



Wenn der Rechner sagt, „I love you“, ist es leider zu spät: Für Schutz vor Viren und anderen Risiken sollte man rechtzeitig sorgen.

EDITORIAL

Bedrohte Sicherheit

Die vielen wohlklingenden e-Wörter (e-Commerce, e-Government etc.) zeigen es: Die Informationstechnik ist dabei, praktisch alle Bereiche des alltäglichen Lebens zu erobern. Die immer wiederkehrenden Schlagzeilen über Hackereinbrüche und Viren belegen aber auch unsere wachsende Abhängigkeit von der IT-Sicherheit. Deren Werkzeuge liefert die Kryptographie: zum Beispiel Verfahren zum Verschlüsseln und Authentisieren von Daten oder für digitale Signaturen, die Grundlagen jedes IT-Sicherheitssystems. Für diese Krypto-Verfahren gibt es heute genaue Standards. Sie sind nach *heutigem* Kenntnisstand als ausreichend sicher einzuschätzen, wenn die jeweiligen Schlüssellängen entsprechend groß gewählt werden. Trotzdem ist es jederzeit möglich, wenn auch unwahrscheinlich, dass neue Angriffstechniken oder übersehene Schwachstellen es Angreifern erlauben, diese Verfahren zu knacken.

Darüber hinaus müssen Krypto-Verfahren natürlich so implementiert werden, dass sie nicht umgangen werden können. Und genau hierin besteht ein Hauptproblem bei der praktischen Realisierung von IT-Sicherheit, z. B. die Abwehr von Hackern (Penetrationsangriffen), Viren und Trojanern, besonders bei einigen der weit verbreiteten Betriebssysteme, die digitales Ungeziefer aller Art anziehen. Zur praktischen Realisierung von IT-Sicherheit gehört auch die sichere Schlüsselerzeugung. All dies muss durch organisatorische Maßnahmen ergänzt werden: Ohne verantwortungsbewusstes Verhalten der Nutzer bringen auch die besten Kryptoverfahren nichts.

IT-Sicherheit ist nicht nur Thema bei (vernetzten) Rechnern. Die nächste Generation von IT-Anwendungen mit PDAs, UMTS-Handys und unzähligen weiteren mobilen Kommunikationspunkten, die über ad-hoc Netze verbunden sind, stellt ein enormes Sicherheitsproblem dar. Smart-Cards mit Krypto-Algorithmen wie die Telefonkarte werden daher immer stärker genutzt. Solche Karten sind im Prinzip hervorragend zur sicheren Speicherung geheimer Schlüssel geeignet. Aber unlängst entwickelte Angriffsverfahren, die den Stromverbrauch einer Smart Card analysieren, können es Angreifern erlauben, die Karten zu „brechen“ und z. B. zu duplizieren. Die Kartenhersteller kennen das Problem und haben teilweise Schutzmechanismen implementiert.

Die Realisierung von IT-Sicherheit ist ein evolutionärer Prozess. Jeder neue Angriff führt zur Entwicklung neuer Gegenmaßnahmen und umgekehrt. Nur ständige Anstrengung kann IT-Sicherheit erreichen. Der potentielle Schaden, der angerichtet werden kann, wenn etwa bei weltweit eingesetzten Standards schwerwiegende Lücken auftreten, wird mit der steigenden IT-Nutzung immer größer. Die zunehmende globale Abhängigkeit von Informationstechnologien wird ein wachsender Anreiz für Angreifer sein. In diesem Sinne ist der „Cyberwar“ nicht nur Fiktion.

Hans Dobbertin, Christof Paar, Horst Görtz Institut für Sicherheit in der Informationstechnik

NEUES IT-SICHERHEITSKONZEPT

Gefahr erkannt, Gefahr gebannt

Das Rechnernetz der Ruhr-Universität ist als freizügiges Kommunikationsnetz konzipiert: Jeder Teilnehmer kann die für Administration, Forschung und Lehre erforderlichen Rechnersysteme betreiben. Leider hat diese Freiheit ihren Preis: Ca. 600 mehr oder weniger gut gepflegte Mail- und Webserver bieten ihre Dienste ins Internet an. Unzählige telnet-, ssh-, ftp-, DNS- oder Proxyserver gar nicht mitgerechnet. Beinahe täglich meldet das CERT (Computer Emergency Response Team) Fehler in Betriebssystemen und Serverprogrammen. Die meisten dieser Schwachstellen können Angreifer dazu nutzen, übers Internet in Systeme einzusteigen (s. auch RUBbits Juni 2001). Daher müssten insbesondere Server rechtzeitig mit Sicherheitsupdates der Hersteller versorgt werden. Doch diese Pflicht wird nicht immer so genau genommen. Das zeigt sich daran, dass laufend in Rechner der RUB eingebrochen wird. Neben Schwachstellen sind auch Konfigurationsfehler der Server eine offene Tür für Hacker. Solche Fehler können darüber hinaus die Verfügbarkeit anderer Server in Mitleidenschaft

ziehen. So haben nicht etwa Spam (Werbe-E-mails) oder Email-Würmer dem zentralen Mailhost zu schaffen gemacht, sondern er ist bereits mehrfach durch falsch konfigurierte Server im RUB-Netz überflutet worden. Kurz und schlecht: Unser Rechnernetz ist für alle Angreifer vom Hackerexperten bis zum Mochtegern-Hacker ein lohnendes Ziel.

Wer hieraus schließt, dass IT-Sicherheit ein reines Administrationsproblem sei, liegt jedoch falsch. Endnutzer verschärfen durch Unwissenheit oder hohe Risikobereitschaft das Problem. Auch ein einfacher Doppelklick am Endgerät kann sich zur Attacke auf Vertraulichkeit, Integrität und Verfügbarkeit von Rechnersystemen entwickeln. Neue Formen von Schadprogrammen, die im amerikanischen als „blended threats“ bezeichnet werden, nutzen gar beide Wege zur Verbreitung: Sie können sowohl über Betriebssystem-Schwachstellen als auch durch das Fehlverhalten von Nutzern in ein Netzwerk eindringen. Nimda,

ein an der Ruhr-Universität nicht auszurottendes Schadprogramm, ist ein Beispiel dafür.

Diese Bedrohungen lassen sich nicht durch technische Einzelmaßnahmen ausräumen. Vielmehr müssen alle Teilnehmer am hochschulweiten Rechnernetz in den Sicherheitsprozess einbezogen werden. Der Rektor der RUB hat das Rechenzentrum daher beauftragt, ein IT-Sicherheitskonzept zu entwickeln, dessen Strategien die im Mai

2002 an die Organisationseinheiten der RUB versandte „Leitlinie zur IT-Sicherheit“ formuliert. Das Konzept sieht Sicherheitsrichtlinien vor, die gemeinsam mit den Einrichtungen der RUB ausgearbeitet werden. Ergänzend soll es detaillierte Anleitungen geben, die den Administratoren und Benutzern bei ihrer täglichen Arbeit helfen sollen. Zudem ist ein zielgruppenspezifisches Schulungskonzept geplant (s. Kasten auf Seite 4).

Wichtiger Bestandteil des Sicherheitskonzepts ist auch eine verbesserte Kommunikation. Das RZ erhält als offizielle Beschwerdestelle für die Domäne der RUB häufig Beschwerden über kompromittierte Systeme. Leider lassen sich deren Betreiber aber nicht immer oder nur mit großem Aufwand ausfindig machen. Um bei Problemen schnell handeln und mögliche Schadensersatzansprüche abwehren zu können, müssen Betroffene schneller erreichbar sein. Da sich Angriffsszenarien oft schon erkennen lassen, bevor sie Realität werden, muss auch diesbezüglich der Informationsaustausch verbessert werden. Die Leitlinie sieht daher Sicherheitsbetreuer als Ansprechpartner in den Einrichtungen vor.

Ein „Info-Forum IT-Sicherheit“ rundet das Konzept ab. Dort sollen alle sicherheitsrelevanten Infos für jeden Intranetnutzer nachlesbar hinterlegt sein. Die Information über Pro und Kontra wird die Akzeptanz der Maßnahmen stärken. Denn es soll nicht wieder so laufen wie bei der Einführung des Virencanners auf dem zentralen Mailhost: Zwei Jahre lang konnte er wegen massiver Proteste Einzelner nicht in Betrieb gehen. Seit August 2001 tut er trotz Protest seinen Dienst und hat in einem Jahr rund 70.000 Viren ausgefiltert. Viren wie Loveletter, MTX, Klez haben dadurch 70.000 Chancen verpasst. *Brigitte Wojcieszynski*

DFN@HOME AUCH MIT FLATRATE

Billiger ans HIRN

Noch günstiger ins Internet kommen RUB-Angehörige seit dem 1. September 2002: Der Zugang zum HIRN (Hochschul-interne Rechnernetz der RUB), den die Firma mediaWays in Zusammenarbeit mit dem DFN-Verein und der RUB anbietet, kostet nun nur noch 0,99 Cent pro Minute (über ISDN und Modem). Kunden mit einem T-ISDN-XXL Anschluss können mit der XXX-Tarifoption an Sonn- und bundeseinheitlichen Feiertagen kostenlos ins Netz der RUB. Außerdem ist für die DSL-Benutzer eine Flat-Rate zum Preis von 14,95 Euro pro Monat im Angebot. Die Ruhr-Universität gehört zu den ersten Hochschulen der Bundesrepublik, die es ihren Kunden erlauben, über die Flat-Rate von DFN@Home im Netz der Hochschule zu arbeiten. Da der Internetzugang der Flat-Rate über das Netz der RUB geschieht, gelten die globalen Be-

schränkungen des Anschlusses der RUB an das Wissenschaftsnetz. Erlaubt sind zurzeit 12.000 GigaByte pro Monat. Um diese Volumengrenze nicht zu überschreiten, wird der Datenverkehr bewirtschaftet. Das heißt: Dienste wie E-Mail und WWW (unter Verwendung des Proxy-Servers) werden bevorzugt behandelt. „Normaler“

Internet-Verkehr (ohne Proxy) wird normal transferiert. Peer-to-Peer- und Filesharing Anwendungen (wie KaZaA, Napster, Morpheus etc.) müssen mit einer stark erniedrigten Priorität vorlieb nehmen. Gleichzeitig ist der Datenverkehr der angeschlossenen Studentenwohnheime ins Internet auf einen Anteil von 25 Prozent begrenzt. Nähere Informationen über die Art und den Umfang der Einschränkungen finden sich auf den Info-Seiten des RZ (siehe Linkslage). *Volker Riedel*



LINKSLAGE

Nähere Infos zu den Artikeln im Web

Skillspace
<http://www.ruhr-uni-bochum.de/skillspace/>

FACTScience
<http://www.ruhr-uni-bochum.de/fact>

Informationen zu DFN@Home
<http://www.dfnhome.net>

Informationen zur Bewirtschaftung des Datenverkehrs
<http://www.ruhr-uni-bochum.de/rz/dienste/netze/gwin/>

Immatrikulation
<http://www.tldevelop.com>
<http://www.c-vis.com>
<http://www.geniusbytes.com>

ITAusbildungsberufe
<http://www.rub.de/fachinformatik/>

Dekanatsdisketten online
<http://www.rub.de/verwaltungssoftware>

Rechtliche Bedeutung von „Disclaimer“ auf Homepages
<http://www.dfn.de/service/ra/checkliste/Disclaimer.html>

Institut für Informations-, Telekommunikations- und Medienrecht (ITM), Universität Münster
<http://www.uni-muenster.de/Jura.itm/ie.html>

Skriptum Internet-Recht (Prof. Hoeren Stand: Oktober 2002)
<http://www.uni-muenster.de/Jura.itm/hoeren/material/Skript.pdf>

DFN-Kompetenzzentrum Recht
<http://www.dfn.de/service/ra/home.html>

Zooming-Server
<http://RuhrUniBochum.de/rz/dienste/ressourcen/fs/zoom>

Lizenzen
<http://www.ruhr-uni-bochum.de/rzalt/software/rubdesign/>

Scanfoto: Felix Freiler

RZ NEUE VERSION

Blackboard kann jetzt viel mehr

Seit dem Start von Blackboard im November 2000 hat die Web-basierte Lehr-/Lernumgebung an der RUB erfolgreich Karriere gemacht: Nach anfänglichem Zögern waren immer mehr Dozenten von seinen Funktionen überzeugt, inzwischen sind 240 Kurse und 2.800 Studierende im System eingetragen. Das hat das Rektorat bewegt, Blackboard auch in den nächsten Jahren weiter zu unterstützen. Statt der bisherigen "Entry-Version" läuft ab jetzt die "Enterprise-Version". Außerdem wurde der neue Lizenzvertrag so gestaltet, dass auch die Bochumer weiterführenden Schulen das System nutzen können.

Blackboard bietet neben der strukturierten Bereitstellung von Informationen auch Kommunikationselemente wie E-Mail, Newsgroups, Chat und Whiteboard für alle Kursteilnehmer oder auch für einzelne Arbeitsgruppen. Die neue Version kann noch mehr: Zum einen ist sie besser in die IT-Umgebung der Hochschule zu integrieren. So kann die Software Studierendendaten aus der Studierendendatenbank der Uni übernehmen, und Nutzer können sich über ihre LoginID und ihr Passwort vom Rechenzentrum bei Blackboard anmelden. Eine weitere wesentliche Neuerung ist zum anderen die Mehrsprachigkeit des Systems. Studierende können sich für die Menü-Führung selbst eine Sprache auswählen.

Durch diese Erweiterungen am System kann die Software nicht mehr wie bisher auf dem zentralen WWW-Server der Universität laufen. Deshalb hat das Rechenzentrum eigens für Blackboard einen neuen, leistungsfähigen Server beschafft, der es erlaubt, 40.000 Studierende/Schüler und 5.000 Kurse zu verwalten. Die neue Blackboard-Version ist bereits verfügbar; Kurse, die in der alten Version angeboten wurden, sind auch in der neuen zugänglich. **Völker Riedel**

Alle Jahre wieder ein Kraftakt



Foto: Babette Sponheuer

IUK IMMATRIKULATION - DER ABLAUF

Jedes Jahr im September ist es wieder so: Innerhalb von vier Wochen müssen die Mitarbeiter des Studierendensekretariats den Hauptantrag der neuen Erstsemester (dieses Jahr 4.385 Leute) für das Wintersemester an der RUB immatrikulieren. Dieser Kraftakt stellt natürlich hohe Ansprüche an Mensch und Technik. Die Datenverarbeitungs-Infrastruktur wurde daher mit dem Ziel entwickelt, die zugrundeliegenden Prozesse zu optimieren und zu integrieren und gleichzeitig möglichst einfache, im Bedarfsfall schnell ersetz- oder kopierbare Arbeitsplätze zu haben.

Menügeführte Erstsemester

Herzstück dieses Konzepts ist ein Application-Server der Firma Techno Logic Development (s. Linkslage), an dem Rechnerarbeitsplätze hängen, die wahlweise sowohl als Studierenden- als auch als Sachbearbeiterplatz dienen können. An einem Studierendenplatz können die künftigen Erstsemester menügeführt ihre persönlichen Daten selbst eingeben, vereinfacht durch die Möglichkeit, Name, Anschrift und Krankenversicherungsdaten von der Versichertenkarte einzulesen zu können. Außerdem können sie sich hier mit einer einfachen WebCam fotografieren – ein Passbild müssen sie nicht mehr mitbringen. Den richtigen Bildausschnitt aus dem Kamerabild wählt die

Immatrikulations-Software automatisch mit Hilfe des FaceSnap® -Moduls der Firma C-VIS (s. Linkslage), das mit Gesichtserkennungsalgorithmen arbeitet.

Diese erste Station entfällt für Studierende, die sich über einen Zulassungsbescheid (der RUB oder der ZVS in Dortmund) einschreiben wollen. Viele Daten sind in diesem Fall bei der Antragstellung an der RUB schon erfasst bzw. von der ZVS übermittelt, so dass der Sachbearbeiter sie anhand des Zulassungsbescheids einfach aufrufen kann. Am Sachbearbeiterplatz ruft ein Sekretariatsmitarbeiter nun die eingegebenen Daten auf und vervollständigt sie nach entsprechender Beratung. Auch hier kann noch per WebCam ein Bild generiert werden; mit einem speziellen Stativ können hierbei auch ganz normale Passfotos als Quelle dienen, die jetzt nicht mehr aufwändig gescannt werden müssen.

Fotos nicht mehr mitbringen

Sind alle benötigten Daten erfasst, wird durch einen einzigen Knopfdruck die Matrikelnummer vergeben, ein Account in der Kundendatenbank des RZ erzeugt, und alle Dokumente (z.B. der Immatrikulationsantrag) werden gedruckt. Ist dieser Antrag vom Studierenden unterschrieben, wird "immatrikuliert" – alle Daten werden in die richtigen Tabellen übertragen und ein Auftrag zur Er-

stellung eines Studierendenausweises in der Datenbank erzeugt. Benötigt der Sachbearbeiter noch weitere Funktionen, kann er über einen CITRIX-Server der Verwaltung alle sonstigen Sekretariatsprogramme aufrufen. Die Ausweise erstellen automatisch zwei Druckserver der Firma Genius-Bytes (s. Linkslage). Diese Druckplätze holen sich anhand eines Druckauftrags selbständig die Daten aus Studierenden- und RZ-Datenbank, um den Chip zu beschreiben und die Oberfläche zu bedrucken. Von GeniusBytes stammt auch die SB-Terminal-Software.

Application-Server bringen für ein Projekt wie die Einschreibung immense Vorteile: Zum einen sind die Arbeitsplatzrechner einfach einzurichten – aufwändige Software-Installationen und Konfigurationen sind nur einmal auf dem Server nötig. Bei Problemen sind die einzelnen Rechner zügig und ohne Fachwissen ersetzbar. Zum anderen lässt sich solch ein System leicht anpassen: Die Anzahl der Arbeitsplätze ist nur durch die Leistungsfähigkeit des Servers und noch eher durch die Anzahl der verfügbaren Mitarbeiter begrenzt. Die enge Zusammenarbeit von Institutionen wie RZ oder ZVS vereinfacht den Ablauf weiter, weil Daten nur einmal erfasst werden müssen.

Als nächsten Schritt plant die RUB die Online-Immatrikulation. Neue Studierende sollen sich im Idealfall ohne Wartezeiten nur noch ihren Ausweis vor Ort abholen müssen. **Michael Ernst**



Foto: Babette Sponheuer

FACTSCIENCE BEI DEN MEDIZINERN

Leistungen online

Den Überblick über die vielfältigen Forschungsaktivitäten an der Medizinischen Fakultät behält seit Sommer 2002 FACTScience. Das neue Intranetportal ist ein Informations- und Organisationssystem, mit dessen Hilfe die Fakultät Forschungsleistungen dezentral

erfassen und leistungsbezogen prämiieren kann. Mit seiner Anschaffung führen die Mediziner ihren 1996 eingeschlagenen Kurs fort.

Die Hauptfunktion von FACTScience ist es, Leistungen im Wissenschaftsbetrieb und deren Bewertung zu erfassen und auszuwerten. Dazu zählen Drittmittelwerbungen und zukünftig auch Publikationsleistungen der Autoren sowie deren Bewertung über Zitationskennzahlen, Publikationsanteile und Fachkategorien. Zusätzlich können weitere Leistungskennzahlen oder Bezugsgrößen flexibel zur Evaluation herangezogen werden. Zu diesem Zweck kann FACTScience die Struktur von Einrichtungen und Projekten sowie die Daten von Personen, ihren Rollen und Publikationen und auch von Lehrveranstaltungen verwalten.

Das Programm ist somit ein umfassendes Analysewerkzeug zur Leistungsbewertung und leistungsorientierten Mittelvergabe für Einrichtungen und Wissenschaftler der Medizinischen Fakultät. Es analysiert die verschiedenen Leistungsinformationen und ermöglicht es, zu vergleichen und verschiedene Evaluationsmodelle einzusetzen. FACTScience fasst Daten, die bisher an der Fakultät häufig getrennt oder sogar mehrfach geführt wurden, zentral zusammen, was die gesamte Datenverwaltung der Fakultät vereinfacht.

Damit die Fakultätsmitarbeiter die Software nutzen kann, muss das Rechenzentrum die entsprechenden Dienste gesondert freischalten. Das RZ übernahm auch die Programmierung einer speziellen Schnittstelle zwischen Benutzerverwaltung und FACTScience, die für die Zugangskontrolle zum System notwendig war. Die Entwicklung der Software durch die Aachener Firma FACT erfolgte in enger Abstimmung mit der Humboldt-Universität und der Universitätsklinik Charité zu Berlin. **Thorsten Wiethage**

RZ NEUE MICROSOFT-SOFTWARE-LIZENZEN

Verträge zur Software

Die RUB hat mit der Firma Microsoft einen neuen Lizenzvertrag zur Beschaffung von Softwareprodukten (Select 5 mit einer Laufzeit bis zum 30.06.2004) abgeschlossen. Das ist das Lizenzprogramm für Kunden aus Bildung, Forschung und Lehre mit großem Softwarebedarf. Sie können damit Software von Microsoft für Ihre Einrichtung schneller beschaffen, günstiger erwerben und einfacher verwalten und darüber hinaus sicher sein, dass Sie die rechtlichen Lizenzbedingungen einhalten. Die Lizenzen aus diesem Vertrag können nur über unseren Kooperationspartner der ASKNET AG erworben werden. Bereits beim Kauf einer Software lohnt es sich, zu überlegen, wie man sie nutzen will. Nur so kann man am besten entscheiden, für welche Lizenz man sich entscheidet.

Bei Microsoft gibt es z.Z. folgende Lizenzarten: **License:** Recht, die zur Zeit des Lizenzvertrags aktuelle Version zeitlich unbefristet zu nutzen. **Software Assurance:** Recht, die während der Laufzeit des Lizenzvertrags aktuellen Versionen zeitlich unbefristet zu nutzen (zum Preis von ca. 30 % des Softwarepreises pro Jahr).

License & Software Assurance Package: Kombination von License und Software Assurance in einer Artikelnummer (SKU).

Dabei ist wichtig, dass eine Software Assurance nur zeitgleich mit einer neuen Lizenz oder im Anschluss an bereits bestehende Software Assurance erworben werden kann. Die Software Assurance kann immer nur für ein ganzes Jahr gekauft werden und endet automatisch mit dem Ende des Selectvertrages. Das bedeutet auch, dass ein Softwareupdate nur noch über die Software Assurance zu erhalten ist. Wenn also nicht immer das aktuellste Produkt benötigt wird, reicht es, bei Bedarf eine Neu-Lizenz zu erwerben.

Für Interessenten, die immer die aktuellen Office-Produkte einsetzen möchten, gibt es auch die Möglichkeit eines Campus-Vertrages, der immer für ein ganzes Institut bzw. Lehrstuhl abgeschlossen werden muss. Nähere Infos dazu stehen im Netz (s. Linkslage). Der aktuelle Vertrag läuft bis März 2003 und wird dann wieder für ein Jahr verlängert. Anfang 2003 gibt es daher wieder eine Umfrage, um den aktuellen Bedarf zu ermitteln. **Lothar Schäfer**

SICHERHEITSLAGE

Zwanzig kritischste IT-Sicherheitslücken

<http://www.sans.org/top20/>

SANS (SysAdmin, Audit, Network, Security) Institute
<http://www.sans.org/aboutsans.php>

Common Vulnerabilities and Exposures (CVE)
<http://cve.mitre.org/>

IT-Sicherheitsforum der RUB
<http://www.ruhr-uni-bochum.de/sec/forum>

Schulungen zur IT-Sicherheit
<http://www.ruhr-uni-bochum.de/sec/forum/schulungen/schulungen.htm>

Leitlinie zur IT-Sicherheit
<http://www.ruhr-uni-bochum.de/sec/forum/leitlinie.pdf>



Die neue Zooming-Server-Software der Firma MGI erlaubt verschiedene Darstellungen ein und desselben Bildes, das auf dem zentralen WWW-Server der RUB liegt: Bilder können in verschiedenen Größen, Auflösungen, Ausschnitten, Kontrastangaben und vielen anderen Attributen dargestellt werden, wobei nur ein Original – dieses allerdings in voller Schönheit (Auflösung) – abgelegt werden muss. Die Darstellungsattribute sind in der Internetadresse festgelegt. Der Betrachter kann außerdem an einer selbst gewählten Position in das Bild hineinzoomen. Mehr dazu im Internet, s. Linkslage.

schließt die Fakultät für Elektrotechnik und Informationstechnik der RUB mit dem international einzigartigen Diplomstudiengang „Sicherheit in der Informationstechnik“. Die breite Ausbildung basiert auf den drei Säulen Informatik, Elektro- und Informationstechnik und IT-Sicherheit. Schon das erste Semester beginnt mit Vorlesungen über die Grundlagen der Kryptographie, Daten- und Systemsicherheit. Parallel finden Laborpraktika statt, in denen z. B. Firewalls konfiguriert oder Smart Card Systeme angegriffen werden. Im Hauptstudium gibt es Spezialvorlesungen zu IT-Sicherheitsthemen. Die zweite Säule der Ausbildung bilden Vorlesungen aus der Informatik, u.a. Softwaretechnik, Netzwerke und Programmiersprachen. Dritte Säule ist eine solide Ausbildung in den technischen, d.h. ingenieurwissenschaftlichen Fächern wie Computertechnik, Chipdesign und Nachrichtentechnik. Praxisnah macht das Studium ein Fachpraktikum in einem spezialisierten IT-Sicherheitsunternehmen. Zahlreiche Firmen aus dem In- und Ausland haben bereits Interesse an der Kooperation mit dem Studiengang und dem Horst-Görtz-Institut für IT-Sicherheit bekundet.

TUK NEUE CITRIX-SERVER SIND ONLINE

Immer sicherer Zugriff

Seit Sommer ist in der Verwaltung der RUB die aktuelle Version der Terminalserver-Software Meta-Frame der Firma Citrix in Betrieb. Die neue Version läuft nicht mehr unter Windows NT, sondern unter Windows 2000 Server. Diese neue Lösung erlaubt es, Benutzern im Netzwerk ununterbrochenen und sicheren Zugriff auf Anwendungen zu gewähren. Dabei spielt es fast keine Rolle, mit welcher Hardware und welchem Betriebssystem der einzelne Rechner des Nutzers ausgestattet ist, da es für nahezu jede Kombination einen ICA-Client (Independent Computing Architecture) gibt. Anwendungen, die den Benutzern zugänglich sein sollen, müssen zunächst auf den beiden Citrix-Servern installiert werden. Sie bilden als sog. Server-Farm eine Einheit und können somit eine Lastverteilung durchführen. Danach wird die Software



veröffentlicht und erscheint im ICA-Client der berechtigten Anwender. So stehen z. B. die Personal- und Vorlesungsverzeichnis-Software i3v, das Zeitmanagement-Tool TaskTimer und diverse RUB-interne Programme zur Haushaltsverwaltung über die Citrix-Server zur Verfügung. Im Rahmen des Sicherheitskonzepts "Technischer Datenschutz für die Verarbeitung personenbezogener Daten", das das Dez. 6 entwickelt hat, spielt diese Terminalserver-Architektur eine zentrale Rolle: Alle Programme, die zur Verarbeitung personenbezogener Daten an der RUB benutzt werden, sind auf dem Server installiert. Über ICA-Clients haben nur berechnete Mitarbeiter an ihren Rechnern Zugriff darauf. Die Kommunikation zwischen Terminalserver und ICA-Client erfolgt hochverschlüsselt. Die Datenbank mit den personenbezogenen Daten ist somit nur vom Terminalserver aus erreichbar. *Marcus Klein*

EUROBITS HGI UND GITS AG

IT-Sicherheit auf zwei Säulen

Die Idee entstand 1999: Ein Kompetenzzentrum für IT-Sicherheit in Bochum (EUROBITS), bestehend aus zwei Säulen, einem "In-Institut" in Form einer zentralen wissenschaftlichen Einrichtung der RUB, und einem "An-Institut", der Gesellschaft für IT-Sicherheit (GITS AG). Die GITS AG wurde Anfang des Jahres gegründet und hat ihren Sitz im Gebäude für IT-Sicherheit direkt neben dem RUB-Campus. Auf dem Weg von der Idee zur Verwirklichung hatte EUROBITS einen entscheidenden Helfer: Horst Görtz, Gründer der Firma Utimaco, die auf dem Gebiet IT-Sicherheit seit vielen Jahren etabliert ist, hat das Projekt durch eine großzügige Spende ermöglicht. Das In-Institut trägt heute seinen Namen: "Horst Görtz Institut für Sicherheit in der Informationstechnik" (HGI). Kern des HGI sind drei Lehrstühle der RUB: Einer in der mathematischen Fakultät (Prof. Dr. Hans Dobbertin) und einer in der Fakultät für Elektrotechnik und Informationstechnik (Prof. Dr. Christof Paar) sind seit Oktober 2001 besetzt, ein weiterer wird in Kürze besetzt. Diese Lehrstühle vertreten die Grundlagen und technischen Aspekte der IT-Sicherheit. Teil des HGI ist außerdem das "Institut für Sicherheit im e-Business" der Wirtschaftswissenschaftler der RUB. Eine Erweiterung des HGI durch Experten der Rechts- und Sozialwissenschaften ist in nächster Zeit vorgesehen. Derzeit

wird schon ein Drittmittelprojekt, das sich mit der Sicherheit von Infrastrukturen in der Bundesrepublik befasst, interdisziplinär bearbeitet.

Internationale Projekte

Das HGI arbeitet bereits in zahlreichen nationalen und internationalen Forschungs- und Industrieprojekten. In der Aufbauphase des ersten Jahres hat es bereits Drittmittel von mehr als 400.000 Euro u.a. von den Sun Research Labs in Silicon Valley und dem Bundesamt für Sicherheit in der Informationstechnik eingeworben. Das HGI ist auch Mitinitiator von zwei strategisch bedeutsamen EU-Projekten, die den Aufbau eines europäischen "Networks of Excellence" im Bereich IT-Sicherheit und die Festlegung einer "Roadmap Cryptography 2010" zum Ziel haben. Das HGI ist in seiner Art eine einzigartige Einrichtung auf deutscher und internationaler Ebene durch die Kooperation von erstklassigen technischen Experten mit dem Institut für Sicherheit im e-Business, Sozialwissenschaftlern und Juristen. Der neue Studiengang Sicherheit in der Informationstechnik (siehe Artikel „Studieren für das 21. Jahrhundert“) ist ebenfalls der erste seiner Art. Die Zusammenarbeit mit der GITS AG rundet das innovative Profil des HGI ab. *Hans Dobbertin, Christof Paar*

Studieren für das 21. Jahrhundert

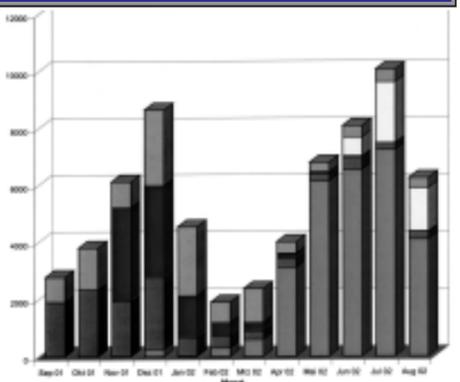
EUROBITS IT-SICHERHEIT

Seit Jahren machen der "I love you" Virus, Attacken gegen Internetseiten, Hackereinträge in Regierungcomputer, gefälschte Telefonkarten und Cyberterrorismus Schlagzeilen. Und diese IT-Sicherheitsprobleme sind nur die Spitze des Eisbergs: fast jeder Netzwerkadministrator kann von Angriffen berichten. Sicherheit hat daher in fast allen zukünftigen IT-Anwendungen große Bedeutung, und der Bedarf an Fachkräften ist hoch. Dem steht bisher allerdings nur ein wenig entwickeltes Ausbildungsangebot gegenüber. Die meisten Hochschulen bieten keine oder nur wenige Spezialvorlesungen zur IT-Sicherheit an. Diese Lücke

Viren keine Chance

RZ FILTER AUF DEM MAILHOST

Seit August 2001 untersucht ein Virenfilter alle über den Mailhost transportierten Mails auf Viren. Bei Befall werden sie nicht zugestellt, sondern der Absender (und der Empfänger, falls an der RUB) benachrichtigt. Die Filterung hat sich als sehr erfolgreich herausgestellt: Pro Monat wurden bis zu 10.000 Viren-Mails aussortiert. Wie das Diagramm zeigt, folgen die Virenmails in Wellen der Aussetzung neuer gefährlicher Viren. Im Augenblick gibt es eine abflauende "Klez"-Welle und eine "Yaha"-Welle auf dem Höhepunkt. Das Bild zeigt leider auch, dass sehr viele Rechnerbenutzer sich immer noch nicht ausreichend vor Viren schützen. *Jost Krieger*



BIT

Top-20 der Sicherheitslücken

Die Top-20 der IT-Sicherheitslücken – zehn für Windows- und für Unix-Systeme – haben die US-Bundespolizei FBI und das SANS-Institut nun veröffentlicht: Nutzer können ihr eigenes System auf Sicherheitslöcher überprüfen und die Auswirkungen evtl. entdeckter Lücken unter sog. CVE- bzw. CAN-Nummern im Internet nachsehen. Mehr dazu im Netz s. Sicherheitslage.

IMPRESSUM

Herausgeberin: Pressestelle der Ruhr-Universität Bochum;
Leiter: Dr. Josef König (v.i.S.d.P.);
Redaktion: Meike Drießen, md; Hanspeter Zoller, hpz;
Koordination: Meike Drießen, Hanspeter Zoller, RZ;
Redaktionsanschrift: Pressestelle der RUB, UV 3/366, 44780 Bochum, Tel.: 0234/32-23999, -22830, Fax: 0234/32-14136, Internet: <http://www.ruhr-uni-bochum.de/pressestelle>;
Layout und Satz: bsp Bildesign, Babette Sponheuer, Bochum;
Layoutkonzept: Tradeland GmbH, Kirchharpener Str. 52, 44805 Bochum, Tel.: 0234/92282-0, Fax: 0234/92282-33;
Anzeigenverwaltung und -herstellung: Alpha-Informationssysteme mbH, Finkenstraße 10, 68623 Lampertheim, Verkaufsleitung: Peter Asel, Tel. 06206/939-0.
Anzeigenschluss für Ausgabe 11 (Juni 2003) ist der 5. Mai 2003; Mediadaten: <http://www.ruhr-uni-bochum.de/rubens/mediadat.htm>
RUBbits erscheint zweimal pro Jahr als Service-Beilage zu RUBENS, Zeitschrift der Ruhr-Universität Bochum (<http://www.ruhr-uni-bochum.de/RUBbits>).
Namentlich gekennzeichnete Beiträge gehen nicht unbedingt die Meinung der Redaktion wieder. Anfragen und Mitteilungen per E-Mail: rubbits@ruhr-uni-bochum.de
Auflage: 15.000