inforum

Zentrum für Informationsverarbeitung der Universität Münster
Jahrgang 28, Nr. 2 – Juli 2004 ISSN 0931-4008

Inhalt

Impressum

infoWWW
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 Auflage: 1400

Editorial

E. Sturm

Wenn man sieht, was die armen Kollegen so treiben, die für ZIV-Cert (die Stelle im ZIV, die sich u. a. um Beschwerden aus dem Internet kümmert) verantwortlich sind, kann man nur zur Meinung gelangen, dass sich hier etwas ändern muss.

These 1: Alles wird noch viel schlimmer!

Immer mehr Viren erwecken einen offiziellen Eindruck und verführen Menschen dazu, eine Mail-Anlage zu öffnen. Jetzt werden schon die ersten Mails gesichtet, die sich als Beschwerde tarnen, dabei aber einen Spam- oder Virenanhang mitbringen. Wenn das noch mehr um sich greift, kann man nur noch der folgenden These zustimmen.

These 2: Beschwerde-E-Mail darf man nicht mehr beantworten!

Da E-Mail beliebig gefälscht werden kann, ist E-Mail keine rechtsgültige Art der Beschwerde. Auf automatisiert verschickte Beschwerden kann man auf Grund der wachsenden Menge nur automatisiert reagieren. Wenn dann aber bei einer Mail, die sich über eine Virenmail beschwert, wieder die originale Mail angehängt wird, wird sie wiederum als Virenmail eingestuft und eine Beschwerde abgeschickt. Damit ist klar, dass eine automatisierte Antwort nur heißen kann: Keine Antwort. Man muss zur Zeit einfach tolerieren, dass ab und zu ein PC von einem Virus befallen ist, da PC-Nutzer das nicht wirklich verhindern können, sondern nur die in der letzten These genannten.

These 3: Nur Bill Gates und Linus Thorwalds können dem Spuk ein Ende bereiten!

Abgesehen von Buffer-Overflows kann man das Hacken von Rechnern nur verhindern, wenn das Betriebssystem sich weigert, ein Programm auszuführen, das nicht explizit installiert wurde. Explizite Installation heißt, dass ein Mensch festlegen muss, wie viel Speicherplatz, relative Rechenzeit und Zugriff auf Verzeichnisse und ins Netz erlaubt sein sollen.

Mit anderen Worten: Erst wenn Viren keine Wirkung mehr haben, werden sie aussterben. Buffer-Overflows wird es natürlich auch weiterhin geben, da die Benutzung der Programmiersprachen C und C++ von niemandem in Frage gestellt wird. (Aber das wäre Stoff für eine vierte These.)

ZIV-Aktuell

Viren, Würmer und kein Ende, dazu noch Spam

W. Held

Die Angriffe gegen die Informationsverarbeitung (IV) in unserer Universität und überall in der Welt sind unerträglich geworden. Allein im April wurden über 2 Mio. Viren von den E-Mail-Servern des ZIV abgefangen, viermal so viele wie in den Vormonaten.

ZIV und IV-Versorgungseinheiten unternehmen in den Netzen und auf den Servern zahlreiche Maßnahmen zum Schutz der IV. Viele Mitarbeiter/innen und Studierende setzen darüber hinaus bereits weitere Mechanismen ein, um ihre Rechner am Arbeitsplatz und zu Haus zu schützen.

Leider werden die Schutz-Möglichkeiten für Arbeitsplatz-Rechner noch nicht überall und von allen genutzt. Und die ungeschützten Systeme werden gehackt und zu weiteren Angriffen in der Universität und in der Welt missbraucht. Dies führt zu großen wirtschaftlichen Schäden und gefährdet den Ruf unserer Hochschule; zeitweise akzeptieren andere Mail-Server keine Mails mehr aus Münster. Jeder IV-Nutzer sollte wissen, dass er andere Rechner und den Informationsfluss in den Rechnernetzen beeinflusst. Um Schaden von sich und anderen abzuwenden, muss man sich daher – wie im Straßenverkehr – an Regeln halten. Diese Regeln ergeben sich u. a. aus Datenschutzgesetzen, Telekommunikationsgesetz, Teledienst-Gesetz und Strafgesetzbuch.

Das Rektorat hat dazu Ende 2003 bereits früher beschlossene Regelungen zur IV-Sicherheit in der Universität Münster ergänzt: „Zur deutlichen Verbesserung der IV-Sicherheit und damit zur möglichst weitreichenden Vermeidung von Schäden in der Universität, wird die Nutzung von IV-Arbeitsplatzsystemen im/am Netz der Universität durch Regelungen und Verpflichtungen, die mit Durchsetzungsrechten und Reglementierungen verbunden sind, abgesichert. Notwendige Maßnahmen werden den technischen Entwicklungen folgend durch das IV-Sicherheitsteam in Abstimmung mit den Informations-Versorgungseinheiten (IVV) und dem ZIV festgelegt und der IV-Kommission zur Kenntnis gebracht. ... Wer den durch das IV-Sicherheitsteam angeordneten Maßnahmen und Verpflichtungen nicht nachkommt, wird nur eingeschränkte Zugänge zum Netz und begrenzte Handlungs- und Nutzungsmöglichkeiten der Ressourcen der Universität erhalten.“

IV-Kommission und IV-Lenkungsausschuss haben diesen Beschluss auf Empfehlung von ZIV und IVVen jetzt weiter konkretisiert:

1. Virenschutz-Software

Die Software (McAfee der Firma NAI) steht zum Einsatz auf dienstlichen und privaten Rechnern, wenn diese auch zum Zugang zur Universität genutzt werden, kostenlos bereit. Sie **soll** eingesetzt und dann automatisch aktualisiert werden. Bis auf weiteres finden Sie auf der ZIV-Homepage (`www.uni-muenster.de/ZIV`) in der Rubrik „Service“ unter dem Stichwort „Sicherheit“, wie Sie diese Software auf ihre Rechner laden und danach automatisch aktualisieren können.

Bitte bleiben Sie aber weiterhin sehr vorsichtig, auch wenn Sie diese Software einsetzen: Keine Virenschutz-Software schützt mit letzter Sicherheit vor manipulierenden Angriffen. Neue Viren-Mechanismen oder geschickte Täuschungsmanöver werden manchmal nicht erkannt oder erst mit einer kleinen Zeitverzögerung wirksam. Maßnahmen, die Sie daher auch mit Virenschutz-Software beachten sollten:

a) Nur Software aus zuverlässiger Quelle ausführen

Jede Viren-Manipulation beruht auf der Ausführung eines unerwünschten Programmstücks. Die Einschätzung der Zuverlässigkeit der Herkunft ist das erste und zuverlässigste Mittel, um sich zu schützen. Grundsätzlich darf nur Software aus zuverlässiger Quelle ausgeführt werden. Für die Fälle, in denen man einer Fehleinschätzung oder Täuschung der Quelle unterliegt, ist dann die Virenschutz-Software da.

b) Konfiguration der Makro-Fähigkeit der verwendeten Software-Produkte

Ausführbar sind nicht nur Programme im eigentlichen Sinne, sondern auch Kommandosequenzen (Makros) in Anwendungsprogrammen. Fast alle größeren Programm-Systeme bieten solche Möglichkeiten und sind damit ein potenzielles Einfallstor für die Viren-Manipulation. Programme wie Word, WordPerfect, StarOffice, Excel, Photoshop usw. gehören dazu. In allen Programmen sollte die automatische Ausführung von Makros unterbunden werden.

2. Personal-Firewall

Auf jedem Rechner **soll** auch eine Personal-Firewall eingesetzt werden. Dazu werden in Kürze weitere Informationen gegeben, denn die angemessene Parametrierung des Produktes der Firma NAI (McAfee, dienstlich oder privat mit Zugang zur Universität; ebenfalls kostenlos nutzbar) wird zzt. noch getestet.

Die in Windows XP standardmäßig implementierte Firewall bietet für die meisten Benutzer auch einen gewissen Schutz. Sie ist ebenfalls ohne Kosten zu aktivieren. Diese Möglichkeit ist schon jetzt zu nutzen.

Sowohl die Virenschutz-Software und ihre Aktualisierung als auch die Personal-Firewall sind nicht sehr speicherintensiv. Sie können selbst über relativ langsame Modem- und ISDN-Verbindungen problemlos geladen und aktuell gehalten werden.

3. Update der Betriebssysteme

Betriebssystem-Updates **sollen** in Zukunft ebenfalls auf allen dienstlichen und privaten Rechnern, wenn man diese auch zum Universitäts-Zugang nutzt, regelmäßig eingespielt werden. Weitere Informationen folgen dazu in Kürze, weil noch einige technische Hilfen vorbereitet werden müssen, damit die Updates auch auf häuslichen Rechnern eingespielt werden können.

Mit den Maßnahmen 1-3 wird der Schutz von Arbeitsplatz-Rechnern bereits deutlich erhöht. Bitte helfen Sie, die vorstehenden Beschlüsse umzusetzen!

Spam-Mail

Eine weitere Plage stellen Spam-Mails dar. Für viele Nutzer/innen machen sie mehr als 90 % der E-Mails aus. Auf den zentralen E-Mail-Servern werden deshalb Spam-Marker eingesetzt, die zzt. allerdings noch nicht individuell eingestellt werden können. Ergänzen Sie diesen zentralen Spam-Marker deshalb unbedingt durch Spam-Marker auf ihrem Rechner am Arbeitsplatz. Teilweise sind diese Marker in der von ihnen eingesetzten Mail-Software (Netscape, Outlook usw.) aktivierbar. Das ZIV stellt alternativ den sehr leistungsfähigen, selbst lernenden Spamfilter bereit, der von Herrn Sturm entwickelt wurde. Er dürfte in vielen Fällen einsetzbar sein. Sie finden Deleatur auf der ZIV-Homepage (`www.uni-muenster.de/ZIV`) in der Rubrik *Service* unter dem Stichwort *ZIV-soft*.

Die/der Technisch Verantwortliche für vernetzte IV-Systeme

W. Held

Das Rektorat hat nach Vorlage der IV-Kommission und des IV-Lenkungsausschusses am 08.06.2004 Regelungen für Technische Verantwortliche (TeVe) beschlossen. Diese beinhalten u. a.:

1. Einrichtungen, die Objekte im Kommunikationssystem betreiben wollen, müssen einen oder mehrere TeVe für vernetzte IV-Systeme sowie einen Vertreter bestellen. Die Bestellung erfolgt in der Regel durch die Leitung der jeweiligen Einrichtung.
2. Die den TeVe zuzuordnenden Objekte sind die zu betreuenden Endgeräte und Zugangseinrichtungen im Kommunikationssystem in allen Formen (Rechner, Drucker oder Laborgeräte mit Netzanschluss, Anschlussdosen bei Festnetzzugängen usw.). Darüber hinaus können dem TeVe übergeordnete Objekte zugeordnet werden, die im Rahmen besonderer Vereinbarungen mit dem ZIV für IV-Leistungen jeglicher

Art definiert werden, um bestimmte quantitative oder qualitative Betriebsgrößen zu erzielen (z.B. Übertragungsqualität oder Verfügbarkeit, Zugangsbeschränkungen oder Verkehrsfilterung aus Sicherheitsgründen).

3. Zum TeVe darf nur bestellt werden, wer in einem Beschäftigungsverhältnis zur Westfälischen Wilhelms-Universität Münster steht und die zur Erfüllung der Aufgaben erforderliche Fachkunde besitzt.
4. Die Einrichtung hat den TeVe bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere die notwendigen Ressourcen zur Verfügung zu stellen. Auch ist sicherzustellen, dass die Aufgaben im Zusammenwirken mit den unmittelbaren Betreibern der Endgeräte wahrgenommen werden können. Als unmittelbare Betreiber gelten zunächst die Administratoren.
5. Der TeVe ist Kontaktperson mit entsprechender technischer Koordinierungsfunktion zwischen dem jeweiligen Betreiber der IV-Systeme einerseits und der Einrichtung und den zentralen sowie dezentralen IV-Einrichtungen andererseits. Der Aufgabenbereich umfasst die notwendigen Verwaltungsfunktionen, die Integration, den Betrieb und die Sicherheit.
6. Der TeVe
   a) führt alle in diesem Kontext entstehenden latenten und akuten Problemstellungen selbst oder unter Inanspruchnahme fachkundiger Hilfe wirksam und zeitgerecht einer Lösung zu,
   b) leitet bei Gefahr im Verzuge die notwendigen Abwehrmaßnahmen umgehend ein und setzt notfalls eigenständig die Gefahrenquelle außer Betrieb,
   c) ist für die Durchführung aller in diesem Kontext entstehenden notwendigen technischen Verwaltungsaufgaben, wie beispielsweise die Dokumentation der Objekte mit technischen Parametern in lokalen und externen Datenbanken, verantwortlich.

Weitere Einzelheiten sind auf der ZIV-Homepage `www.uni-muenster.de/ZIV/` zu finden, dort unter der Rubrik *Service* im Unterteil *Sicherheit* und dann weiter unter *Übersicht über Regelungen zur IV-Sicherheit in der WWU* mit der Überschrift *Die/der Technisch Verantwortliche für vernetzte IV-Systeme*.

Aus der Pressemitteilung des DFN-Vereins vom 15.06.2004

W. Held

e-Science-Initiative gestartet.

Deutschland wird seine Spitzenposition bei den Wissenschaftsnetzen und in der Telekommunikation nutzen, um Vorreiter der Internet-Technik von morgen zu sein. Anlässlich des 20-jährigen Bestehens des Deutschen Forschungsnetzes (DFN) hat Dr. Wolf-Dieter Dudenhausen, Staatssekretär im Bundesministerium für Bildung und Forschung (BMBF), ein neues Projekt zur Entwicklung innovativer Netztechnik gestartet. Ziel von VIOLA (Vertically Integrated Optical Testbed for Large Applications) ist, intelligente Anwendungen für Wissenschaft und Wirtschaft zu erproben. Das mit zehn Millionen Euro vom BMBF geförderte Projekt ist gleichzeitig der Start der von Bundesministerin Bulmahn im März dieses Jahres angekündigten e-Science-Initiative.

Durch e-Science könnten sich Forschungsteams künftig wesentlich einfacher vernetzen und über so genannte „Grids“ (englisch: Gitter, Netz) weltweit auf Supercomputer, wissenschaftliche Daten und Großgeräte wie Radioteleskope oder Teilchenbeschleuniger zugreifen, erläuterte DFN-Vorsitzender Jessen. „Damit wird die Ergiebigkeit der wissenschaftlichen Arbeit signifikant erhöht und durch Synergien können zudem neue Qualitäten erreicht werden“, so Jessen. Die Entwicklung werde zu gravierenden Veränderungen der heute üblichen Kommunikationswege führen, ähnlich wie das World Wide Web die Nutzung des Internets verändert habe.

Staatssekretär Dudenhausen begrüßte die in diesem Zusammenhang von Expertinnen und Experten aus Wissenschaft und Wirtschaft (D-GRID-Initiative) erarbeiteten Konzepte für eine deutsche e-Science-Infrastruktur. Sie stelle zugleich ein Testfeld für das Internet der Zukunft dar, bei dem ebenfalls der Zugriff auf das weltweite Wissen und auf verteilte Ressourcen im Vordergrund stehe. e-Science ist damit ein wesentlicher Beitrag zur Innovationspolitik in Deutschland.

Einzelheiten zu den Programmen kann man im ZIV erfahren.

Preissenkung für uni@home plus

W. Held

Für den Dienst **uni@home plus**, den das ZIV für Studierende und Bedienstete zur Einwahl von häuslichen Computern in das Universitätsnetz erbringt, hat die Deutsche Telekom auf ihren Leitungen die Preise um knapp 20 % gesenkt. Ab April 2004 geben wir diesen Nachlass an die Nutzer von **uni@home plus** weiter:

Bereich	**Neuer Preis**	**Bisheriger Preis**
City	0,77 Cent/Min	0,91 Cent/Min
Region 50	1,29 Cent/Min	1,54 Cent/Min

Die übrigen Kostenanteile (Grundgebühr, Sondergebühren beim fehlgeschlagenem Lastschrifteinzug oder für die Ausfertigung einer schriftlichen Rechnung) bleiben unverändert. Ausführliche Hinweise zu **uni@home plus** findet man unter der Homepage des ZIV (`www.uni-muenster.de/ZIV/`).

ZIV-Pools im ZIV täglich rund um die Uhr zugänglich

W. Held

Die ZIV-Pools (Computer-Pools) im Erdgeschoss des ZIV in der Einsteinstraße 60 sind seit dem 15.05.2004 täglich (auch samstags, sonntags und an Feiertagen) 24 Stunden lang nutzbar.

Dazu muss man für 5 € einen elektronischen Schlüssel erwerben, mit dem man die Eingangstür öffnen kann. Für Nutzer, die keinen elektronischen Schlüssel haben, sind die Rechner nur noch eingeschränkter als bisher nutzbar, nämlich montags bis freitags von 7.30–17.30 Uhr.

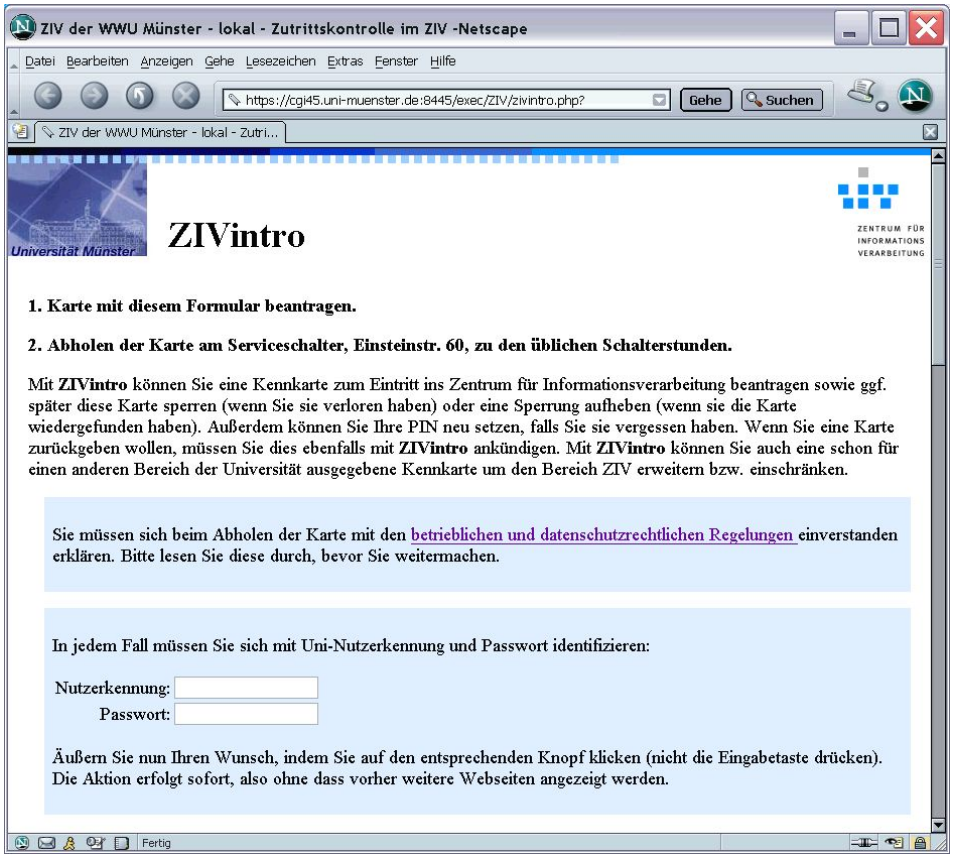
Wie man einen elektronischen Schlüssel erhält und welche Modalitäten bei seiner Nutzung zu beachten sind, findet man auf der Homepage des ZIV unter **ZIVintro** und auf Aushängen in der Einsteinstraße 60.

ZIVintro - Schlüsselkarten fürs ZIV

von E. Sturm

Seit Mitte Mai sind ZIV-Pools rund um die Uhr geöffnet. Per Webinterface kann man Schlüsselkarten beantragen.

Wie im Artikel "ZIV-Pools im ZIV täglich rund um die Uhr zugänglich" in diesem infoWWW vorgestellt, kann man jetzt auch außerhalb der Öffnungszeiten des ZIV sowie samstags, sonntags und an Feiertagen den ZIV-Pool im Erdgeschoss der Einsteinstr. 60 nutzen, sofern man eine Schlüsselkarte besitzt. Eine solche kann man auf der ZIVintro-Webseite beantragen, zu der man von der ZIV-Startseite aus gelangt:



In der oben stehenden Bildschirm-Abbildung sehen Sie schon die Dinge, auf die es ankommt:

- Sie sollten sich die „betrieblichen und datenschutzrechtlichen Regelungen“ anschauen, da Sie diese beim Abholen der Schlüsselkarte unterschreiben müssen.
- Sie identifizieren sich per Kennung und Passwort schon im Internet, weil dies am Serviceschalter nicht gut möglich ist.

Es folgen auf der Webseite Abschnitte, die es Ihnen erlauben, die gewünschten Funktionen aufzurufen.

Zugang

Im ersten Abschnitt geben Sie noch zweimal Ihre Anfangs-PIN ein und können dann Ihre Karte beantragen. Nach Klicken auf den entsprechenden Knopf bekommen Sie gesagt, dass Sie Ihre Karte am Serviceschalter abholen können und dabei 5 € und einen Zettel mit Ihrer Kennung in Druckbuchstaben (nicht Ihrem Passwort) mitbringen sollen. Dies sollte wirklich nicht per Zuruf geschehen, bei der Eingabe der Kennung darf kein Fehler passieren. Die PIN wird übrigens bis zur Übergabe der Karte verschlüsselt in einer Datenbank des ZIV gespeichert, nach der Übergabe befindet sie sich nur noch im Schließsystem selbst.

Erweiterung

Sollten Sie schon eine Schlüsselkarte aus einem anderen Bereich der Universität besitzen, so können Sie diese um den ZIV-Pool erweitern. Jeder bekommt also nur eine Karte für alle Schließbereiche der Uni. Auch hierzu ist nur die Eingabe von Kennung und Passwort erforderlich. Allerdings müssen Sie sich auch in diesem Fall ins ZIV bemühen, um die oben erwähnte Erklärung zu unterschreiben. Erst dann wird Ihre Karte für das ZIV zugelassen.

Sperrung

Mit Kennung und Passwort können Sie Ihre Karte sperren, falls sie Ihnen etwa in Australien gestohlen wurde. Sollten Sie sie dann doch wiederfinden, so bietet das ZIVintro-Webinterface auch die Möglichkeit, die Sperrung wieder aufzuheben.

PIN-Änderung

Sie können jederzeit eine neue PIN eingeben, wenn Sie die Schlüsselkarte erst einmal besitzen. Sie brauchen die alte PIN nicht zu kennen, Uni-Nutzerkennung und Passwort reichen zur Authentifizierung aus.

Kündigung

Wenn Sie die Schlüsselkarte nicht mehr benötigen, sollten Sie sie kündigen, damit Ihre Daten sofort aus der Datenbank gelöscht werden und nicht erst, wenn das ZIV davon benachrichtigt wird, dass Ihre Nutzerkennung abgelaufen ist.

Benutzung

Noch ein paar Hinweise zur Benutzung:

- Wenn Sie abends oder am Wochenende den ZIV-Pool nutzen wollen, müssen Sie die Vereinzelungsanlage links von der Haupteingangstür wählen. Der zugehörige Kartenleser befindet sich am Pfahl auf der linken Seite. Der Leser auf der rechten Seite des Pfahls ist für die Haupteingangstür zuständig.
- Nachdem Sie die Karte kurz vor den Leser gehalten haben, werden Sie zur PIN-Eingabe aufgefordert. Nehmen Sie jetzt die Karte in die andere Hand, damit Sie bei der PIN-Eingabe nicht dauernd wieder die Karte an den Leser halten und wieder entfernen. Dies wäre nämlich die einfachste Art, eine ungültige PIN einzugeben. Nach vier ungültigen PINs ist eine Karte für diesen Tag gesperrt.
- Die Vereinzelungsanlage ist auf 40 kg Körpergewicht eingestellt. (Sollten Sie weniger wiegen, bemühen Sie sich bitte ins nächst gelegene Taucherfachgeschäft.)
- Tagsüber sollten Sie die Schlüsselkarte nicht benutzen – und wenn doch, dann sowohl für das Betreten als auch für das Verlassen, damit Sie in der Anwesenheitsliste nicht noch für die ganze Nacht als anwesend geführt werden.
- Sollten Sie im Pool nach 17 Uhr von der Nachricht überrascht werden, dass Ihr Rechner heruntergefahren wird, weil Sie nicht angemeldet seien, brauchen Sie nicht in Panik zu verfallen. Vor dem Pool finden Sie an der Wand einen extra gekennzeichneten Kartenleser, den Sie (ohne das Haus verlassen zu müssen) zur Anmeldung nutzen können.

Nur indirekt mit der Schlüsselkarte zu tun hat eine weitere Maßnahme: Zur Vermeidung von Missbrauch wird pro Schlüsselkarte nur eine Windowssitzung erlaubt.

Wie vertrauenswürdig sind E-Mails?

St. Ost

Zeitnah zur Europa-Wahl 2004 wurden Spam-Mails rechtsradikalen Inhalts verschickt. Die angeblichen Absender wussten davon nichts und haben unter der Rufschädigung zu leiden.

Will man sich veranschaulichen, wie vertrauenswürdig und authentisch der E-Mail-Verkehr ist, so kann man als Analogie den Brief der ehemals gelben Post heranziehen. Jeder kann, ohne sich auszuweisen, einen Brief beliebigen Inhalts in einen Briefkasten stecken. Die Post verifiziert den Absender nicht, verlangt nicht einmal, dass ein solcher angegeben ist. Der Brief wird zugestellt, es sei denn, er ist nicht zustellbar oder es geht eine erkennbare Gefahr (z. B. Briefbombe) von dem Brief aus. Ist er nicht zustellbar, so geht er zurück an den Absender. Wir schätzen einen Brief als echt ein, wenn wir den Absender kennen und der Inhalt zu dem passt, was wir vom Absender erwarten. Jeder würde misstrauisch werden, wenn ihm die Stadtwerke Kontoauszüge seines Giro-Kontos zuschickten.

Aktuelle Spam-Viren variieren den Inhalt von Mail-Adressbüchern, die sie auf den von ihnen infizierten Rechnern finden, zu fantasievollen realen und ausgedachten Adressen, die sie dann beliebig als Absender oder Adresse verwenden. Manchmal tragen Sie zusätzlich als absendenden Rechner den Mail-Server ein, mit dem sie als erstes in Kontakt treten. Die besseren Viren versuchen zusätzlich auch die Mail-Received-Zeilen im Mail-Header zu ändern, was ihnen allerdings nicht vollständig gelingt. Wir haben versucht, dieses Problem im Zusammenhang mit der Benachrichtigung über Viren-Mail zu beschreiben, siehe

`http://www.uni-muenster.de/ZIV/Hinweise/EMailVirusBericht.html`

Was können Sie selbst tun? Leider wenig. Wenn in ihrem Namen Mail verschickt wird, so kann das niemand verhindern. Wenn Sie Mail erhalten, so halten Sie diese bitte nicht deshalb schon für echt, bloß weil sie Ihnen ein Rechner geschickt hat. Wenn ihnen E-Mail im oben beschriebenen Sinne als nicht plausibel erscheint, dann ist sie eben nicht echt und sie kann ignoriert werden.

Wenn Sie Mail als eindeutig von Ihnen kommend verifizierbar machen wollen, müssen Sie sie mit kryptografischen Methoden signieren. Damit ist dann auch sichergestellt, dass niemand den Inhalt der Mail verändert hat. Wenn die Mail zusätzlich auch nicht von Fremden gelesen werden soll, so muss sie zusätzlich verschlüsselt werden. Leider sind diese Hinweise nur eingeschränkt nützlich, denn die flächendeckende Infrastruktur, Signaturen verifizierbar zu machen, fehlt fast vollständig.

Sicheres Mail-Lesen von POP-Servern

St. Ost

„Secure POP“ ermöglicht verschlüsselte Mail-Übertragung.

Der Artikel wendet sich **ausschließlich** an alle, die bislang den Dienst `POP.UNI-MUENSTER.DE` zum Lesen (nicht zum Versenden!) ihrer Mail verwendet haben. Einige Mail-Programme nennen diese Funktion auch „Server für eingehende Mail“.

Der gravierende Nachteil des bisherigen Verfahrens besteht in der unverschlüsselten Datenübertragung zwischen POP-Server und ihrem Mail-Programm. Dabei sind nicht nur die Mail-Inhalte unverschlüsselt, sondern auch die Nutzer-Kennungen und ihre Passwörter.

Das ZIV bietet den POP-Dienst jetzt auch in einer verschlüsselten Variante an. In Ihrem Mail-Programm können Sie einstellen, ob die Datenübertragung verschlüsselt wird oder nicht. Bitte nutzen Sie die Möglichkeit des verschlüsselten Mail-Lesens! Es ist ein weiterer Schritt, die Datenverarbeitung insgesamt ein wenig sicherer zu machen.

Einstellung der Mail-Programme für verschlüsseltes Mail-Lesen

Generell gilt: Um die Verschlüsselung einzuschalten, verändern Sie die Eigenschaften ihres schon **existierenden** Mail-Kontos. Es ist nicht nötig, ein neues Konto anzulegen. Geändert werden müssen die Attribute:

Attribut	Alter Wert	Neuer Wert
Verschlüsselungsart	..keine..	SSL
Port	110	995

Der Server-Name `pop.uni-muenster.de` bleibt in jedem Fall unverändert.

Leider ist die Art und Weise, wie diese Einstellung vorgenommen wird, stark vom Mail-Programm abhängig. Lesen Sie bitte auf unserer Webseite

`http://lostws.uni-muenster.de/~ost/SecurePOP/Secure-POP.html`

wie dies zu geschehen hat. Erläutert wird das Vorgehen für die populärsten Mail-Programme an Hand von Screenshots. Zur Anwendung kamen dabei die jeweils aktuellsten

Programm-Versionen. Die Bildschirminhalte älterer Versionen können im Detail verschieden zu unseren Screenshots sein, aber das grundsätzliche Vorgehen wird übereinstimmen.

Gehirnwäsche

K. Tormählen, Uni Hamburg

Verborgene Informationen in Word-Dokumenten

Hinter den Kulissen eines Word-Dokumentes verbergen sich standardmäßig Informationen, die man möglicherweise bei der Weitergabe des Dokuments nicht offen legen möchte. Bei der Verschlüsselung des Textes werden intern die Angaben aus dem Register *Benutzerinformationen* des Dialogfeldes *Optionen* abgelegt. Zu den nicht sichtbaren Inhalten gehören aber auch verborgene (ausgeblendete) Texte, Kommentare und im Überarbeitungsmodus gelöschte Passagen. Ferner werden der Name der Dokumentvorlage, Textmarken, die beim ersten Speichern aktuelle Versionsnummer von Word sowie Ordnerangaben bei verknüpften Objekten im Dokument abgelegt. Ungewünschte Inhalte können auch durch die Schnellspeicherung (*Extras*, *Optionen*, *Speichern*, *Schnellspeicherung zulassen*) entstehen, da bei dieser Methode alte Inhalte nicht gelöscht, sondern nur unkenntlich gemacht werden. Das Aufzeichnen mehrerer Versionen speichert ggf. ebenfalls unerwünschte Informationen (*Datei*, *Version* bzw. *Versionen*). Bei mehreren Bearbeitern können entsprechende Namen, E-Mail-Adressen, Firmen- und Computernamen gespeichert sein.

Will man ein Dokument auf verborgene Inhalte überprüfen, so kann man es mit einem normalen Editor (z. B. *Notepad*) oder einem Hex-Editor (z. B. *Hex-Editor MX*, zu erhalten über `http://www.nextsoft.de`) öffnen. Normale Editoren zeigen möglicherweise nicht alles an (hängt von der internen Art der Verschlüsselung ab). Dabei ist zu bedenken, dass von Word manche Angaben, wie z. B. Textmarken, mit Leertasten oder anderen kryptischen Symbolen zwischen den einzelnen Zeichen abgelegt wurden.

Zum Vermeiden der Ablage von unerwünschten Inhalten in Word-Dokumenten gibt es mehrere Möglichkeiten:

- Ab Word-Version 2002: Option *Persönliche Informationen beim Speichern aus dieser Datei entfernen* im Register *Sicherheit* des Dialogfeldes *Optionen* setzen (zu erreichen auch über *Extras*, *Sicherheitsoptionen* im Dialogfeld *Speichern unter*).
- Angaben im Register *Benutzerinformationen* des Dialogfeldes *Optionen* entfernen.
- Angaben im Register *Zusammenfassung* des Dialogfeldes *dateiname Eigenschaften* (wobei *dateiname* der Name des Dokuments ist) entfernen (*Datei*, *Eigenschaften*).
- Kommentare entfernen (Symbolleiste *Überarbeiten*, *Kommentare löschen*).
- Änderungen entfernen (alte Versionen: *Extras*, *Änderungen verfolgen*, *Änderungen akzeptieren* oder *ablehnen*; neue Versionen: Symbolleiste *Überarbeiten* und entsprechende Einträge in den Menüs).
- Versionsaufzeichnungen entfernen (*Datei*, *Version* bzw. *Versionen*).
- Den gesamten Inhalt eines Dokuments kopieren und in ein neues einfügen.
- Den gesamten Inhalt eines Dokuments mit einem Editor in eine TXT-Datei kopieren.
- Datei als PDF-File speichern (behält i. Allg. Informationen über den Autor und das Speicherdatum).
- Datei als RTF speichern (behält Informationen über Autor, Bearbeiter, Speicherdatum und alle Elemente, die zur Word-Bearbeitungstechnik gehören, wie Textmarken und Kommentare).

Das Microsoft-Tool *Remove Hidden Data*

Für die Versionen Word 2002 und 2003 stellt Microsoft seit Anfang 2004 ein Tool zur Verfügung, mit dem persönliche Daten aus einem Dokument entfernt werden können. Das Tool heißt *Remove Hidden Data* und läuft nur unter Windows XP. Der Download kann über `http://www.microsoft.com/downloads` und dann mit der Suche des Keywords *Remove Hidden Data* erfolgen. Die Installationsdatei heißt `rhdtool.exe`. Die Installation erfolgt als Administrator durch Ausführen. Nach der Installation findet sich im Menü *Datei* der Eintrag *Remove Hidden Data...* Nach dem Aktivieren startet ein Assistent, der u. a. einen Dateinamen für die bereinigte Fassung abfragt. Bei kritischen Inhalten wird ggf. eine Abfrage eingeblendet, die das Erhalten oder Löschen ermöglicht. Außerdem erscheint eine Warnung, dass ein erneutes Öffnen und Speichern wieder persönliche Daten ablegt. Zum Bereinigen ist dann ein weiterer Durchlauf mit dem Tool notwendig. Zu beachten ist, dass die Berichtsdateien mit Namen `rhd`*x*`.log` (*x* ist die laufende Nummer) standardmäßig im Ordner *Dokumente und Einstellungen\profil\Lokale Einstellungen \Temp* (*profil* ist das entsprechende Profil) abgelegt werden.

Software Update Service (SUS) am ZIV

O. Winkelmann

Automatisches Windows Update mit SUS

Um seinen Windows-PC vor den Gefahren des Internet zu schützen, man denke nur an Sasser & Co., ist es unbedingt notwendig neue Sicherheitsupdates sofort nach Erscheinen einzuspielen. Mit dem *Windows-Update*-Mechanismus lassen sich Windows-Betriebssysteme einfach auf dem neuesten Stand halten. Alle neuen Updates werden bei diesem Verfahren direkt von dafür vorgesehenen Microsoft-Servern heruntergeladen. Mit SUS bietet Microsoft die Möglichkeit, einen eigenen Update-Server im Netz zu betreiben. Ein SUS-Server stellt alle notwendigen Updates und Service Packs für Windows-Betriebssysteme (Windows 2000, XP und 2003) im lokalen Rechnernetz bereit, die dann automatisch von den Windows-Rechnern abgeholt werden können. Dieses Verfahren bietet den Vorteil einer sicheren Versorgung mit Updates, die auch dann funktioniert, wenn die Internetverbindungen gestört sind. Die Microsoft-Update-Server waren in der Vergangenheit aufgrund starker Wurm-Attacken schon wiederholt überlastet und nicht erreichbar.

Das ZIV betreibt seit einiger Zeit einen zentralen SUS-Server, der für alle Windows-Rechner im Universitätsnetz zur Verfügung steht. Nach einer entsprechenden Konfiguration des Rechners bezieht dieser automatisch alle notwendigen Sicherheitsupdates vom SUS-Server `zivsus.uni-muenster.de`. Ein manuelles Auswählen der Updates vom SUS-Server, wie man es vom Windows-Update-Mechanismus mit dem Internet-Explorer kennt, ist nicht möglich.

Eine ausführliche Anleitung für ein Automatisches Windows Update mit SUS finden Sie auf dem Webserver: `http://winkiosk.uni-muenster.de`.

Nähere Auskünfte erteilt O. Winkelmann (✉ winkeol@uni-muenster.de, ✆ 31618).

Zentrale Lizenz für MATLAB

B. Süselbeck

Das ZIV erweitert sein Angebot an Software für Wissenschaftliches Rechnen

MATLAB ist ein Softwareprodukt für mathematische Berechnungen und Simulationen, das sowohl in der akademischen Welt als auch in der Industrie weite Verbreitung gefunden hat.

Auch innerhalb der Universität Münster existieren in verschiedenen Instituten unterschiedliche Lizenzen. Da in letzter Zeit die Nachfrage nach Produkten der MATLAB-Familie, insbesondere auch für die Lehre, stark zugenommen hat, wurde vom Zentrum für Informationsverarbeitung in enger Abstimmung mit einigen Fachbereichen aus zentralen Mittel eine Lizenz beschafft. Sie besteht aus 40 so genannten "concurrent licen-

ses" für die MATLAB-Suite, die aus dem Basisprodukt MATLAB, dem Simulationstool Simulink und der Symbolic Math Toolbox für symbolische Berechnungen besteht.

Das ZIV beabsichtigt diese Produktfamilie zukünftig unter Wartung zu nehmen. Dabei ist es möglich, schon bestehende Lizenzen in der Universität kostengünstig mit einzubeziehen. Dies könnte speziell für eine Reihe von Erweiterungsmodulen (Tool Boxes) interessant sein.

MATLAB steht für alle vom Hersteller unterstützten Rechnerplattformen zur Verfügung, also Windows, Mac und Linux/Unix. Die Installation erfolgt im zentralen Dateisystem des ZIV.

Nähere Auskünfte erteilt Dr. B. Süselbeck (✆ 31686, ✉ suselbe@uni-muenster.de).

Erschließung ungenutzter Ressourcen zum Number-Crunching

H. H. Adam, Th. Bauer, B. Baumeier, W. Zierau

Im NWZnet, dem ‚Active directory'-Verbund der IVV 4 – Naturwissenschaften, sind derzeit etwa 1000 PCs unter Windows in Betrieb. Viele von diesen, insbesondere auch in den CIP-Pools sind neue leistungsfähige Rechner, deren Rechenkapazität nur zu einem Bruchteil genutzt wird. Nachts, an den Wochenenden, an Feiertagen stehen die meisten dieser Rechner leer.

Andererseits gibt es einen hohen Bedarf an reiner Rechenleistung, der mit den vorhandenen Kapazitäten im NWZ (VMS, Linux) und im ZIV (ZIVunix) nicht abzudecken ist. Für Parallelrechnen steht im ZIV das Parallelsystem ZIVCLUSTER mit Pentium P4 CPUs zur Verfügung.

Die Rechenleistung eines PCs mit Pentium 4 ist bereits sehr beachtlich. Eigene Benchmarks zeigen, dass bei vielen Problemen, bei denen die reine CPU-Leistung zum Tragen kommt, ein PC mit Pentium P4 Prozessor der derzeit installierten Server-Basis um Faktoren überlegen ist.

Zur Programmentwicklung sind mittlerweile auch Intel-Fortran-(Version 8)- und Intel-C++-Compiler mit den zugehörigen Libraries (MKL, Lapack, IMSL) im NWZnet standardmäßig verfügbar. Bislang war es jedoch nicht möglich diese verteilte Rechenleistung auch effektiv zum Number-Crunching zu benutzen.

Um diese Lücke zu schließen, haben wir vor etwa einem Jahr das Projekt Morfeus begonnen und nun zu einem arbeitsfähigen Abschluss gebracht. Dieses nutzt das Batchsystem Condor der University of Wisconsin, Madison, um eine große Zahl von PCs in den CIP-Pools der IVV zum Rechnen zur Verfügung zu stellen.

Die Benutzung und die Lastverteilung werden dabei sehr elegant „gemanagt". Eine Erweiterung ist leicht möglich. Der Nutzer kann von jedem Arbeitsplatz-PC, der am Condor-Pool teilnimmt, oder am einfachsten unmittelbar über den Terminalserverzugang „NWZhome" sein Programm an den Condorpool schicken. Beim Abschicken entscheidet er welche Leistungen bezüglich CPU und Speicher benötigt werden. Der Condor-Pool sucht dann automatisch eine geeignete Maschine für den Job aus und startet ihn. Bei Beendigung findet der Nutzer die Ergebnisse in seinem Verzeichnis. Wird während der Laufzeit der betreffende Rechner anders, z. B. interaktiv benutzt, so geht der Job in einen Suspend-Status und läuft danach wieder weiter. Auf diese Weise wird die CPU optimal ausgenutzt, ohne dass es zu gegenseitigen Störungen kommt. Eine Prioritätsverteilung sorgt dafür, dass alle Nutzer gerecht bedacht werden.

Dieses Projekt ist nicht nur auf Windows-PCs beschränkt. Rechner unter Linux lassen sich gleich gut einbeziehen. Einzelheiten hierzu finden Sie unter:

`http://www.uni-muenster.de/IVVNWZ/Morfeus/index.html`

Sprache und Daten kommen sich näher

L. Elkemann

An der Universität Münster werden erstmalig ab Mitte Juni 2004 Sprachdaten mittels so genannter ISDN-over-IP-Gateways über das lokale Rechnernetz (LAN) übertragen. Sprachdaten werden nicht mehr wie herkömmlich leitungsvermittelt sondern paketvermittelt übertragen. Da es sich hier um eine kritische Echtzeitapplikation handelt, müssen spezielle Kriterien beachtet werden, um mögliche Störgrößen, wie große Latenzzeiten und Jitterbildung, zu vermeiden. Zukünftig sind doppelte Anbindungen neuer Standorte, je eine für Sprache und Daten, hinfällig.

Die zum Einsatz kommenden Gateways können darüber hinaus im Voice-over-IP-Umfeld (hier: Standard H.323) genutzt werden. Eine Registrierung bei einem vorhandenen Gatekeeper und eine Alias-Zuweisung ist möglich. Wesentliche Funktionsmerkmale eines Gatekeepers sind die Anrufsteuerung (Signalisierung) und die dafür notwendige Umsetzung von IP-Adresse und Telefonnummer bzw. umgekehrt, die Umwandlung des synchronen Datenstroms in IP-Pakete und die Signalisierung auf den Teilnehmeranschlussleitungen für den Auf- und Abbau von Verbindungen (Q.931). Darüber hinaus können bestehende ISDN-Tk-Anlagen mit vorhandenen Endgeräten weiterhin genutzt werden (Investitionsschutz).

Parallel dazu hat der Aufbau einer Voice-over-IP-Umgebung (kurz VoIP) begonnen, um nicht nur die Konvergenz der Netze voranzutreiben, sondern auch den Mehrwert und die Synergien aus dem Miteinander zu schöpfen. In einer Voice-over-IP-Umgebung, die sich nach innen rein auf das lokale Rechnernetz abstützt, wird in naher Zukunft ein ACD-System seinen Dienst aufnehmen.

Was ist ein ACD-System ?

Einfach übersetzt bedeutet Automatic Call Distribution lediglich die automatische Anrufverteilung. Ein ACD-System ist in der Regel ein Server-gestütztes System, welches an eine vorhandene traditionelle Tk-Anlage oder wie in dem weiter unten erläuterten Szenarium an eine VoIP-Umgebung angeschaltet wird und nach voreingestellten Regeln Anrufe automatisch verteilt.

Anwendungsgebiete für ACD-Systeme

Anwendungsgebiete für ACD-Systeme können u. a. Auskunftsdienste und Hotlines sein. Zur Zeit sind Hotlinefunktionalitäten durch Sammelrufgruppenschaltungen ausschließlich auf Seiten der Tk-Anlagen realisiert. Diese Sammelrufgruppenschaltungen bieten jedoch nur eingeschränkten Bedienungskomfort, was oft zu Fehlbedienungen bzw. zu einem ungewollten Zu- oder Abschalten führt. Alle Funktionen und Einstellungen, die der Sammelrufgruppenteilnehmer vornehmen kann, müssen über die Tastatur des Telefons vorgenommen werden, was eine nur geringe Kontrolle der vorgenommenen Einstellungen nach sich zieht. Die Möglichkeit einer optischen Kontrolle der vorgenommenen Einstellungen ist nicht gegeben. Eine Fülle notwendiger Parametrierungen dieser Sammelrufgruppen sind darüber hinaus nur von zentraler Stelle möglich.

Mit Einführung einer ACD-Lösung, die sich in einem VoIP-Umfeld befindet, werden diese Einschränkungen aufgehoben. Durch unmittelbare Einbindung der ACD-Lösung in das LAN der Universität kann ein Mehrfaches an Funktion, Skalierung und dezentraler Administration realisiert werden. Exemplarisch seien hier 2 Funktionen erwähnt:

- Das Aktivieren von PC-Anwendungen, die unmittelbar mit dem Anruf in Beziehung gebracht werden können. Voraussetzung hierfür ist, dass die rufende Nummer in eine Relation zu vorhandenen Daten gebracht werden kann.
- Die dezentrale Agentenverwaltung innerhalb einer Gruppe. Eine genauere Ressourcenzuteilung, hier in Form der Anzahl von Agenten einer Gruppe, ist möglich.

Um einen genauen Prozessablauf abbilden zu können, sind darüber hinaus weitere umfangreichere Faktoren zu berücksichtigen, die von Fall zu Fall unterschiedlich gewichtet werden müssen. Im Vorfeld der Einführung eines ACD-Systems müssen jedoch grund-

sätzliche Fragen beantwortet sein. Einige dieser Fragen sind hier exemplarisch aufgeführt:

- Nach welchen Regeln werden Anrufe verteilt?
- Auf welchen Mitarbeiter wird der Anruf verteilt?
- Bekommen immer die gleichen freien Mitarbeiter die Gespräche zugewiesen?
- Welche Möglichkeiten gebe ich den Mitarbeitern bei der Abarbeitung dieser Gespräche mit auf den Weg? Bereitstellung von Daten und Informationen aus anderen Systemen.
- Wie wird ein Anruf behandelt, wenn alle Mitarbeiter bereits ein Gespräch führen (Überlaufszenarien)?
- Ist die Identifizierung der anrufenden Nummer möglich, so dass eine Verknüpfung mit vorhandenen Datenbanken durchführbar ist, um Popups von Anwendungen, z. B. vorhandene Trouble-Tickets, zu ermöglichen?
- Habe ich die Möglichkeit, sowohl im IP-Umfeld als auch im ISDN-Umfeld den Status der Endgeräte zu überwachen, so dass nicht irrtümlich manuell von einem Agenten auf einen besetzten Agenten, oder auf einen Agenten, der sich in Pause befindet, vermittelt wird?
- Sollen parallel zu den abzuarbeitenden Gesprächen E-Mail-Nachrichten bearbeitet und beantwortet werden?
- Gibt es die Möglichkeit der Anschaltung von Ansagen, z. B. bei größeren Störungen?

In einer Pilotphase werden zwei bestehende Hotlines durch das neue ACD-System nachgebildet. Durch die Einbindung des Systems in beide Netze (LAN und TK-Netz) und der damit verbundenen Möglichkeit, auf bestehende Datenbanken zugreifen zu können, ist eine Effizienzsteigerung und Erhöhung der Kundenzufriedenheit zu erwarten.

Gigabit-Anbindung des G-WiN-Clusters Münster an das G-WiN/Internet

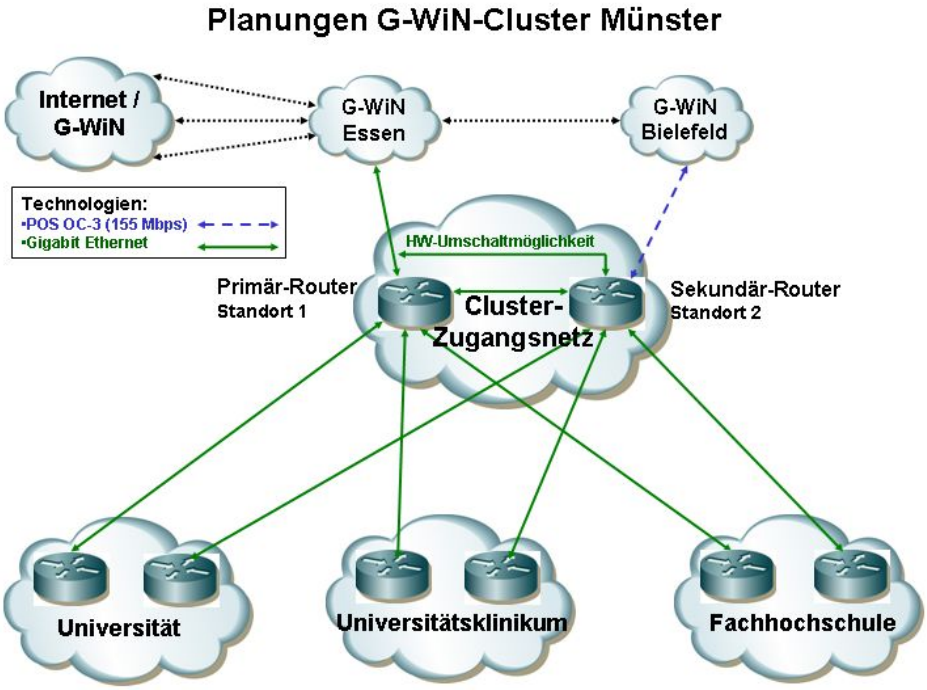
M. Speer

Seit Juni 2004 existiert eine durchgehende Glasfaserleitung zwischen dem G-WiN-Kernnetzstandort Essen und der Universität Münster. Über diese Verbindung soll zukünftig der neue G-WiN/Internet-Anschluss der Universität, des Universitätsklinikums und der Fachhochschule mit einer Bandbreite von 1 Gigabit pro Sekunde realisiert werden.

Bei der zwischen Essen und Münster realisierten ca. 100 km langen Glasfaserleitung handelt es sich als Besonderheit um eine sog. „Dark Fiber“, d. h. eine durchgehende, reine Glasfaserverbindung ohne irgendwelche aktive Netztechnik. Als Netztechnologie wird Gigabit-Ethernet zum Einsatz kommen. Bislang wird im G-WiN für Weitverkehrsverbindungen die klassische sog. SDH-Technologie eingesetzt. Gegenüber dem bisherigen 155 Mbps-Hauptanschluss steht dann zukünftig eine fast 6,5-fache Bandbreite zur Verfügung. Die Glasfaserleitung zwischen den Städten Essen und Münster wurde von der Firma GasLINE bereitgestellt. In Zusammenarbeit mit dem Unternehmen TROPOLYS wurden die Verbindungen innerhalb der beiden Stadtbereiche realisiert. Die Leitung wurde dem Betreiber des G-WiN, dem DFN-Verein, anlässlich des 20-jährigen DFN-Jubiläums überlassen. Die für den Betrieb der – für Gigabit-Ethernet-Verhältnisse extrem langen – Leitung notwendigen speziellen Geräte wurden von der Firma Dimension Data zur Verfügung gestellt.

Vor der Übernahme der „Dark Fiber“-Verbindung in den Produktionsbetrieb soll die Verbindung zunächst erprobt werden, um keinerlei Einbußen in der Verfügbarkeit gegenüber der bisherigen G-WiN-Backup-Konfiguration hinnehmen zu müssen (vgl. Artikel im infoWiki Nr. 3/2003). Durch eine direkte Primäranbindung an den G-WiN-Kernnetzstandort Essen ist auf jeden Fall die bisher noch gegebene Abhängigkeit vom G-WiN-Standort Bielefeld beseitigt (vgl. Abb.). Es ist geplant, den mit dem Standort Bielefeld verbundenen Sekundäranschluss, der bei Ausfall des Primäranschlusses verwendet wird, von 34 Mbps auf 155 Mbps hochzurüsten. Durch den Wegfall der 34-Mbps-E3-Technologie wird dann auch eine Reduzierung der eingesetzten Netztechnolo-

gien erzielt, wobei für den Regelbetrieb dann nur noch die Standard-Technologie Gigabit-Ethernet zum Einsatz kommt. Um einen Totalausfall des Primär-Routers abfangen zu können, soll weiterhin eine Hardware-Umschaltmöglichkeit des neuen Primär-Anschlusses auf den Sekundär-Router existieren.



Ergänzende Information:

Pressemitteilung des DFN-Vereins vom Juni 2004: „Dark Fiber zum Geburtstag“ `http://www.dfn.de/content/presse-information/pressemitteilungen/pm010604/`

Rechnernetz im UKM erhielt eigene Anbindung

N. Gietz

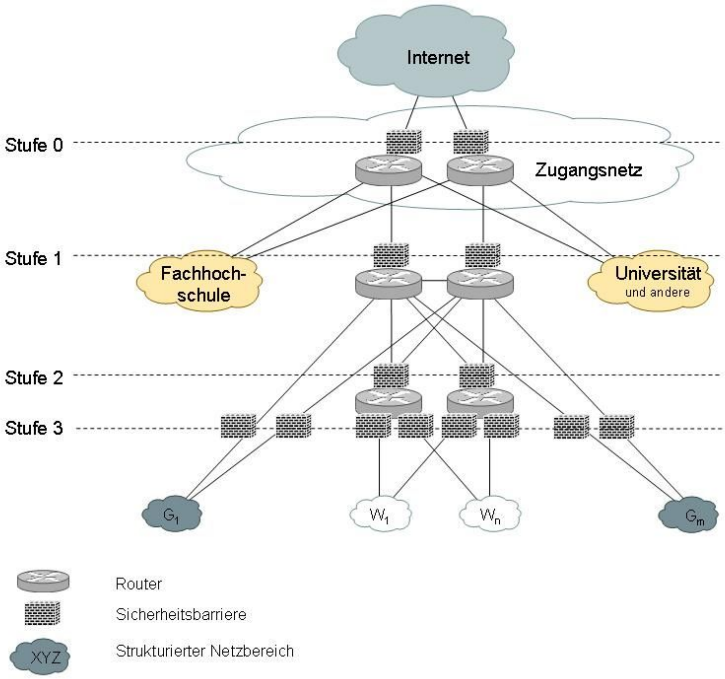
Hohe Anforderungen an Sicherheit und Verfügbarkeit von Rechnernetzen erfordern angepasste Netzwerkstrukturen. Das Universitätsklinikum (UKM) erhielt jetzt eine neue Anbindung an das LAN der Universität.

Seit der Indienststellung der ersten Rechnernetzanschlüsse im UKM waren diese in das LAN der Universität integriert. In den ersten Jahren wurde zunächst ein reines Layer-2-Netzwerk in der Ethernet-Technologie betrieben, das sich über den Campus der gesamten Universität erstreckte. Dieses wurde mit der Einführung von FDDI-Routern Mitte der neunziger Jahre auf Layer-3 des OSI-7-Schichtenmodells als IP-Netzwerk strukturiert. Mit der Einführung von ATM standen 1998 dann erstmals virtuelle LANs zur Netzstrukturierung zur Verfügung und im Januar 2002 hielt die Gigabit-Technologie Einzug in das LAN.

Anfang dieses Jahres fiel dann die Entscheidung, durch Umstrukturierung auch das LAN im UKM separat neben der Universität und der Fachhochschule an das Zugangsnetz der WWU zum Internet anzubinden (siehe infoWWW Nr. 3/2003: „Neue Netzstrukturen für den Interner/GWIN-Anschluss der Universität und der Fachhochschule). Hierzu wurden zunächst die Core-Gigabit-Switches zu einer neuen Backbonestruktur verschaltet und an das Zugangsnetz angeschlossen. Diese Arbeiten konnten ohne negative Auswirkungen auf den Betrieb des Netzes innerhalb der üblichen Arbeitszeiten durchgeführt werden. Im nächsten Schritt musste das Layer-3-IP-Routing für alle Rechner des UKM auf diese neue Struktur übertragen werden. Hierzu war eine detaillierte Planung für jedes einzelne der 200 betroffenen IP-Subnetze notwendig. Neben Festlegung der exakten Zeitpunkte der einzelnen Maßnahmen waren Routerkonfiguration festzulegen und ACLs (Access

Control Lists) anzupassen und zu prüfen. Weiterhin musste für jedes IP-Subnetz auch auf Layer-2 die richtige Verteilung des zugehörigen VLANs (virtuellen LAN) auf die neue Backbone-Struktur vorbereitet werden.

Damit auch das Routingprotokoll OSPF (Open Shortest Path First) des LAN im UKM von dem der restlichen Universität entkoppelt werden konnte, musste ein dynamisches Verfahren, das über das Zugangsnetz der WWU arbeitet, getestet und implementiert werden. Alle diese Vorbereitungsmaßnahmen konnten innerhalb von 4 Wochen abgeschlossen werden. In den nachfolgenden 6 Wochen wurde sukzessive das Routing für alle Bereiche des UKM auf das neugestaltete Backbone übertragen. Dies geschah ohne nennenswerte Komplikationen, für die meisten Nutzer fast unbemerkt, ebenfalls während der normalen Dienstzeiten. Lediglich für die Umschaltung der zentralen Server im Klinikum wurde auf andere Tageszeiten ausgewichen.



Schematische Darstellung der neuen Netzwerkstruktur im UKM

Ziel dieser umfangreichen Maßnahmen war neben der Einführung neuerer leistungsfähigerer Technologien die Erhöhung der Verfügbarkeit und Sicherheit des LANs. Hierzu müssen in weiteren, zum Teil bereits angelaufenen Schritten strukturierte Bereiche innerhalb des LANs geschaffen werden, in denen Rechner mit identischen (Sicherheits-) Anforderungen zusammengefasst werden. Dadurch ist es möglich Bereiche mit verwandten Anforderungen wiederum zu gruppieren und hierüber eine Hierarchie mit zurzeit vier Ebenen zu bilden.

An den Übergängen zu den einzelnen Hierarchieebenen (Stufe) werden Sicherheitsbarrieren eingebracht. Diese können im einfachsten Fall aus auf Layer 3 und 4 basierenden ACLs bestehen; aber auch der Einsatz von dedizierten Firewallprodukten, die bis auf Anwendungsebene (Layer 7) arbeiten, ist an diesen Stellen möglich. In der Stufe 0 werden Sicherheitsmaßnahmen realisiert, die für alle über den Internetzugang versorgten Einrichtungen und Hochschulen identisch sind. Dies sind z. B. ACLs, die die von Windows verwendeten Ports 136, 137,138 und 445 sperren. Auf der Stufe 1 werden die Sicherheitsbarrieren, die für das gesamte Universitätsklinikum gelten, implementiert. Die Stufe 2 deckt die Bedürfnisse der Gruppe der zentralen klinischen Anwendungen ab, während auf Stufe 3 die individuellen Anforderungen der einzelnen Bereiche abgedeckt werden. Bereiche, die sich nicht den Beschränkungen und Anforderungen der Stufe 2

unterordnen können, werden direkt unter Umgehung der Stufe 2 angebunden. Diese Hierarchisierung ermöglicht komplexe Sicherheitsfunktionen in handhabbarer und überschaubarer Weise effizient und performant umzusetzen.

Das gesamte Konzept ist im Corebereich redundant ausgelegt und skaliert hinsichtlich Redundanz und Performance über die Möglichkeit Verbindungen als LAG (Link Aggregation Group) mehrfach auszulegen.

10.000 LAN-Anträge

M. Kamp

Das NIC (Netzwerk-Informations-Center) hat in den vergangenen 17 Jahren 10.000 Antragsvorgänge zu LAN-Anschlussdosen oder Netzzugängen für Endgeräte bearbeitet. Der erste Antrag dieser Art wurde am 30.06.1987 an das ZIV gerichtet und stammte aus der Mathematik. Der Antrag mit der Nummer 10.000 wurde vom Historischen Seminar gestellt und ging am 14.05.2004 ein.

Während es 1987 noch bei insgesamt 18 Anträgen für vier Dosen und 58 Geräte blieb, steigerte sich die Zahl auf 1546 Anträge für 1277 Dosen und 2646 Geräte im Jahr 2003. Aktuell sind für das Daten-Netz der Universität 31.000 Endgeräteanschlüsse dokumentiert, an denen ca. 18.000 Endgeräte betrieben werden.

ZIV-Lehre

Veranstaltungen in der vorlesungsfreien Zeit (August-Oktober 2004)
für Hörer aller Fachbereiche

Beratung zum Lehrangebot durch Herrn W. Bosse jeweils Di, Do 11-12, 83-3 15 61

Für alle Veranstaltungen ist eine frühzeitige Online-Anmeldung erforderlich, die ausgehend von der Webadresse `http://www.uni-muenster.de/ZIV/Content-Lehre.html` unter „Anmelden zu den Veranstaltungen" erfolgen kann. Für den Dialog muss dabei auf die dort angebotene verschlüsselte (abhörsichere) Datenübertragung umgeschaltet werden. Anmeldungen zu den Veranstaltungen sind möglich ab 1. Juli 2004 für die vorlesungsfreie Zeit.

260010 Sichere Kommunikation im Internet — Perske, R.
vom 30.08. bis 03.09.2004, Mo-Fr 10-17 Uhr
Hörsaal: ZIV-Pool 3, Einsteinstr. 60

260024 cms@uni – Werkzeuge für den Webauftritt — Neukäter, B.
vom 13.09. bis 24.09.2004, Mo-Fr 10-12 und 13-15 Uhr
Hörsaal: ZIV-Pool 3, Einsteinstr. 60

260043 Neuere Entwicklungen in der Programmiersprache Java — Süselbeck, B.
vom 13.09. bis 24.09.2004, Mo-Fr 9-11 Uhr
Hörsaal: M4, Einsteinstr. 64

260058 Statistische Datenanalyse mit dem Programmsystem SPSS — Zörkendörfer, S.
vom 04.10. bis 15.10.2004, Mo-Fr 9-11 Uhr, nachmittags n.V.
Hörsaal: ZIV-Pool 3, Einsteinstr. 60

260062 Einführung in Grid-Computing — Leweling, M.
vom 11.10. bis 15.10.2004, Mo-Fr 9-11 Uhr
Hörsaal: Raum 206, Röntgenstr. 9-13

260077 Betriebssystem Linux/Unix: Einführung und Grundlagen — Grote, M.
vom 16.08. bis 27.08.2004, Mo-Fr 10-16 Uhr
Hörsaal: ZIV-Pool 3, Einsteinstr. 60

260081 Systemadministration für Linux-Systeme — Hölters, J.
vom 27.09. bis 01.10.2004, Mo-Fr 9-16 Uhr
Hörsaal: ZIV-Pool 3, Einsteinstr. 60

260096 Administration eines Windows-Systems — Kämmerer, M.
vom 06.09. bis 10.09.2004, Mo-Fr 9-17 Uhr
Hörsaal: M4, Einsteinstr. 64 und ZIV-Pool 3, Einsteinstr. 60
Beginn: 06.09.2004, 9 Uhr, M4

260100 Systemadministration für Windows-Server — Winkelmann, O.
vom 04.10. bis 08.10.2004, Mo-Fr 9-16 Uhr
Hörsaal: Raum 206, Röntgenstr. 9-13
Lange, W.

Veranstaltungen in der Vorlesungszeit (Wintersemester 2004/2005)
für Hörer aller Fachbereiche

Beratung zum Lehrangebot durch Herrn W. Bosse jeweils Di, Do 11-12 83-3 15 61

Für alle Veranstaltungen ist eine frühzeitige Online-Anmeldung erforderlich, die ausgehend von der Webadresse `http://www.uni-muenster.de/ZIV/Content Lehre.html` unter „Anmelden zu den Veranstaltungen“ erfolgen kann. Für den Dialog sollte dabei vorzugsweise auf die dort angebotene verschlüsselte (abhörsichere) Datenübertragung umgeschaltet werden. Anmeldungen zu den Veranstaltungen sind möglich ab 1. September 2004 für die Vorlesungszeit.

260039	Programmieren in C++ Mi 13-15 Uhr Hörsaal: M4, Einsteinstr. 64, Beginn: 27.10.2004	Mersch, R.
260115	Programmieren in Java Mi 9-11 Uhr Hörsaal: M4, Einsteinstr. 64, Beginn: 20.10.2004	Sturm, E.
260120	Statistische Datenanalyse mit dem Programmsystem SPSS Mi 11-13 Uhr Hörsaal: ZIV-Pool 3, Einsteinstr. 60, Beginn: 20.10.2004	Nienhaus, R.
260134	Multimedia Praktikum 2-stündig n. V. Hörsaal: ZIV-Pool 3, Einsteinstr. 60 Beginn: Di 19.10.2004, 10-12 Uhr (Vorbesprechung)	Kisker, H.-W.
260149	Rechnernetze und Internet: Technische Grundlagen Do 14-16 Uhr Hörsaal: Raum 206, Röntgenstr. 9-13, Beginn: 21.10.2004	Richter, G. Forsmann, A. Kamp,M. Speer, M. Wessendorf, G.
260153	Kolloquium des Zentrums für Informationsverarbeitung Fr 14-16 Uhr Hörsaal: Raum 206, Röntgenstr. 9-13	Held, W.

Kommentare zu den Veranstaltungen

260010 Sichere Kommunikation im Internet

Das Internet ist eine mächtige und leistungsfähige Kommunikations-Infrastruktur, birgt aber auch erhebliche Gefahren, welche für einen unbedarften Nutzer nur schwer zu erkennen sind.

In der Veranstaltung wird gezeigt, welche Gefahren bestehen und wie man sich ohne große Mühe vor den meisten dieser Gefahren schützen kann. Praktisch geübt werden kurz das Absichern des eigenen Rechners am Beispiel von Windows 98 oder XP sowie ausführlich das Einrichten und die Benutzung entsprechender Software zur sicheren Kommunikation:

- Sichere E-Mail mit Pretty Good Privacy und mit Secure MIME
- Sichere Dialog- und Datenverbindungen mit Secure Shell
- Sichere Interaktion im WWW mit SSL/TLS (HTTPS

Den Teilnehmerinnen und Teilnehmern wird dabei deutlich, dass Verschlüsselung, elektronische Unterschriften und Zertifikate viel einfacher zu benutzen sind als man sich gemeinhin vorstellt. Vorausgesetzt werden Erfahrungen im Umgang mit den Internetan-

wendungen E-Mai, WWW, Telnet und FTP sowie Grundkenntnisse der Funktionsweise (wozu braucht man IP-Adressen? Portnummern? Nameserver? Router?).

260024 cms@uni – Werkzeuge für den Webauftritt

Das Internet wird neben den traditionellen Medien in immer stärkerem Umfang zur Öffentlichkeitsarbeit genutzt. Zur Realisierung der Dokumente im Web dient die Hypertext Markup Language (HTML). Um den Publizierenden auch ohne Kenntnisse der HTML den Zugang zum Web zu ermöglichen, werden Content-Management-Systeme (CMS) eingesetzt.

Die Teilnehmer/innen dieser Veranstaltung sollen die Methoden der Inhaltsverwaltung im Web und den Aufbau eines CMS kennen lernen. Für sie wird ein Zugang zu dem an der Universität verwendeten System Imperia eingerichtet, an dem die erworbenen Kenntnisse in die Praxis umgesetzt werden können.

Kenntnisse im Umgang mit dem PC und dem World Wide Web (WWW) werden vorausgesetzt.

260043 Neuere Entwicklungen in der Programmiersprache Java

Mit dem Erscheinen der Version 1.5.0 der Java 2 Standard Edition werden einige neue Sprachelemente für Java zur Verfügung gestellt. Dies sind u. a.

- Autoboxing/Unboxing
- Enhanced for-Loop
- Generics
- Metadata
- Static Import
- Typesafe Enums
- Varargs

Ziel der Vorlesung ist es, eine Übersicht zu diesen neuen Eigenschaften der Programmiersprache zu geben und anhand von Beispielen die neue Programmiertechnik vorzustellen bzw. zur bisherigen Arbeitsweise abzugrenzen.

Zusätzlich sollen die Teile der Java-Klassenbibliotheken, die die neuen Sprachstandards besonders nutzen, wie beispielsweise die so genannte Collection-API, intensiver behandelt werden.

Grundlegende Kenntnisse der Programmiersprache Java werden vorausgesetzt.

260058, 260120 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.

260062 Einführung in Grid-Computing

Unter „Grid Computing" versteht man alle Methoden, die Leistung vieler Computer in einem Netzwerk (also z. B. das Internet) so zusammenzufassen, dass die – idealerweise parallele – Lösung extrem rechenintensiver Probleme möglich wird. Meist wird dabei auf bereits bestehende, zum Teil ungenutzte oder nicht optimal genutzte Rechenkapazitäten zurückgegriffen, so dass durch Grid Computing prinzipiell die Leistung heutiger einzelner Supercomputer zu deutlich geringeren Kosten übertroffen werden kann. Die Idee des Grid Computings wurde bereits in verschiedenen Projekten realisiert. Die Projekte UNICORE und UNICORE+ (www.unicore.de, www.unicore.org) verbinden vorwiegend deutsche HPCs miteinander. In den USA wurde das Projekt Globus (`www.globus.org`) ins Leben gerufen. Als wesentliche Bestandteile der deutschen D-Grid-Initiative sollen unter anderem diese beiden Projekte vorgestellt werden.

260077 Betriebssystem Linux/Unix: Einführung und Grundlagen

Linux ist ein leistungsstarkes Unix-System für viele Hardware-Architekturen. Als preiswerte Windows-Alternative ist es augenblicklich in aller Munde. Die Vorlesung will in die Linux-Benutzung einführen. Sie besteht aus zwei Teilen. Zuerst erfolgt eine an üblichen Unix-Einführungen orientierte Beschreibung des Unix-Datei-Systems und der wesentlichen Unix-Befehle. Anschließend wird die grafische Oberfläche KDE behandelt, die für viele ein Linux-System erst attraktiv macht.

260081 Systemadministration für Linux-Systeme

Die Vorlesung richtet sich an fortgeschrittene Linux-Anwender/innen, die Unterstützung bei der Installation und System-Integration von Linux-Systemen benötigen. Voraussetzung sind grundlegende Kenntnisse der Unix-Kommandos und der Shell-Script-Sprache. Die Teilnehmer/innen werden in der Veranstaltung ein Linux-System selbst installieren und in die Netzwerk- und Systeminfrastruktur der Universität einbinden. Ferner wird demonstriert, wie man einen speziell auf die Hardware-Ausstattung des Rechners optimierten Kernel generiert.

260096 Administration eines Windows-Systems

Für Hörer/innen mit Windows-Vorkenntnissen werden Arbeiten zum Aufbau und Betrieb eines Windows-Servers vorgestellt und gemeinsam erprobt. Die folgenden Themen werden u. a. behandelt:

- Installation und Konfiguration des Servers,
- Benutzer- und Gruppenverwaltung, lokale Administration,
- Druck-, Datei-, Logon- und allgemeine Programm-Services,
- Zugriffsrechte und Netz-Freigaben,
- Diagnose- und Überwachungsfunktionen,
- Internet, LAN, Netz-Protokolle,
- Absicherung des Servers gegen Angriffe von außen.

Die speziellen Dienste E-Mail-, Datenbank-, Web- und Media-Server können im Rahmen dieser Veranstaltung nicht bearbeitet werden. Die Einbindung des Servers in eine Windows Active Directory Domäne wird nur am Rande erwähnt werden. Wir verweisen auf die weitere Veranstaltung Systemadministration für Windows-Server (260100).

260100 Systemadministration für Windows-Server

Die Veranstaltung richtet sich an fortgeschrittene Windows-Benutzer, die ihre Kenntnisse mit Blick auf die Anforderungen in einem großen Rechnernetz erweitern möchten. Als Schwerpunkte sind u. a. der Aufbau und Betrieb von Servern im Windows-Netzwerk (Active Directory) vorgesehen.

Themenauswahl:

- Installation und Konfiguration;
- Benutzerverwaltung;
- Sicherheit u. a.: Dateisystem, Registry, Netzwerk, Sicherheitsrichtlinien;
- Server im Active Directory: Gesamtstrukturen, Domänenstrukturen, Domänen, Organisationseinheiten (OU), Vertrauensstellungen, Standorte, Replikation, Gruppenrichtlinien;
- Softwareverteilung und Systemüberwachung.

Im Rahmen der Veranstaltung wird auch Gelegenheit zu praktischen Übungen gegeben.

260039 Programmieren in C++

C++ erweitert die Programmiersprache C mit ihren durch Assembler-ähnliche Sprachelemente einerseits und Elemente moderner blockstrukturierter Sprachen andererseits sehr vielseitigen Einsatzmöglichkeiten um objektorientierte Konzepte. Diese Verbindung einer sehr erfolgreichen Programmiersprache mit einem seit einigen Jahren boomenden Programmier-Paradigma macht C++ zu einer der am meisten benutzten Programmiersprachen. In der Lehrveranstaltung wird C++ gemäß dem 1998 erschienenen ISO/ANSI-Standard von Grund auf vorgestellt. Kenntnisse einer anderen Programmiersprache wären hilfreich, werden aber nicht vorausgesetzt.

STROUSTRUP: *Die C++ Programmiersprache*, dritte Auflage, Addison-Wesley

260115 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 ohne Vorkenntnisse im Programmieren geeignet.

260134 Multimedia Praktikum

Das Praktikum führt in die elementaren Techniken der Bildgewinnung und deren Präsentation ein. Es besteht aus einem vorbereitenden theoretischen Teil, der vorab im Internet veröffentlicht wird, und einem Praktikumsteil, zu dem die neu eingerichteten Multimedia-Räume des ZIV genutzt werden.

Im theoretischen Teil werden unter andere folgende Themen behandelt:

- Die Grundlagen der Gewinnung eines digitalen Fotos (Bayer-Muster)
- Algorithmen zur Umwandlung von Bayer-Mustern in Fotos
- Die Qualität digitaler Bilder (Modular Transfer Function)
- Grundlagen der Farbenlehre
- Aufbau farbkalibrierter Arbeitsumgebungen
- Bildbearbeitungsalgorithmen (Farbumfang, Schärfung usw.)
- Bildformate (Jpeg, Tiff, Gif usw.)
- Kurzeinführungen in die verwendeten Standardprogramme (Photoshop, Acrobat usw.)

- Schrittweise Arbeitsanleitungen für die Experimente des praktischen Teils. Im praktischen Teil werden die Hörer Erfahrung im Umgang mit Flachbett-Scannern, Dia-Scannern, digitalen Kameras, Videokameras und Webcams gewinnen. Gleichzeitig wird auch die Präsentation des gewonnen Bildmaterials als Druckausgabe, Photo-CD, Video-CD und Life-Internet-Übertragung trainiert.

Im Einzelnen sind folgende Experimente vorgesehen:

- Gewinnung von gerasterten Bildern (von Druckvorlagen); Gerät: Flachbettscanner; Präsentation: Druck
- Gewinnung von Bildern mit kontinuierlicher Farbverteilung (von Fotos); Gerät: Dia-Scanner; Präsentation: Druck
- Bildgewinnung mit einer digitalen Kamera; Gerät: Digitale Kamera; Präsentation: Still-Video-CD
- Bildgewinnung mit Video-Kamera (d. h. Filmerstellung); Gerät: Video-Kamera digital und analog; Präsentation: Video-CD
- Bildgewinnung und Präsentation in Echtzeit (d. h. Video-Konferenz); Gerät: Webcam; Präsentation: Bildschirm
- Herstellen einer farbkalibrierten Umgebung; Gerät: Scanner, Bildschirm, Drucker
- Bewertung der Bildqualität; Gerät: Digitale Kamera, genormte Bildvorlagen, spezielle Programme

Alle Experimente finden in den neu eingerichteten Multimedia-Räumen des ZIV statt. Die Teilnehmer des Praktikums arbeiten in Gruppen von maximal drei Personen. Die zeitliche Zuteilung der Experimente (und Räume) zu den Gruppen wird nach Vereinbarung durchgeführt. Die Experimente werden von den Mitarbeitern des ZIV betreut. Die Teilnehmer des Praktikums legen ein Praktikumsbuch an.

Das Praktikum erfordert eine Voranmeldung. Der Termin für eine Vorbesprechung, in der Gruppen und Termine festgelegt werden, ist unbedingt wahrzunehmen.

260149 Rechnernetze und Internet: Technische Grundlagen

Diese Veranstaltung gibt einen Einblick in die technischen Grundlagen der Rechnernetze unter besonderer Berücksichtigung des Internets.

Folgende Themen werden behandelt:

- Architekturmodell für Rechnernetze (OSI-Modell), Kommunikationsprotokolle
- Techniken für lokale Rechnernetze (LANs): Ethernet, Fast Ethernet, Gigabit Ethernet
- Kopplung/Strukturierung von Rechnernetzen: Routing, Bridging und Switching
- Grundlegende Internet-Protokolle: IP, TCP, UDP, ICMP, ARP, DNS, DHCP, WINS
- TCP/IP-Software: Konfiguration und Diagnose
- spezielle TCP/IP-Funktionen unter Windows
- Funk-LANs
- Struktur und Funktionen des Rechnernetzes der Universität Münster

260153 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:

KeyID 4CB7658D: Zertifizierungsstelle Universitaet Muenster (E-Mail) <ca@uni-muenster.de>
2048 Bits, Fingerprint: 383D 0F16 CEFC 1F9E B7C3 04B1 2020 FCE6
KeyID 94E799B5: DFN-PCA (2004), ENCRYPTION Key <dfnpca@dfn-pca.de>
2048 Bits, Fingerprint: A9F8 2DC4 09CC DA7F DC67 8FE5 28DE AAAC

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.

infoforum Juli 2004

Liebe Leserin, lieber Leser,

wenn Sie **infoforum** regelmäßig beziehen wollen, bedienen Sie sich bitte des unten angefügten Abschnitts. Hat sich Ihre Adresse geändert oder sind Sie am weiteren Bezug von **infoforum** 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 **infoforum**

☐ 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 **infoforum**
Zentrum für Informationsverarbeitung
Röntgenstr. 9–13
48149 Münster

☐ Meine Anschrift hat sich geändert.
Alte Anschrift:

_____

_____

Absender:

Name: _____

FB: _____ Institut: _____

Straße: _____

Außerhalb der Universität:

_____

(Bitte deutlich lesbar in Druckschrift ausfüllen!)

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

_____ _____

Ort, Datum Unterschrift