58DB1: DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2002-2003)
<http://www.dfn-pca.de/>
2048 Bits, Fingerprint: DE31 690D BC6A E779 4DCD A1B5 8180 FE7B
KeyID 63EB5391: DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2001)
<not-for-mail>
2048 Bits, Fingerprint: CFAF 6C29 4E57 4E0E E81C BDB4 54FD 2AAB
KeyID F7E87B9D: DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 1999-2000)
<not-for-mail>
2048 Bits, Fingerprint: 6570 7274 B5E0 3FF0 EA7C ABE4 465F B8B2
KeyID 35DBF565: DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 1997-1998)
<not-for-mail>
2048 Bits, Fingerprint: 097C 0919 D3C3 86DC 7A30 1511 1295 8DE3

X.509-Zertifikate der WWUCA

Inhaber: C=DE, O=Universitaet Muenster,
CN=Zertifizierungsstelle 2004-2005/Email=ca@uni-muenster.de
Aussteller: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA,
CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
Seriennummer: 64774066 (0x3dc5fb2)
MD5-Fingerprint: 2619 6BEF 66B2 7044 52CC BE11 4C5F 3CB8
SHA1-Fingerprint: 1765 AE6D 57C7 7914 D2AF BAF3 439C E139 66E1 A0AE
Inhaber: C=DE, O=Universitaet Muenster,
CN=Zertifizierungsstelle 2002-2003/Email=ca@uni-muenster.de
Aussteller: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA,
CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
Seriennummer: 1774668 (0x1b144c)
MD5-Fingerprint: A431 AD41 D8F2 1856 4E31 CC69 71E6 174F
SHA1-Fingerprint: 6945 20CA 1AFE 5CFA 6C37 52EB B772 B054 90EC D979

X.509-Wurzelzertifikat der DFN-PCA

Inhaber: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA,
CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
Aussteller: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA,
CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
Seriennummer: 1429501 (Ox15cffd)
MD5-Fingerprint: 3E1F 9EE6 4C6E F022 0825 DA91 2308 0503
SHA1-Fingerprint: 8E24 22C6 7E6C 86C8 90DD F69D F5A1 DD11 C4C5 EA81

Alle Angaben zur DFN-PCA ohne Gewähr.

infoRUM Juli 2004

Liebe Leserin, lieber Leser,

wenn Sie **infoRUM** regelmäßig beziehen wollen, bedienen Sie sich bitte des unten angefügten Abschnitts. Hat sich Ihre Adresse geändert oder sind Sie am weiteren Bezug von **infoRUM** nicht mehr interessiert, dann teilen Sie uns dies bitte auf dem vorbereiteten Abschnitt mit.

Bitte haben Sie Verständnis dafür, dass ein Versand außerhalb der Universität nur in begründeten Einzelfällen erfolgen kann.

Vielen Dank!

Redaktion **infoRUM**

☐ Ich bitte um Aufnahme in den Verteiler.

☐ Bitte streichen Sie mich/den nachfolgenden Bezieher aus dem Verteiler.

☐ Mir reicht ein Hinweis per E-Mail nach dem Erscheinen einer neuen WWW-Ausgabe.
Meine E-Mail-Adresse:

_____

An die
Redaktion **infoRUM**
Zentrum für Informationsverarbeitung
Röntgenstr. 9–13
48149 Münster

☐ Meine Anschrift hat sich geändert.
Alte Anschrift:

_____

_____

Absender:

Name: _____

FB: _____ Institut: _____

Straße: _____

E-Mail: _____

Außerhalb der Universität:

_____

(Bitte deutlich lesbar in Druckschrift ausfüllen!)

Ich bin damit einverstanden, dass diese Angaben in der **infoRUM**-Leserdatei gespeichert werden (§ 4 DSG NW).

_____ _____

Ort, Datum Unterschrift