Inhalt

IT-Sicherheit – was ist das?

Christian Rossa

Einleitung

In der modernen Informations- und Kommunikationsgesellschaft ist der Einfluss der Informationstechnik (IT) nahezu in allen Bereichen zu spüren. Die Komplexität des gesamten IT-Bereichs ist heute selbst für Experten nur noch sehr schwer zu überschauen. Die Innovationszyklen der IT-Produkte werden immer kürzer, die Vielzahl der installierten IT-Produkte nimmt stetig zu und der Umfang der über die Medien transportierten Informationen wächst unaufhaltsam.

Da die Hochschulen auch bei der Entwicklung und der Einführung der Informationstechnik eine Vorreiterrolle übernommen haben, gibt es an der Universität Würzburg schon seit Jahren keinen Bereich mehr, der sich nicht irgendwelcher IT-Produkte zur Bewältigung seiner Aufgaben bedient. Die Abhängigkeit ist mittlerweile so groß, dass man ohne Übertreibung behaupten kann, dass die meisten Einrichtungen der Universität ohne den Einsatz der Informationstechnik in ihrer Arbeit stark beeinträchtigt wären – angefangen bei der Zentralverwaltung mit der Verwaltung der Studierenden und der Mitarbeiter über die naturwissenschaftlichen bis hin zu den geisteswissenschaftlichen Einrichtungen.

Spektakuläre Vorfälle wie der Melissa-Virus, der Loveletter-Virus, der SQL-Slammer-Wurm oder Einbrüche in große Firmennetze lassen weite Kreise aufhorchen. Solche Ereignisse zeigen sehr deutlich, welchen Gefahren die IT-Systeme (Rechner, Programme und Daten) ausgeliefert sind. Nachdem oben auf die zentrale Rolle der Informationstechnologie innerhalb der Universität Würzburg hingewiesen wurde, stellt sich die berechtigte Frage, welcher Stellenwert hier nun der Sicherung der IT-Strukturen zukommt.

Bedrohungen

Die Gefahren für die IT-Systeme können aus sehr unterschiedlichen Bereichen kommen. Im Folgenden sollen die sicherlich größten Gefahrenquellen kurz beleuchtet werden – *Hacker* und *Viren*.

Die Bedrohungen der IT-Ressourcen durch Hacker werden nach den Erkenntnissen des Rechenzentrum immer noch nicht ernst genug genommen. Einerseits verfügen Einrichtungen der Universität ebenso wie hochsensible Industrieunternehmen über besonders schützenswerte, teilweise sogar sicherheitsrelevante Daten, andererseits reklamieren sie für sich die Freiheit von Lehre und Forschung und pochen auf ihre hohe Selbständigkeit.

Angreifer haben oft leichtes Spiel, denn die meisten Einrichtungen sorgen nur mangelhaft vor. Nach Beobachtungen eines Consulting-Unternehmens, das bereits seit 1998 jährlich Untersuchungen zur Informationssicherheit durchführt, zielen im Internet weit über 80% der Angriffe auf altbekannte Schwachstellen, für die es bereits Abhilfen (Patches) gibt. Nach Untersuchungen einer US-Behörde hat sich die Anzahl der bekannten Sicherheitslücken in den beiden letzten Jahren fast vervierfacht – von etwa 1.100 auf rund 4.100. Die Beobachtungen des Rechenzentrums von Anfang 2003 zeigen, dass im Hochschulnetz derzeit sehr viele Rechner pro Tag im Mittel zwischen 10 und 20 Einbruchsversuche über eine einzige bekannte

Schwachstelle zu verzeichnen haben. Multipliziert man dies mit der Anzahl der Rechner im Hochschulnetz und der Anzahl der bekannten Sicherheitslöcher, dann ist anzunehmen, dass die tatsächliche Anzahl der Einbruchsversuche pro Tag im Hochschulnetz vermutlich im fünfstelligen Bereich liegt. Folglich ist davon auszugehen, dass die Zahl der erfolgreichen Computer-Einbrüche in den letzten Jahren dramatisch zugenommen hat. Wie viele Hacker-Angriffe tatsächlich erfolgreich verliefen, kann das Rechenzentrum nicht sagen, da die Systemverantwortung für die meisten IT-Ressourcen in den Fachbereichen/Instituten und Einrichtungen liegt.

Das Gefahren-Spektrum eines erfolgreichen Hacker-Angriffs reicht von den Risiken für das Erscheinungsbild und den Ruf der Universität über den Vertrauensverlust bis hin zum Verlust von Daten und der Verfügbarkeit der IT-Ressourcen. Es entsteht beträchtlicher Aufwand für die Wiederherstellung der System- und Anwendungsumgebung und die eventuelle Rekonstruktion der Daten.

Die Gefahren durch Computer-Viren konnten im Hochschulnetz durch die Inbetriebnahme eines zentralen E-Mail-Virenscanners und die Zentralisierung der E-Mail-Ströme deutlich reduziert werden. In Abhängigkeit von der akuten Ausbreitung von „Virus-Epidemien“ werden derzeit pro Tag aus dem gesamten E-Mail-Aufkommen der Universität zwischen 200 und 1.200 verseuchte E-Mails ausgefiltert. Trotzdem sollten die Gefahren, die durch Viren den IT-Systemen der Universität weiterhin drohen, nicht unterschätzt werden, da die Nutzung mobiler Geräte stark zunimmt.

Was ist zu tun?

Aufgrund der zentralen Rolle der Informationstechnologie an der Universität Würzburg muss auch der Sicherung der IT-Strukturen ein entsprechender Stellenwert zukommen. Klar muss sein, dass es keinen hundertprozentigen Schutz geben kann und dass IT-Sicherheit nicht allein durch technische Maßnahmen erreicht werden kann. Eine nicht zu unterschätzende Bedeutung kommt den erforderlichen organisatorischen Maßnahmen zu. Der Sensibilisierung und der Schulung zur bewussten Nutzung der IT-Ressourcen muss ein entsprechender Rahmen eingeräumt werden.

Eine Schlüsselrolle fällt im IT-Sicherheitskonzept der Universität der qualifizierten und kompetenten Betreuung der IT-Ressourcen zu. Folgt man den Empfehlungen des Betreuungskonzepts (siehe Artikel „Maßnahmen zur Erhöhung der IT-Sicherheit an der Universität Würzburg“), dann sollte in Zukunft die Verantwortung für die Betreuung der IT-Systeme ausschließlich in den Händen hauptamtlicher Fachkräfte liegen und nicht durch Hilfskräfte, „Computer-Freaks“ oder nebenbei erledigt werden.

Diese Erwartung kommt auch in der Empfehlung der Hochschulleitung an die Fachbereiche vom Herbst 2001 zum Ausdruck. Der sorglose Umgang Einzelner untergräbt die ernsthaften Bemühungen all derer, die sich der Sicherheitsproblematik bewusst sind. Umgekehrt profitieren von den positiven Auswirkungen einer qualifizierten Betreuung der IT-Systeme auf die IT-Sicherheit nicht allein die direkt betroffene Einrichtung, sondern indirekt auch alle anderen Teile der Universität. Durch eine kompetente Betreuung der IT-Systeme wird die Wahrscheinlichkeit, über gehackte Systeme Einfluss auf andere Rechner im Hochschulnetz zu nehmen, zumindest deutlich reduziert. Das macht deutlich, dass hier die Solidarität aller dringend gefordert ist. Den Kopf in den Sand zu stecken ist verantwortungslos: sowohl gegenüber dem Steuerzahler als auch gegenüber den restlichen Einrichtungen der Universität.

Doch ebenso wichtig ist es, dass die Bemühungen der Einrichtungen durch ein Bündel zentraler Maßnahmen unterstützt werden. Dazu zählen neben dem Betrieb zentraler technischen IT-Sicherheitskomponenten (z.B. Firewall-Anordnungen) in erster Linie Schulungsmaßnahmen und Unterstützung der IT-Experten in den Einrichtungen der Universität in den Bereichen Systemadministration und Umsetzung von IT-Sicherheitsmaßnahmen.

Sniffer, Hacker, Firewalls

Markus Krieger, Hartmut Plehn

Meldungen und Berichte in den Medien, die anhand aktueller Vorfälle die Unsicherheit des Internets beklagen, sorgen vielerorts für größere Unruhe. Auch an der Universität Würzburg wurden in den letzten Monaten etliche Rechner bereits Opfer von elektronischen Eindringlingen (Hackern), die sich über das Internet unerlaubten Zugang zu den Rechnern verschafft haben. Der folgende Artikel versucht, soweit fürs Verständnis erforderlich, die technischen Grundlagen über die im Internet verwendete Protokoll-Familie TCP/IP (Transmission Control Protocol/ Internet Protocol) zu vermitteln, die typische Arbeitsweise der Hacker an einem Beispiel zu verdeutlichen und die Funktionsweise einer Firewall zu durchleuchten.

IP-Adressen und Ports – Hausnummern und Briefkästen

Im Internet erfolgt der Austausch von Datenpaketen zwischen Endgeräten (*Clients*) und Dienste-Rechnern (*Servern*) über das Internet-Protokoll (IP). Damit die Datenpakete vom Quell- zum Zielrechner und die Antwortpakete auch zurück finden, sind in jedem Datenpaket die „Hausnummern" der beiden Rechner, die so genannten *IP-Adressen*, enthalten. Der WWW-Server der Universität hat beispielsweise die IP-Adresse 132.187.3.5. Da es für die meisten Benutzer unmöglich ist, sich die Unzahl der aus vier Bytes bestehenden IP-Adressen zu merken, sorgen *Domain Name Server* dafür, dass in Endanwendungen Internet-Namen wie www.uni-wuerzburg.de statt IP-Adressen eingegeben werden können. Kaum jemand ruft die Homepage der Universität mit der WWW-Adresse http://132.187.3.5/ statt mit http://www.uni-wuerzburg.de/ auf, obwohl in beiden Fällen dieselbe Seite zurückgeliefert wird.

Die IP-Adressen stellen lediglich die Wegfindung von Paketen zwischen den Rechnern im Internet sicher. Auf einem Server werden oft viele unterschiedliche Dienste nebeneinander bereitgestellt. Die Unterscheidung dieser Dienste erfolgt anhand einer eindeutigen, als *Port* bezeichneten „Briefkastennummer". Für viele im Internet verwendeten Dienste wird über so genannte RFCs (Requests for Comments), die von der IETF (Internet Engineering Task Force) verabschiedet werden, festgelegt, was in den Datenpaketen eines bestimmten Dienstes stehen muss oder darf. Die Tab. 1 zeigt einige wichtige Dienste und Protokolle sowie die Ports, unter denen Clients diese Dienste standardgemäß erwarten.

Beschreibung des Dienstes	Protokoll	Name	Port
Dateitransfer	File Transfer Protocol	ftp	21
Sichere Terminalverbindung und Dateitransfer	Secure Shell	ssh	22
Terminalverbindung	telnet	telnet	23
Vermitteln von E-Mails	Simple Mail Transfer Protocol	smtp	25
Abruf von WWW-Seiten	Hypertext Transfer Protocol	http	80
Abholen von E-Mails vom POP3-Server	Post Office Protocol (v3)	pop3	110
Abholen von E-Mails vom IMAP-Server	Internet Mail Access Protocol	imap	143
Verschlüsselnde Version von http	http over Transport Layer Security (TLS)	https	443
Verschlüsselnde Version von pop3	pop3 over TLS	pop3s	995
Verschlüsselnde Version von imap	imap over TLS	imaps	993

Tabelle 1: Einige wichtige Internet-Dienste mit den zugehörigen Port-Nummern.

IP-Datenpakete und Sniffer

Bei vielen Protokollen werden zur Kommunikation in den Datenpaketen Anweisungen in mehr oder weniger stark vereinfachter englischer Sprache verwendet. Die Inhalte der Datenpakete können mit so genannten *Paket-Sniffern* sichtbar gemacht werden. Abb. 1 zeigt beispielhaft die Funktionsweise eines Sniffers, wie er beim Abruf der Uni-Homepage die ausgetauschten Datenpakete mitprotokolliert und wieder zusammensetzt.

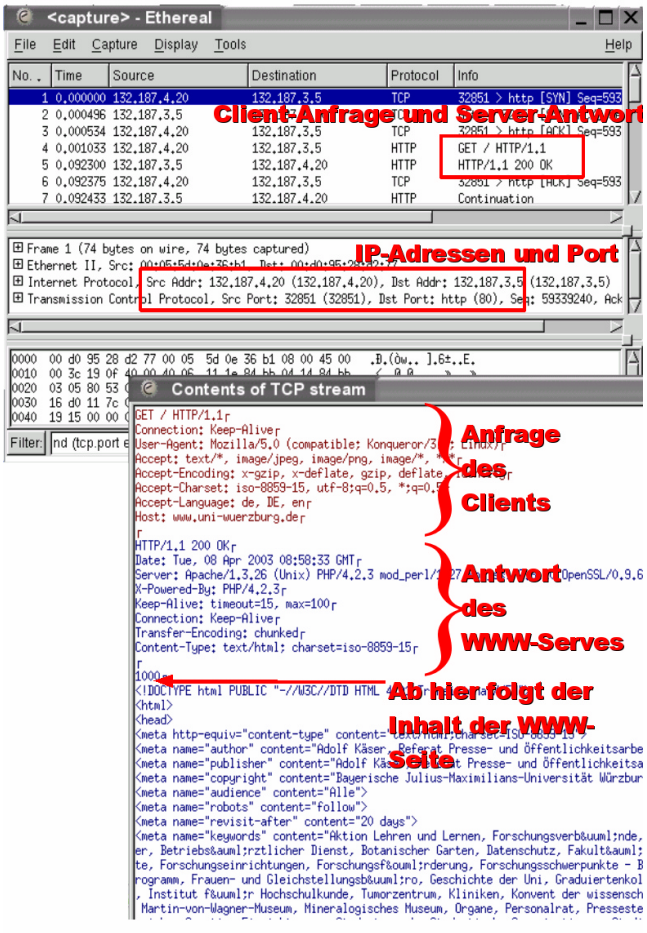

Abbildung 1: Mit einem Paket-Sniffer abgehörte Kommunikation zwischen einem WWW-Browser auf dem Rechner mit der IP-Adresse 132.187.4.20 und dem WWW-Server der Universität mit der IP-Adresse 132.187.3.5. Im oberen Bereich sieht man eine Kurzbeschreibung der Paket-Inhalte und in der Mitte den für http benutzten Port 80 sowie die beteiligten IP-Adressen. Unten sind alle zum Abruf der Uni-Homepage ausgetauschten Pakete zusammengesetzt dargestellt. Im Wesentlichen werden die von Server und Client unterstützten Parameter übermittelt, bevor der Inhalt der WWW-Seite übertragen wird. Genau dieser Text ist auch zu sehen, wenn man sich im WWW-Browser den HTML-Quelltext anzeigen lässt.

Beim Dienst http wird wie bei vielen anderen Protokollen der Inhalt der Datenpakete nicht verschlüsselt. Sie können, wie in Abb. 1 dargestellt, abgehört werden, wenn man zu einem Rechner Zugang hat, der sich im Übertragungsweg der Datenpakete befindet. Besonders kritisch ist dies bei Diensten, bei denen schützenswerte Daten, insbesondere Benutzernamen und Passwörter, übertragen werden. Daher wurden für die meisten sicherheitskritischen Dienste verschlüsselnde Varianten entwickelt (Tab. 1). Es wird empfohlen diese in jedem Falle zu verwenden, falls sie vom Client und Server unterstützt werden. In Abb. 2 ist der Inhalt der beim Aufruf der Uni-Homepage abgehörten Datenpakete dargestellt, wobei die WWW-Adresse https://www.uni-wuerzburg.de/ aufgerufen wurde und die verschlüsselnde Version *https* des http-Protokolls zur Ausführung kam.

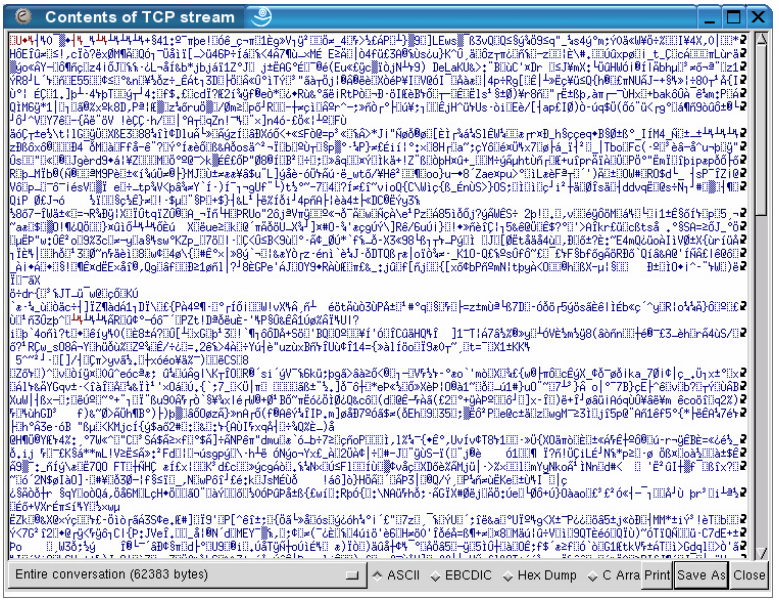

Abbildung 2: Falls der Zugriff auf eine WWW-Seite per https erfolgt, ist der Inhalt der abgehörten Pakete nicht lesbar und nach aktuellem Stand der Technik auch nicht entschlüsselbar.

Motivation der Hacker

Das Spektrum an Motivationen für Computerangriffe ist sehr breit gefächert. Da gibt es zum einen eine große Zahl neugieriger Benutzer, die im Internet auf Hackertools stoßen und diese „einfach mal“ ausprobieren wollen. Zum anderen gibt es Angreifer, die ganz gezielt versuchen in Systeme einzudringen, um sich Zugang zu deren Diensten und Ressourcen zu verschaffen. Manchmal hacken sie Rechner nur, um sie als Sprungbretter für weitere Angriffe zu verwenden und dadurch eine Zurückverfolgung zu verhindern. Nicht unterschätzen sollte man, dass Hacker durch entsprechende erfolgreiche „Hacks“ ihre Macht und ihr Können gegenüber Gleichgesinnten demonstrieren wollen und können.

Rechner an Universitäten sind für Hacker äußerst attraktive Ziele. Dies rührt daher, dass Universitätsnetze einen offenen Charakter haben und die betriebenen IT-Systeme in der Regel eher schlecht abgesichert sind. Des Weiteren sind Universitätsnetze meistens mit einer hohen Bandbreite am Internet angebunden und ermöglichen es einem erfolgreichen Angreifer von einem gehackten Rechner aus, sehr schnell große Teile des Internets abzuscannen oder anzugreifen. Bei häufig von gehackten Rechnern in verschiedenen Universitätsnetzen ausgehenden *Denial of Service* (DoS) *Attacken* werden Server anderer Betreiber mit Paketen beschossen, um gezielt Dienste lahm zu legen.

Hat ein Angreifer einen Rechner erfolgreich gehackt, kann er auf diesem beliebige Programme installieren und starten. Dabei kann es sich z. B. um *Passwort-Sniffer* handeln, mit denen der Angreifer den Datenverkehr im lo-

kalen Netzwerk des gehackten Rechners nach Account-Informationen durchsucht. Er kann einen *Keylogger* installieren, der jeden Tastendruck eines Benutzers am Rechner mitprotokolliert und an den Hacker weitermeldet. Oder er kann einen versteckten FTP-Server installieren, um auf der Festplatte des gehackten Rechners z. B. pornographisches Material oder Raubkopien von Programmen und Filmen abzulegen und diese über die schnelle Anbindung des Rechners vielen seiner „Kunden" gleichzeitig zur Verfügung zu stellen.

Unabhängig von der Motivation der Angreifer muss der Betreiber des Systems immer vom Schlimmsten ausgehen, da er nicht weiß, ob der Angreifer das System tatsächlich böswillig verändert hat oder ob er „nur mal etwas ausprobieren wollte", ohne das System zu beschädigen. Der Arbeitsaufwand zur Wiederherstellung ist für den betroffenen Betreiber in beiden Fällen gleich. Falls Backups vorhanden sind, mag eine Restaurierung möglich sein. Der Verlust der Vertraulichkeit von Forschungsergebnissen und persönlichen Daten wiegt viel schwerer und ist in der Regel nicht mehr rückgängig zu machen.

Wie arbeitet ein Hacker?

Um sich in ein Netzwerk zu hacken, muss ein Angreifer Server mit verwundbaren Diensten finden. Solche Angriffspunkte entstehen durch Fehlkonfiguration eines Dienstes oder durch Sicherheitslücken einer Serverapplikation. Dabei spielen das Betriebssystem des Servers, das Programm, welches den Dienst anbietet und seine Version eine wichtige Rolle.

Im folgenden Beispiel wird ein für Demonstrationszwecke eingerichtetes Teilnetz auf angreifbare Rechner durchsucht und das Sicherheitsloch eines WWW-Servers für einen Einbruch ausgenutzt. Der hier verwendete *Exploit* (Mechanismus zur Ausbeutung des Sicherheitslochs) basiert darauf, dass der Microsoft Internet Information Server (IIS) in älteren Versionen eine Schwachstelle hat, die es Hackern ermöglicht, durch speziell formatierte WWW-Anfragen Zugriff auf den Befehlsinterpreter cmd.exe des Windows-Servers zu erlangen und somit beliebige Kommandos ausführen zu können.

Zunächst wird das Programm nmap verwendet, um die im Subnetz 192.168.1.0 vorhandenen WWW-Server über Port 80 zu finden:

```
$ nmap –p 80 192.168.1.0/24
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
The 1 scanned port on  (192.168.1.1) is: closed
The 1 scanned port on  (192.168.1.4) is: closed
The 1 scanned port on  (192.168.1.8) is: closed
Interesting ports on  (192.168.1.20):
Port       State       Service
80/tcp     open        http
Interesting ports on  (192.168.1.107):
Port       State       Service
80/tcp     open        http
The 1 scanned port on  (192.168.1.50) is: closed
Nmap run completed -- 254 IP addresses (6 hosts up) scanned in 1
second
```

Danach wird aus den Rückmeldungen der WWW-Server durch einen normalen Zugriff bestimmt, auf welchem der Systeme ein Internet Information Server zum Einsatz kommt:

```
$ netcat 192.168.1.20 80
GET / HTTP/1.0

HTTP/1.1 200 OK
Date: Wed, 30 Apr 2003 11:32:29 GMT
Server: Apache/1.3.27 (Linux/SuSE) PHP/4.3.1
...

$ netcat 192.168.1.107 80
GET / HTTP/1.0

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Wed, 30 Apr 2003 11:40:49 GMT
X-Powered-By: ASP.NET
...
```

Im Beispiel läuft auf dem Rechner mit der IP-Adresse 192.168.1.20 der WWW-Server Apache unter Linux, der nicht das Ziel unseres Hackers ist. Der auf dem Rechner mit der IP-Adresse 192.168.1.107 laufende Microsoft Internet Information Server könnte aber verwundbar sein, falls der benötigte Sicherheits-Patch noch nicht eingespielt wurde.

Den geeigneten Exploit zum Angriff auf das ausgespähte potenzielle Opfer könnte sich der Hacker in entsprechenden Foren im Internet besorgen. Noch einfacher ist es aber, sich diese Informationen aus den Log-Dateien eines vom Hacker selbst betriebenen und nicht verwundbaren WWW-Servers „frei Haus“ liefern zu lassen. Auf jedem WWW-Server, der eine gewisse Zeit im Internet erreichbar war, findet man bei der Suche nach der Textfolge „cmd.exe“ in den Log-Dateien Angriffsversuche in Form von Zugriffen der Art

```
GET /scripts/..%255c%255c../winnt/system32/cmd.exe?/c+dir
```

Falls die mit diesem Log-Eintrag korrespondierende WWW-Anfrage

```
http://192.168.1.107/scripts/..%255c%255c../winnt/system32/cmd.exe?/c+
dir
```

im Browser den Verzeichnisinhalt des Laufwerks C:\ zurück liefert, weiß der Hacker, dass die Sicherheitslücke auf diesem System noch nicht durch das Einspielen eines Patches geschlossen wurde, weil er den Befehlsinterpreter cmd.exe mit dem Kommando dir starten konnte. Mit der Möglichkeit zur Ausführung von beliebigen anderen Befehlen auf dem Windows-Server über den Aufruf von cmd.exe ist der Server de facto vollständig unter der Kontrolle des Hackers.

Ab hier dienen die weiteren Schritte nur noch seiner Bequemlichkeit. Zunächst wird mit dem auf jedem Windows-Server verfügbaren Kommando tftp das Programm netcat auf den Windows-Server übertragen und dort gestartet. Danach kann der Hacker von seinem Arbeitsplatz aus mit diesem Programm kommunizieren und beliebige Kommandos auf dem Windows-Server ausführen lassen, als würde er als Administrator an der Eingabeaufforderung vor dem Server sitzen (Abb. 3).

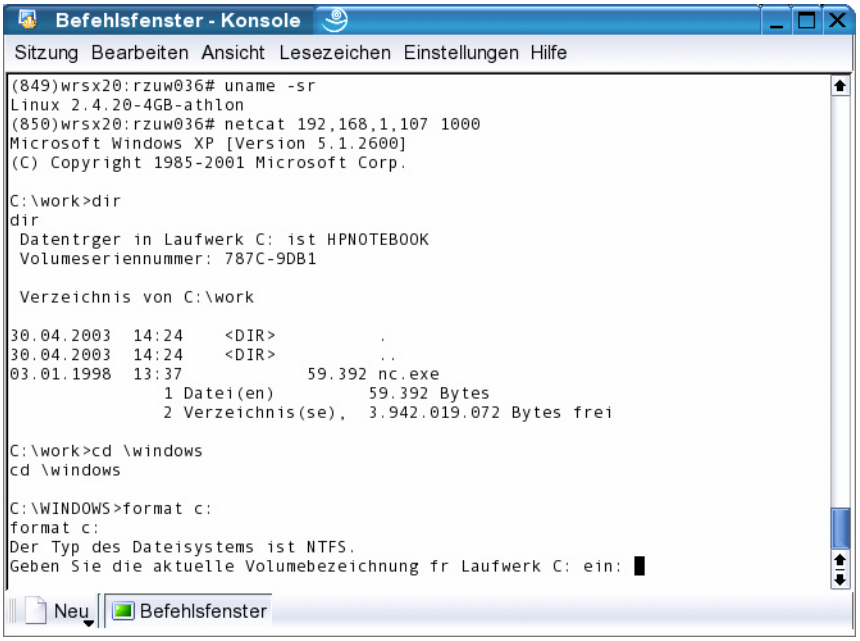

Abbildung 3: Nach der Installation des Netcat-Programms auf dem Windows-Server kann der Hacker den Server von einem beliebigen im Internet befindlichen Rechner aus per Eingabeaufforderung „administrieren". Das gezeigte Fenster ist auf dem (hier Linux-) Rechner des Hackers zu sehen. Im Beispiel wird gerade die Formatierung der Festplatte vorbereitet.

Entwicklung und aktuelles Bedrohungspotenzial

In den letzten 10 Jahren stieg sowohl die Anzahl der Rechner im Internet als auch die der Benutzer exponentiell an. Geht man von einem etwa gleich bleibenden Prozentsatz verwundbarer Rechner aus, dann hat man heute ca. 35.000 mal so viele verwundbare Rechner, die nach einem Einbruch ihrerseits für weitere Angriffe verwendet werden können.

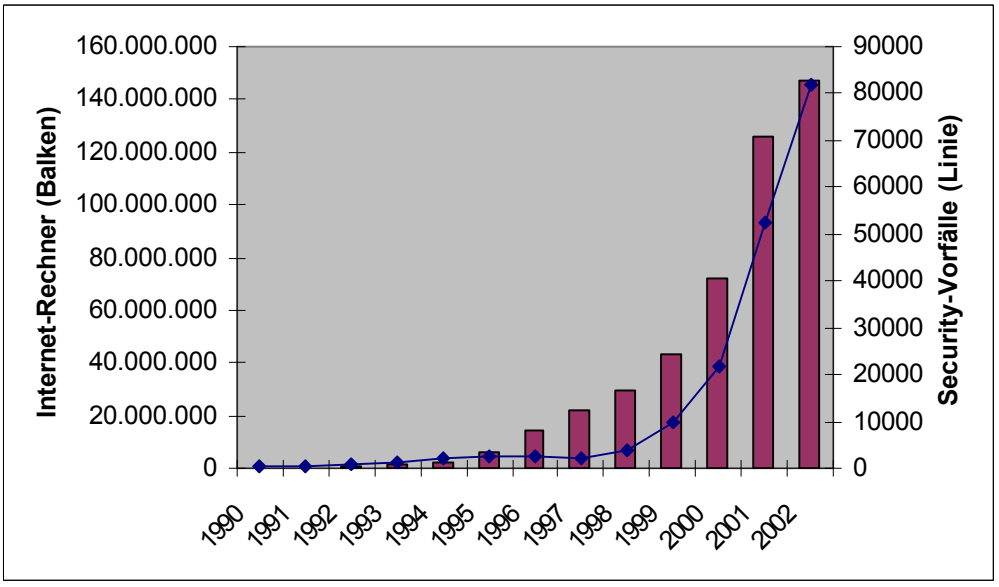

Abbildung 4: Die Anzahl der IT-Security-Vorfälle stieg in den letzten Jahren ähnlich rapide wie die Anzahl der Rechner im Internet. Die Vorfälle beziehen sich auf Meldungen, die bei einem Computer Emergency Response Team (CERT) registriert wurden und die jeweils mehrere betroffene Rechner beinhalten können.

Auch bei den Angreifern ist die Zahl exponentiell gestiegen. Dies kommt nicht nur durch den Anstieg der Benutzer im Internet, sondern vor allem durch die Verfügbarkeit von fertigen Exploits. Nur diejenigen, die eine Sicherheitslücke entdecken und passende Exploits programmieren, müssen fundierte Systemkenntnisse besitzen. Für den größten Teil der Angreifer, so genannte *Script-Kiddies*, ist es ausreichend, vorgefertigte Exploits (zum Teil mit grafischer Oberfläche) zu verwenden.

Das Netz der Universität wird rund um die Uhr gescannt und angegriffen. Früher wurden noch sehr undifferenziert alle theoretisch möglichen 65.535 IP-Adressen der Universität und alle denkbaren 65.535 Ports pro Rechner auf vorhandene Dienste abgesucht. Das war sehr auffällig und konnte durch Maßnahmen am *Wingate*, dem zentralen Zugang zum Internet, festgestellt und unterbunden werden. Heutige Utilities sind sehr viel unauffälliger. Zum einen werden Rechner vor den Scans auf ihre Erreichbarkeit getestet, um unnötige Anfragen auf nicht belegte IP-Adressen auszuschließen. Zum anderen gibt es spezialisierte Scanner, die auf jedem Rechner nach genau einem bestimmten Dienst suchen. Für einen Rechnerbetreiber ist solch ein Zugriff nicht von einer regulären Anfrage zu unterscheiden.

Das Ausmaß der Bedrohung für die Universität Würzburg wird beispielhaft durch einige bekannt gewordene schwerwiegende Vorfälle der letzten Monate belegt:

- 13 MS Internet Information Server wurden innerhalb eines Monats von derselben Gruppe von Angreifern gehackt und als FTP Server missbraucht.
- 18 Linuxrechner wurden auf einen Schlag über nicht aktualisierte OpenSSH-Dienste gehackt und für DoS-Attacken verwendet.
- 2 Server mit einem ungepatchten MS SQL-Server legten nach einer Infektion mit dem SQL-Slammer-Wurm den Internetzugang der Universität für 5 Stunden lahm.
- Viele Rechner wurden Opfer der Nimda- und Code-Red-Würmer.
- Ein Windows Domain Controller wurde gehackt und machte die Neuinstallation aller 68 Rechner in der Domäne notwendig.

Bei allen diesen Vorfällen war ein Sicherheits-Patch, der die Systeme gegen den jeweiligen Angriff immun gemacht hätte, zum Teil schon lange vorher verfügbar, so dass eine rechtzeitige, qualifizierte und kompetente Systemadministration die Vorfälle hätte verhindern können.

Firewalls und ACLs

Sicherheitsvorkehrungen, die dem Schutz des Datennetzes einer Firma oder einer Universität vor Hackern im weltweiten Internet dienen sollen, basieren im Wesentlichen darauf, dass anhand der in den Datenpaketen enthaltenen IP-Adressen und Ports alle unerwünschten Pakete blockiert werden. Im Idealfall sollen die eigenen Nutzer von „innen“, d. h. vom Hochschulnetz aus, auf alle Dienste im Internet möglichst uneingeschränkt zugreifen können. Von „außen“, d. h. vom Internet aus, sollen dagegen nur die dafür vorgesehenen Server im internen Datennetz erreichbar sein.

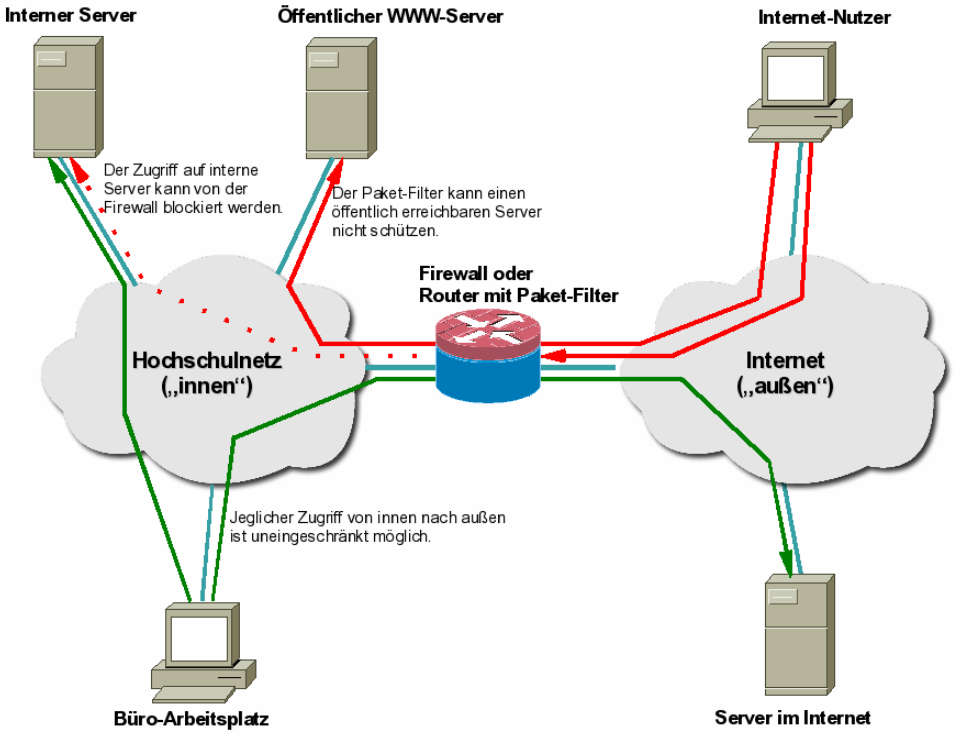

Abbildung 5: Die Aufgabe einer Firewall ist es, unerwünschte Verbindungen von außen nach innen zu blockieren, ohne die Kommunikation der eigenen Nutzer von innen nach außen einzuschränken. Interne Server, die von außen erreicht werden müssen, können durch eine Firewall nicht geschützt werden.

Für diese Zwecke kommen, wie in Abb. 5 schematisch angedeutet, *Firewalls* zum Einsatz. Der Begriff Firewall wird oft undifferenziert für Systeme verwendet, die von einfachen Paket-Filtern bis zu sehr komplexen Application Level Firewalls reichen können. Beim *Paket-Filter* werden auf der am Verbindungspunkt zum Internet eingesetzten Netzwerkkomponente *Access Control Lists* (ACLs, Zugriffs-Kontroll-Listen) definiert, die über die IP-Adressen und Ports festlegen, von welchem Quell- zu welchem Ziel-Rechner Pakete ungehindert weitergeleitet werden. Grundsätzlich muss berücksichtigt werden, in welcher Richtung die Datenübertragung initiiert wurde, da die Antwortpakete zu einem Client durchgelassen werden müssen, auch wenn er von außen direkt überhaupt nicht erreicht werden soll. Für viele Anforderungen sind Paket-Filter aus folgenden Gründen nicht ausreichend:

- Es gibt Dienste, bei denen die verwendeten Ports dynamisch vergeben werden.
- Bei Verwendung des Transportschichtprotokolls UDP statt TCP, z. B. bei Übertragung von Video- und Audio-Daten in Echtzeit, ist die Zuordnung der von außen kommenden Antwortpakete zu einer von innen initiierten Datenübertragung nicht möglich.
- Bei manchen Diensten wird auch bei TCP der Kommunikationsweg von außen nach innen aufgebaut (z. B. X11 oder active ftp).

Eine so genannte *Stateful Firewall* kann hier bedingt Abhilfe schaffen, da sie für derartige Dienste in der Lage ist, ihre Einstellungen dynamisch anzupassen und sich Informationen über vorangegangene Datenpakete zu „merken“. Es gibt aber einige schwerwiegende Argumente, die deutlich machen, dass eine Stateful Firewall alleine die vollständige Sicherheit auch nicht gewährleisten kann:

- Es ist möglich, für einen Dienst einen Port zu verwenden, der für einen anderen Dienst vorgesehen ist.
- Die Tatsache, dass ein Paket den Paket-Filter nach dessen Regeln passieren darf, sagt nichts über seinen potenziell bösartigen Inhalt aus.
- Zunehmend werden Dienste mittels verschlüsselnder Protokolle übertragen, in die die Firewall nicht „hineinsehen“ kann.
- Es gibt einen starken Trend, alle Dienste über WWW-Schnittstellen anzubieten, so dass der ursprünglich für die Informationsbereitstellung gedachte und weitgehend offen zu haltende Port 80 immer mehr zur Steuerung beliebiger Anwendungen verwendet wird.

Eine *Application Level Firewall* würde diese Probleme theoretisch zum Teil entschärfen, da sie den Datenstrom auch darauf prüfen kann, ob der Inhalt der Pakete der Spezifikation des vermeintlichen Dienstes entspricht oder ob ein möglicher Angriffsversuch vorliegt. Allerdings kann auch sie nicht in verschlüsselte Pakete hineinsehen oder per http bedienbare Applikationen und Datenbanken schützen. Vor allem erscheint die Pflege einer Application Level Firewall inkl. der Verwendung von Angriffsmustern auf Anwendungsebene bei den umfangreichen und komplexen Kommunikationsbeziehungen einer großen Universität nicht realisierbar.

Da die öffentlich erreichbaren Server von einer Firewall nicht vor Angriffen geschützt werden können, werden diese üblicherweise in einer so genannten *DeMilitarized Zone* (DMZ) gesammelt. Rechner in der DMZ können von innen zu Administrationszwecken erreicht werden. Ein Zugriff aus der DMZ auf interne Rechner ist nicht möglich, damit die öffentlichen Server nicht als Sprungbrett für weitere Angriffe verwendet werden können. Im Hochschulnetz würde sich die Einrichtung einer DMZ aufwändig gestalten, da die Server auf sehr viele Bereiche verteilt sind.

Die aktuell auf dem Wingate, dem Anschluss-Router der Universität an das Internet, eingetragenen ACLs werden im Artikel „Maßnahmen zur Erhöhung der IT-Sicherheit an der Universität Würzburg“ behandelt. Die bisherige Politik geht dabei davon aus, dass zunächst alle Kommunikationsbeziehungen uneingeschränkt möglich sind und dass nur die sicherheitskritischsten oder definitiv nicht benötigten Dienste blockiert werden. Anzustreben ist ein Zustand, bei dem alle Zugriffsversuche von außen blockiert werden, wenn sie nicht explizit gewünscht und aktiv frei geschaltet wurden. Allerdings würde diese Maßnahme nur dann Sinn machen, wenn gleichzeitig eine angemessene Betreuung der Server, die von außen erreichbar sein sollen, gewährleistet wäre.

Die meisten der oben aufgeführten Rechnereinbrüche wären durch eine Firewall nicht verhindert worden, da Dienste betroffen waren, die von außen erreichbar sein sollten oder die nur im engen und aufwändigen Dialog zwischen Fachbereich und Rechenzentrum hätten abgeschottet werden können.

Klez & Co. – Viren auf dem Vormarsch

Roland Völker

Melissa und Michelangelo sind nicht gerade wohlklingende Namen und Love-Letter ist nicht der heiß ersehnte Liebesbrief, wenn von Computerviren die Rede ist. Diese schmerzliche Erfahrung mussten auch etliche Mitarbeiter unserer Universität machen. Von Zeit zu Zeit machen Meldungen von Computerviren in den Medien die Runde. Häufig wird von einer lawinenartigen Ausbreitung eines Virus berichtet, der global große Schäden anrichtet und in der Regel für große Verunsicherung bei den Anwendern im Internet sorgt. Viele sind schon selbst damit in Kontakt gekommen und haben dafür mit dem Verlust einzelner Dateien oder sogar mit einer neu formatierten Festplatte bezahlt. Die wenigsten wissen aber wirklich was ein Computervirus eigentlich ist.

Was sind Computerviren?

Vom technischen Standpunkt aus betrachtet ist ein Virus meistens ein kleines Stück ausführbarer Code, das in der Lage ist, sich selbst zu vervielfältigen und weiter zu verbreiten. Oft besitzen Viren einen Programmteil, der das infizierte System beschädigt. In ungünstigen Fällen kann eine Schadroutine zum kompletten Datenverlust führen. Viren entstehen nicht spontan aus dem Nichts heraus, sondern werden von Menschen programmiert, die bestimmte Absichten verfolgen. Nach Beobachtungen und Einschätzung von Experten ist der typische Viren-Programmierer meist exzentrisch veranlagt, zwischen 20 und 30 Jahren alt und männlich. Sein Hauptmotiv besteht darin, sich und der gesamten Internet Community zu beweisen, dass er in der Lage ist, fremde Rechner zu manipulieren. Dabei schrecken die Viren-Programmierer nicht davor zurück, die Gefühle und Ängste der Menschen zu missbrauchen, wie das Beispiel des kürzlich in Umlauf gebrachten Virus Coronex zeigt. Dieser verbreitet sich via E-Mail und gibt vor im Anhang wichtige Informationen zur aktuellen SARS-Epidemie zu enthalten. Der Empfänger soll genötigt werden, den Anhang zu öffnen und den Virus auf diese Weise zu aktivieren.

Welche Arten von Computerviren gibt es?

Computerviren lassen sich in drei Grundtypen unterteilen. *Dateiviren* infizieren Programmdateien, indem sie sich zum Beispiel an deren Anfang kopieren. Wird die so manipulierte Datei ausgeführt, wird der Virus aktiv und kann weitere Programme befallen. Seltener kommen heute die so genannten *Bootsektorviren* vor. Sie tragen ihren Namen, da sie sich in den Teil einer Festplatte oder Diskette kopieren, der den Master Boot Record enthält und beim Starten des Computers als allererstes in den Arbeitsspeicher gelesen wird. Bleibt der Virus unentdeckt, wird er bei jedem Bootvorgang neu aktiviert. Die jüngste Virus-Kategorie, die *Makroviren*, besitzt zugleich das größte Bedrohungspotential. Sie vermehren sich durch ausführbaren Code, der in Form von Makros in den Dokumenten von gewöhnlichen Anwendungsprogrammen eingebettet ist. Auf diese Weise kann eine scheinbar harmlose Word-Datei zu einem Sicherheitsrisiko für das Computersystem werden. Während Datei- und Bootsek-

torviren zunehmend an Bedeutung verlieren, erfahren Makroviren eine rasante Verbreitung. Dies hat seine Ursache im rasch ansteigenden Datenaustausch über das Internet und den sehr regen Gebrauch von E-Mail. Ein weiterer Grund ist, dass Makrosprachen auch Laien die Möglichkeit bieten auf einfachste Weise in das System einzugreifen, ohne tiefgehende Kenntnisse davon zu besitzen. Dadurch wächst die Schar der potentiellen Virenautoren um ein Vielfaches.

Einige Viren besitzen die Eigenschaft sich selbständig über Netzwerke hinweg zu kopieren. Sie müssen keine Dateien oder Bereiche von Datenträgern mehr infizieren, um sich zu vermehren. Wegen ihrer Netzwerkfähigkeiten können sie extrem hohe Ausbreitungsgeschwindigkeiten erreichen, was sie zu einer gefährlichen Bedrohung macht. Die zurzeit wirkungsvollsten Viren besitzen diese Eigenschaft. Sie werden als *Würmer* bezeichnet.

Eine weitere Gruppe, die keine Viren im eigentlichen Sinn sind, bilden die so genannten *Hoaxe*. Es handelt sich um bewusst gestreute Falschmeldungen über neue Viren, die überwiegend per E-Mail verbreitet werden. Dem Empfänger wird versucht einzureden, dass sein Rechner infiziert sei und er wird aufgefordert, bestimmte Dateien, meist wichtige Windows-System-Dateien, zu löschen. Zusätzlich soll er die Nachricht an alle seine Bekannten weiterleiten. Das Ziel ist klar: Anwender, die sich aufgrund ihrer geringen Fachkenntnisse verunsichern lassen, sollen selbst ihr eigenes System beschädigen und den Hoax lawinenartig weiterverbreiten.

Zuweilen werden Viren oder anderer bösartiger Code quasi „huckepack“ zusammen mit anderen Programmen verbreitet. Es kann sich dabei z. B. um Spiele, Bildschirmschoner oder nützliche Utilities handeln. Werden diese Programme gestartet, werden zunächst die schädlichen Routinen unbemerkt vom Benutzer aktiviert bevor das eigentliche Programm ausgeführt wird. Der Benutzer wird nicht misstrauisch und die „erweiterte Funktionalität“ bleibt verborgen. Auf diese Weise können *Backdoors* (Hintertüren) auf dem Rechner installiert werden, die es Hackern ermöglichen in das System einzubrechen. Wegen der Analogie zur griechischen Mythologie werden Schadprogramme, die diese Art der Tarnung verwenden, als *Trojanische Pferde* oder kurz als *Trojaner* bezeichnet.

Die Zahl der heute bekannten Viren ist groß, ihr genauer Wert kann nur geschätzt werden. Zum einen gibt es von vielen Viren mehrere Varianten, zum anderen ist oft ein und derselbe Virus unter unterschiedlichen Bezeichnungen bekannt. Alles in allem existieren heute mehr als 65.000 Viren. Das Unternehmen Sophos bietet mit seiner Antivirensoftware zurzeit Schutz gegen etwa 81.000 verschiedene Viren-Varianten. Die Anzahl wächst jährlich um etwa 5.000. Von den bekannten Viren findet man nur ca. 1-2% in „freier Wildbahn“, denn viele existieren nur in Laborumgebungen oder sind nicht effektiv genug, um eine nennenswerte Ausbreitung zu erlangen.

Schäden durch Computerviren

Genaue Zahlen über die Kosten, die durch Viren verursacht werden, existieren nicht, da es keine zuverlässigen Erhebungen und keinen einheitlichen Weg zur Kalkulation gibt. Viele Unternehmen legen aus Angst vor einem Imageverlust ihre Einbußen nicht offen. Die jährlichen Schäden sind enorm hoch und steigen drastisch. So schätzt beispielsweise die Schweizer Rückversicherung Swiss Re die weltweiten Verluste, die im Jahr 2000 durch den Love-Letter-Virus verursacht wurden, auf 2,8 Mrd. €. Der globale Gesamtschaden durch Viren für das Jahr 2000 wird von der Hamburger Unternehmensberatung Mummert + Partner auf 19 Mrd. € beziffert. Die hohe Wachstumsrate wird verdeutlicht, wenn man nach einer Studie von Computer Economics davon ausgeht, dass der weltweite Gesamtschaden durch Computerviren im vorausgehenden Jahr 1999 noch bei rund 12 Mrd. US $ lag.

Trotz der hohen finanziellen Einbußen ist die Virenproblematik erst durch den Ausbruch des Melissa-Virus in das Bewusstsein vieler Unternehmen gelangt. Melissa trat am Freitag, den 26. März 1999 in den USA in Erscheinung und

erfuhr eine weltweite Verbreitung innerhalb weniger Stunden. Dieser Makrovirus befällt Word 97- und Word 2000-Dokumente und benutzt Outlook um Word-Dateien, die er vorher infiziert hat, via E-Mail an weitere Benutzer zu versenden. Er sucht sich dafür die ersten 50 Adressen aus allen Adressbüchern, auf die Outlook zugreifen kann. Wird Melissa auf einem Rechner aktiviert, befällt es alle geöffneten Word-Dokumente. Auf diese Weise ist es möglich, dass auch vertrauliche Word-Dateien weitergeleitet werden. Viele Mailserver wurden durch die Flut von E-Mails, die durch große Anhänge von Word-Dokumenten aufgebläht waren, lahm gelegt. Die Firmen Microsoft und Intel waren gezwungen ihre E-Mail-Systeme komplett herunterzufahren, um eine weitere Verbreitung zu verhindern. Zwar besitzt Melissa keine Schadroutine, allein durch die Beeinträchtigung des E-Mail-Verkehrs entstand in den USA laut ICSA (International Centre for Security Analysis) ein Schaden von umgerechnet 200 Mio. €. Europa wurde durch die Melissa-Epidemie weniger hart getroffen, da zum Zeitpunkt des Ausbruchs aufgrund der Zeitverschiebung das Wochenende bereits begonnen hatte. Viele Unternehmen waren am Montag bereits vorgewarnt und konnten eine größere Ausbreitung verhindern. Das FBI konnte nach einer dreitägigen weltweiten Fahndungsaktion den Autor des Melissa-Virus dingfest machen. Der Täter David Smith wurde in den USA zu 20 Monaten Haft und einer Geldstrafe von 5.000 US $ verurteilt. Das Gericht blieb unter der Höchststrafe von fünf Jahren Haft und einer Geldstrafe von 250.000 US $, weil sich der Angeklagte kooperativ gezeigt hatte.

Geschichte der Computerviren

Obwohl es Computerviren erst seit etwa zwei Jahrzehnten gibt, geht ihre Geschichte weiter zurück. Im Jahre 1949 entwickelt der ungarische Informatiker John von Neumann die Theorie von selbstreproduzierenden Automaten, ohne allerdings an eine derartige Anwendung zu denken. In seinem Roman „The Shockwave Rider“, der 1975 erscheint, beschreibt der Autor John Brunner einen Wurm, der sich in Computernetzen ausbreiten und Daten manipulieren kann. 1980 gibt der Informatikstudent Jürgen Kraus in seiner Diplomarbeit „Selbstreproduktion von Programmen“ einen ersten Hinweis darauf, dass sich Programme unter bestimmten Bedingungen ähnlich wie biologische Viren verhalten können. Knapp drei Jahre später wird der Begriff *Computervirus* von Fred Cohen geprägt. In seiner Dissertation „Computer Viruses – Theory and Experiments“ befasst er sich mit der Theorie selbstreproduzierender Programme und entwickelt den ersten funktionsfähigen Virus.

Im Jahre 1982 erscheinen die ersten Viren auf der Bildfläche. Im Xerox Alto Research Center entwickeln Jon Hepps und John Shock Würmer, die intern zur Realisierung verteilter Rechnungen verwendet werden sollen. Bedingt durch einen Programmierfehler können sich die Würmer unkontrolliert vermehren, wodurch das System nach kurzer Zeit unter der enormen Last zusammenbricht. 1987 wird Brain als erster MS-DOS-Virus an der Universität von Delaware, USA, in freier Wildbahn entdeckt. Ursprünglich in Pakistan entwickelt ist Brain, dessen Existenz zu dieser Zeit bereits seit einem Jahr bekannt ist, der erste Virus der sich global ausbreitet. In der Folgezeit tauchen immer mehr Viren auf, die durch ausgefeiltere Techniken zur Ausbreitung und Tarnung immer erfolgreicher werden. Im November 1988 wird der *Internet-Wurm* frei gesetzt. Er befällt 6.000 Computer, was zum diesem Zeitpunkt etwa 10% aller Computer des Internets entspricht. Der Täter, Robert Morris, kann ermittelt werden und wird zu einer Bewährungsstrafe von drei Jahren, 400 Stunden gemeinnütziger Arbeit, und einer Geldstrafe von 10.000 US $ verurteilt. Im selben Jahr wird auch das erste Virus Construction Kit für den Atari ST veröffentlicht, mit dessen Hilfe auch Einsteiger in der Lage sind, Viren mit bestimmten Eigenschaften zu konstruieren. 1989 tauchen die ersten *polymorphen Viren* auf. Sie sind in der Lage ihr Aussehen bei der Vervielfältigung zu verändern, um die Entdeckung durch Antivirensoftware zu erschweren. In diesem Jahr werden auch die ersten *Tarnkappenviren* (Stealth-Viren) entdeckt. Diese infizieren Dateien und verschleiern die Veränderungen um nicht entdeckt zu werden.

In den folgenden Jahren werden die Abwehrmaßnahmen gegen Viren intensiviert. Die Firmen McAfee und IBM entwickeln erste Virenscanner, die zunächst nur 44 bzw. 22 unterschiedliche Viren erkennen können. 1991 werden die Organisationen EICAR (European Institute for Computer Anti-Virus Research) und CARO (Computer Anti-Virus Research Organisation) gegründet. All dies kann nicht verhindern, dass die Zahl neuer Viren rasant zunimmt. So werden allein 1992 mehr neue Viren entdeckt als zuvor bekannt waren.

1992 sorgt der Bootsektorvirus Michelangelo für die erste weltweite Viren-Hysterie. Der Virus erhielt seinen Namen auf Grund der Tatsache, dass das Auslösedatum der Schadroutine, der 6. März, mit dem Geburtstag des berühmten italienischen Künstlers Michelangelo zusammenfällt. Im Nachhinein zeigte sich jedoch, dass nur wenige Computer infiziert wurden.

Mit Concept tritt 1995 der erste Makrovirus in Erscheinung. Der Virus gerät durch ein peinliches Versehen in Umlauf, denn er wird auf einer offiziellen CD-Rom mit Software der Firma Microsoft ausgeliefert.

1998 erscheint der erste Virus, der in der Lage ist, die Hardware des Computers zu beschädigen. Während bisher aufgetretene Viren nur Daten verändern oder löschen können, überschreibt der Chernobyl-Virus das BIOS des Rechners, was einen Austausch des Chips erforderlich macht.

In den beiden Folgejahren wird die Welt durch die Ausbrüche der Viren Melissa und Love-Letter getroffen, die sich mit einer bisher unbekannten Geschwindigkeit im Internet verbreiteten. Dabei gilt der zweite als besonders perfide, da er sich, als Liebesbrief getarnt, über Outlook verbreitet. Der Urheber, ein philippinischer Student, wird verhaftet, später aber wieder freigelassen. Das Programmieren von Viren war zum Tatzeitpunkt auf den Philippinen nicht strafbar.

Im August 2001 infiziert der Massen-Mailer SirCam innerhalb weniger Stunden eine viertel Million Computer. Er ist der erste Virus, der mit einer eigenen SMTP-Engine versehen ist, was ihn unabhängig vom Vorhandensein anderer Mailprogramme macht. SirCam nutzt eine weitere Verbreitungsmöglichkeit, indem er sich selbst auf freigegebene Netzlaufwerke kopiert. Dort kann er durch das Eingreifen eines lokalen Benutzers aktiviert werden.

Die Fähigkeit alternative Wege zur Ausbreitung nutzen zu können trägt wesentlich zum Erfolg neuer Viren bei. Im September 2001 bricht Nimda aus, der sich über E-Mail und fremde Netzwerkfreigaben auch mit Hilfe von Microsofts Internet Information Server (IIS) verbreiten kann. Er benutzt verschiedene Schwachstellen des weit verbreiteten Webservers, um auf ihm infizierte Dateien zu platzieren. Erstmalig können sich Anwender nur durch den Besuch einer kompromittierten Website einen Virus einfangen. Nimda nutzt außerdem eine Sicherheitslücke in den Microsoft-Produkten Outlook, Outlook Express und Internet Explorer, um den Virencode in den Anhängen der verschickten Mails automatisch starten zu lassen. Ein Zutun des Empfängers ist nicht mehr nötig.

Das Jahr 2002 steht eindeutig im Zeichen von Klez und Bugbear. Im April wird eine neue Variante des Klez-Virus entdeckt, die eine starke Verbreitung erfährt. Ähnlich wie SirCam besitzt diese Version eine eigene SMTP-Routine. Dadurch ist es Klez möglich, die Absenderadresse der Virenmails zu fälschen, was dazu führt, dass unschuldige Benutzer fälschlicherweise in den Verdacht geraten, den Virus zu verbreiten. Bugbear tritt Ende September in Erscheinung und ist im letzten Quartal des Jahres der meist verbreitete Virus. Bugbear und Klez benutzen beide die seit langem bekannte IFRAME-Schwachstelle in verschiedenen Microsoft-Produkten, um die Anhänge ihrer Mails automatisch auszuführen.

Abwehrmaßnahmen gegen Computerviren

Die rasante Zunahme an neuen Viren verursacht jährlich steigende Schäden. Wurden vor rund 20 Jahren nur wenige neue Viren in einem Jahr entdeckt, sind es heute etwa ein Dutzend pro Tag. Wesentliche Gründe sind einerseits der zunehmende Austausch von Daten über das Internet und andererseits die weltweite Dominanz von MS Windows. Da etwa 90% aller Computer unter dem Betriebssystem von Microsoft laufen, ist es für Viren meistens ein Leichtes stets genug verwundbare Systeme zu finden, um sich effektiv verbreiten zu können. Die häufig unqualifizierte Administration der Systeme verbunden mit einem undifferenzierten Einräumen von Zugriffsrechten auf Dateien und Freigaben macht Windows zum idealen Nährboden für Viren und andere Malware.

Tröstlich ist, dass der verstärkte Einsatz von Anti-Viren-Software (AV-Software) es neuen Viren zunehmend schwerer macht, eine große Verbreitung zu erlangen. Zwar bieten heute weit verbreitete Werkzeuge, wie Virenbaukästen, auch unerfahrenen Nutzern die Möglichkeit, eigene Viren zu entwickeln, was die Zahl der potentiellen Virenprogrammierer und der neuen Viren deutlich erhöht. Deren Produkte stellen die Hersteller von AV-Software in der Regel aber vor keine großen Schwierigkeiten. Die letzten größeren Virusausbrüche haben gezeigt, dass für die Entwicklung eines erfolgreichen Virus gute Detailkenntnisse und innovative Ideen benötigt werden. Dazu gehören u. a. die Verbesserung der Netzwerkfähigkeiten und das Ausnutzen neuer Sicherheitslöcher in vorhandenen Programmen. Anderseits ist festzustellen, dass die Sensibilität bezüglich der Systemsicherheit bei vielen Usern und Systemadministratoren immer noch mangelhaft ist. So ebnete die IFRAME-Sicherheitslücke den Klez- und Bugbear-Viren erst den Weg für eine erfolgreiche Ausbreitung, obwohl das Sicherheitsproblem bereits seit langem bekannt war und Microsoft schon Monate zuvor einen Patch zur Beseitigung der Sicherheitslücke zur Verfügung gestellt hatte. Dieses Beispiel zeigt deutlich, wie wichtig die Verwendung von aktueller Software zur Abwehr von Viren ist. Dazu ist es nötig, bei den eingesetzten Produkten stets auf dem Laufenden zu sein, um ggf. verfügbare Sicherheitsupdates einspielen zu können. Das gilt natürlich ganz besonders für die benutzte Anti-Viren-Software.

Dass ein Virenscanner, der in regelmäßigen Abständen die Festplatte kontrolliert, stets in der neuesten Version verwendet wird, sollte eigentlich selbstverständlich sein. Zum Schutz gegen aktuelle Viren bieten alle gängigen Hersteller von AV-Software periodische Updates ihrer Produkte an. Im Falle eines massiven Ausbruchs eines neuen Virus gibt es diese häufig auch aus aktuellem Anlass. Um zu verhindern, dass Viren gar nicht erst auf den eigenen Computer gelangen, sollte man grundsätzlich keine Software aus unbekannter Herkunft, wie Tauschbörsen, installieren. Außerdem sollte man unangekündigte Anhänge an E-Mails generell nicht öffnen, auch wenn die E-Mail von einer bekannten Person stammt. Wollen Sie Dateien mit Freunden oder Partnern über E-Mail austauschen, dann ist eine vorherige Absprache stets ratsam.

Welche Maßnahmen das Rechenzentrum im Kampf gegen Computerviren ergreift, können Sie in diesem Heft im Artikel „Zentrale Maßnahmen des Rechenzentrums gegen Viren und Spam“ lesen.

Spam-Mail – mehr als nur ein Ärgernis

Roland Völker

Mit Werbematerial, das die Briefkästen überquellen lässt, haben wir gelernt umzugehen. Möchte man nicht, dass unangeforderte Wurfsendungen und Zeitungen in seinem Briefkasten landen, dann kann man einen entsprechenden Aufkleber gut sichtbar am eigenen Briefkasten anbringen. Wie sieht es mit Werbesendungen und eventuellen Abwehrmechanismen bei E-Mail aus? In diesem Artikel wird versucht die aktuellen Entwicklungen und ihre Auswirkungen aufzuzeigen.

Entwicklung der elektronischen Werbesendungen

Seitdem immer mehr Unternehmen das Internet für ihre Zwecke entdeckt haben, leiden die Nutzer unter einer stetig wachsenden Flut von Werbe-Mail. Verstopfte E-Mail-Folder (Briefkästen) und das sehr aufwändige und mühsame Aussortieren unerwünschter E-Mails stehen auf der Tagesordnung. Die Palette der angepriesenen Produkte reicht von schmuddeligen Sex-Angeboten über Offerten für Glücksspiele oder dubiose Kredite bis hin zu Wegen, wie man ohne große Mühe innerhalb von kurzer Zeit zum Millionär werden kann. Die Angebote sind offensichtlich meist unseriös und lassen die E-Mailboxen vieler Nutzer überlaufen.

Im Netz-Jargon werden solche E-Mails als *Spam* bezeichnet. Der Begriff geht auf ein Produkt der Firma Hormel Foods Corporation zurück und ist ein Akronym für "Spiced Pork And Ham" (gewürztes Schweine- und Rindfleisch). Das Dosenfleisch, das bereits in den 30er Jahren des vergangenen Jahrhunderts vertrieben wurde, spielt in einem Sketch der britischen Komikertruppe Monty Python eine zentrale Rolle. In einem Schnellrestaurant stellt ein Ehepaar fest, dass alle Speisen einen mehr oder weniger großen Anteil an Spam enthalten. Aufgrund dieser Tatsache entwickelt sich ein amüsanter Dialog mit der Kellnerin, der mehrmals durch den Gesang einer Horde von Wikingern unterbrochen wird: "Lovely Spam, wonderful Spam!" Alles in allem wird der Begriff Spam innerhalb weniger Minuten mehr als 120-mal wiederholt. Aufgrund dieses Sketches bezeichnete man anfangs Beiträge, die in einer unakzeptabel großen Anzahl in einer oder mehreren Newsgroups veröffentlicht werden, als Spam. Heute wird der Begriff meist synonym zu unerwünschten Werbe- (Unsolicited Commercial E-Mail, UCE) oder Massenmails (Unsolicited Bulk E-Mail, UBE) verwendet.

Schätzungen zufolge liegt der Anteil von unerwünschter Werbe-Mail heute im Durchschnitt bei etwa 38%, mit stark steigender Tendenz. Bereits im Jahre 2006 rechnet man mit einem Aufkommen von etwa 20 Mrd. Spam-Mails pro Tag. Sollte sich dieser Trend bestätigen – vieles spricht dafür – wird in naher Zukunft eine sinnvolle Kommunikation über E-Mail so gut wie unmöglich werden. Die Gründe für diesen negativen Boom liegen auf der Hand. Das

Medium E-Mail ist im Vergleich zu herkömmlicher Werbung, wie dem Schalten von Zeitungsinseraten oder Verteilen von Printmedien, unschlagbar billig. Durch Massenmails kann man in kürzester Zeit und mit relativ geringem Aufwand viele Empfänger erreichen. Sie gibt auch kleinen Firmen die Möglichkeit, kostengünstig eine große Anzahl potentieller Kunden auf sich aufmerksam zu machen. Es wird geschätzt, dass etwa 1.000 bis 10.000 Werbe-Mails nötig sind, um ein einziges Exemplar eines Produktes zu verkaufen. Dies ist für viele Unternehmen attraktiv genug, um selbst den Imageverlust, der zu erwarten ist, wenn der Firmenname als Spamversender in Erscheinung tritt, in Kauf zu nehmen.

Befürworter führen an, dass Spam für mehr Chancengleichheit von kleineren Firmen gegenüber großen Konzernen sorge und so zu mehr Wirtschaftswachstum führe. Spam sei kostengünstig und verursache keine Schäden. Zudem sei sie durch das Recht auf freie Meinungsäußerung gedeckt. In den USA wurde eine Interessenvereinigung der Werbe-Mail-Versender gegründet, die kürzlich erst eine Reihe von Spam-Gegnern auf Schadenersatz in Höhe von 75 Mio. US $ verklagt hat.

Auswirkungen von Spam-Mails

Ein privater Nutzer wird durch Spam zwar nicht direkt geschädigt, da er unerwünschte E-Mails ohne weiteres löschen kann. Um entscheiden zu können, ob eine Nachricht von Interesse ist, muss sie aber erst vom E-Mail-Server herunter geladen werden. Dies führt zu mehr Verbindungskosten, falls der Kunde nicht eine Flatrate sein eigen nennt. Das hohe Aufkommen von Spam verschwendet Bandbreite und Ressourcen. Die Internet-Service-Provider werden gezwungen, mehr Speicherplatz auf ihren E-Mail-Servern zur Verfügung zu stellen, um ein Überlaufen der E-Mail-Boxen ihrer Kunden zu verhindern. Bei dienstlicher Nutzung von E-Mail muss die Arbeitszeit einkalkuliert werden, die beim Umgang mit Spam-Mail verloren geht. Um ihre durch Werbe-Mails verärgerte Kundschaft zu befriedigen, müssen sowohl für private als auch für die dienstlichen Nutzer Abwehrmaßnahmen ergriffen werden. Es muss eine geeignete Anti-Spam-Software erworben und in Betrieb genommen werden, was zusätzliches Personal erfordert. Die entstehenden Mehrkosten werden auf den Anwender umgelegt. Legt man diese Kalkulation zugrunde, dann entstehen durch Spam-Mail insgesamt Verluste in Milliardenhöhe. Laut einer Studie des britischen Marktforschungsunternehmen Benchmark Research aus dem Jahr 1998 wurden bereits damals durch die Flut von Spam-Mails allein in Großbritannien und Irland jährlich Verluste von 7 Mrd. € verursacht. Dabei wurden neben den reinen Verbindungskosten auch die Arbeitszeitverluste berücksichtigt, die durch das Lesen, Löschen und das gelegentliche Reagieren auf solchen Werbemüll entstehen.

Wie hoch sind die Arbeitszeitverluste durch Spam-Mail an der Universität Würzburg? Für eine konservative Abschätzung gehen wir von einem mittleren E-Mailaufkommen von etwa 50.000 Mails pro Tag aus und nehmen an, dass nur ein Drittel davon Spam-Mails sind (derzeit werden rund 50% als Spam eingestuft). Wenn ein Benutzer eine E-Mail in drei Sekunden an Hand von Absenderadresse und Betreffzeile als Spam erkennen und löschen kann, werden allein hierfür wöchentlich fast 100 Stunden aufgewendet. Unterstellt man noch, dass zumindest ein kleiner Teil der Spam-Mails geöffnet und gelesen wird, kann man die verlorene Zeit getrost verdoppeln. Dies bedeutet, dass bereits jetzt der Aufwand für die Bearbeitung nicht gewollter Werbesendungen der Arbeitszeit von mindestens fünf Vollzeitstellen entspricht – Tendenz steigend.

Ist Spam-Mail legal?

Auch wenn in manchen Werbe-Mails das Gegenteil behauptet wird, Spam ist illegal. In den Ländern der EU gilt eine "Opt-In"-Regelung. Sie besagt, dass Werbung via E-Mail nur dann erlaubt ist, wenn der Empfänger ausdrücklich sein Einverständnis erteilt hat. Eine Verbotsregelung erreicht nur dann ihren Zweck, wenn man den Spammer dingfest machen kann, und das ist das große Problem. Das Versenden von Spam erfolgt in der Regel anonym. Spammer versuchen ihre Spuren so gut wie möglich zu verwischen. Um ihre Massenmails an den Mann zu bringen, verwenden sie bevorzugt Einmal-Accounts. Außerdem bedienen sie sich häufig offener *Relays*, das sind E-Mail-Server, die ohne Überprüfung jede E-Mail akzeptieren und weiterleiten. Normalerweise sollte ein Server nur E-Mails annehmen, die an seine eigenen Benutzer gerichtet sind oder von diesen stammen. Bei vielen schlecht administrierten E-Mail-Servern ist dies nicht der Fall. Häufig stehen diese in Ländern, die dem europäischen Recht entzogen sind. Die Chancen, eines Spammers habhaft zu werden, sind in diesen Fällen äußerst gering.

Was kann gegen Spam-Mail getan werden?

Wenn man den Spammer selbst schon nicht erwischen kann, so könnte man zumindest versuchen keine E-Mails mehr aus dubiosen Quellen zuzulassen. Tatsächlich existieren im Internet mehrere so genannte *Real Time Blacklists* (RBLs). Es handelt sich um Datenbanken, in denen die Adressen offener Relays gespeichert sind und die (hoffentlich) permanent aktualisiert werden. Ein E-Mail-Server soll eine Nachricht erst dann akzeptieren, wenn die Anfrage bei einer solchen Datenbank negativ verläuft. Eine derartige Blockadepolitik schafft leider mehr Probleme als sie löst. Während durch den Einsatz von RBLs schätzungsweise weniger als ein Viertel aller Spam-Mails abgeblockt werden, wird auch etwa jede dritte legitime Nachricht nicht durchgelassen.

Ein systemweites Ausfiltern von E-Mails, z. B. aufgrund bestimmter Stichworte, ist äußerst problematisch. Bei einer Nachricht mit dem Wort "Breast" im Betreffsfeld wird es sich vermutlich in den meisten Fällen um ein pornographisches Angebot handeln. Ist der Adressat jedoch ein Mediziner, der sich beruflich mit dem Thema Brustkrebs beschäftigt, wird das in der Regel nicht zutreffen. Dieses einfache Beispiel macht deutlich, dass es an zentraler Stelle äußerst schwierig ist wirksam gegen Spam vorzugehen, da es nicht möglich ist, eine E-Mail allgemeingültig als Spam zu klassifizieren. Letztlich kann nur der Anwender selbst diese Bewertung durchführen. Nebenbei hat jeder Betreiber eines E-Mail-Servers aufgrund des Briefgeheimnisses die Aufgabe und die Pflicht jede E-Mail ohne inhaltliche Bewertung zuzustellen.

Was tun, wenn man eine Spam-Mail in seinem Eingangsordner findet? Grundsätzlich ist hierzu zu sagen: Kaufen Sie niemals etwas, das Ihnen in einer Werbe-Mail angeboten wird! Eine Vergrößerung des Erfolgs des Spammers wird in der Zukunft noch mehr Spam nach sich ziehen. Löschen Sie die Nachricht. Das ist am einfachsten und spart viel Zeit. Beantworten Sie Spam-Mails niemals, denn in der Regel wird Ihre Antwort nicht zustellbar sein und es wird lediglich das Mailaufkommen weiter erhöht. Im schlimmsten Fall erhält der Spammer aus einer Antwort die Information, dass Ihre E-Mail-Adresse gültig ist, was zur Folge haben kann, dass Sie in Zukunft mit noch mehr Werbemüll bedacht werden. Falls Sie sich damit nicht zufrieden geben wollen, dann beschweren Sie sich bei dem Provider, von dessen E-Mail-Server Sie die Spam-Mail erhalten haben. Wenden Sie sich dazu an die hierfür vorgesehenen Adressen „postmaster" oder „abuse" aus der Domain des jeweiligen Providers. Die Aussichten, dass Sie in Zukunft keine Spams mehr aus dieser Quelle erhalten werden, sind gut. Der Provider ist meist selbst Opfer und hat Interesse daran, seinen guten Ruf zu wahren. Für eine derartige Reaktion ist es allerdings erforderlich zu wissen, wie man die IP-Adresse des E-Mail-Servers aus dem Header herauslesen kann und wie man damit auf den Provider schließen kann.

Um zukünftig von weiterer Spam verschont zu werden, bleiben Sie nach Möglichkeit bei Ihren Aktivitäten im Internet anonym. Manche Dienste setzen die Angabe einer gültigen E-Mail-Adresse voraus. Verwenden Sie hierfür Einmal-Accounts, die von verschiedenen Sites angeboten werden. Das sind E-Mail-Adressen die nur für einen begrenzten Zeitraum gültig sind. Spammer verwenden häufig *Spyder*, um an E-Mail-Adressen zu gelangen. Spyder sind Programme, die das Internet nach E-Mail-Adressen absuchen. Veröffentlichen Sie Ihre Adresse auf Ihrer Homepage nur in einer Form, die nicht von automatisierten Spionen gelesen werden können. Benutzen Sie geeignete Programme, die an Ihre individuellen Bedürfnisse angepasst sind, um die eingehende Post zu filtern.

Aktuelle Utilities zur Abwehr von Spam sind sehr effektiv und übertreffen einfache Filter, die lediglich nach bestimmten Schlagwörtern suchen, bei weitem. Es sei hier noch einmal betont: Jeder Benutzer ist für sich selbst verantwortlich. Niemand kann einem die Entscheidung abnehmen, ob man eine bestimmte E-Mail erhalten will oder nicht.

Welche Maßnahmen das Rechenzentrum gegen Spam-Mail ergreift und welche Werkzeuge dem Benutzer zur Unterstützung angeboten werden, können Sie in diesem Heft in den Artikeln „Zentrale Maßnahmen des Rechenzentrums gegen Viren und Spam" und „Webmail – ein E-Mail-System für die Anforderungen von heute" lesen.

Zentrale Maßnahmen des Rechenzentrums gegen Viren und Spam

Roland Völker

Die in den vorstehenden Artikeln aufgezeigten Probleme in Verbindung mit dem Kommunikationsmittel E-Mail machen auch vor der Universität Würzburg nicht halt. In den vergangenen Monaten wurde sie immer häufiger Opfer von Virenattacken. Die wachsende Flut von Werbe-Mails führt zu steigendem Unmut bei den Empfängern. Im Folgenden soll aufgezeigt werden, was das Rechenzentrum unternimmt, um an dieser Front der Situation Herr zu werden.

Das externe Mailrelay (Mailgate)

Um den Problemen effektiv zu begegnen, war es notwendig, das Mailsystem der Universität zu zentralisieren und den Mailfluss über ein System aus Relay-Servern zu leiten (Abb. 1). Das externe Mailrelay besteht aus zwei redundanten Servern, über die ausnahmslos alle Mails geleitet werden, die von außen in die Universität gelangen. Die Umleitung der Mail an Zieladressen innerhalb des Universitätsnetzes wurde durch eine Änderung der Einträge im Domain Name Server (DNS) erreicht. Die Sperrung des SMTP-Ports am Verbindungsknoten zum Internet (Wingate) erzwingt, dass alle Mails von außerhalb das Mailrelay passieren müssen. Es ist gewährleistet, dass beide Rechner gleichmäßig ausgelastet werden und die Universität bei einem Ausfall eines der beiden Relay-Server noch immer von außen über E-Mail erreichbar ist.

Der zentrale Mailviren-Scanner

Die Relay-Server verteilen die entgegengenommen Mails gleichmäßig an zwei weitere Server, auf denen ein Mailviren-Scanner installiert wurde. Ziel war es, möglichst freie Software zu verwenden, um die Kosten gering zu halten und das System so flexibel wie möglich gestalten zu können. Es wurde eine Lösung auf der Basis von *AMaViS* (Another Mail Virus Scanner) gewählt. Dabei handelt es sich um eine Filter-Software, die von allen gängigen Mailservern angesprochen werden kann. Als *Mail Transfer Agent* (MTA) kommt das Produkt *postfix* zum Einsatz. AMaViS selbst ist ein in Perl programmiertes Skript, das die Anhänge von Mails in ein Verzeichnis entpackt, wobei falls nötig Archive und Dateien dekomprimiert werden. Anschließend wird ein normaler Virenscanner aktiviert, der die Dateien untersucht. AMaViS arbeitet mit allen gebräuchlichen Scannern zusammen. Wegen seiner hohen Performance wurde als Virenscanner *sophie* gewählt. Die einzig benötigte kostenpflichtige Komponente, die Bibliothek *libsavi* der Firma Sophos, ist durch einen Campusvertrag der Universität Würzburg ohne zusätzliche Kosten verfügbar. Um die Erkennungsrate zu verbessern, wird parallel ein zweiter kostenfreier Virenscanner *clamav* eingesetzt. Wird eine infizierte Mail entdeckt, wird die Auslieferung der Mail gestoppt und Sender und Empfänger werden über den Vorfall informiert. Die Virenscanner werden mehrmals täglich durch

automatische Updates der Viren-Pattern aktuell gehalten, um auch auf neu auftretende Viren sofort reagieren zu können. Daneben ist monatlich ein manuelles Update der libsavi Bibliothek notwendig.

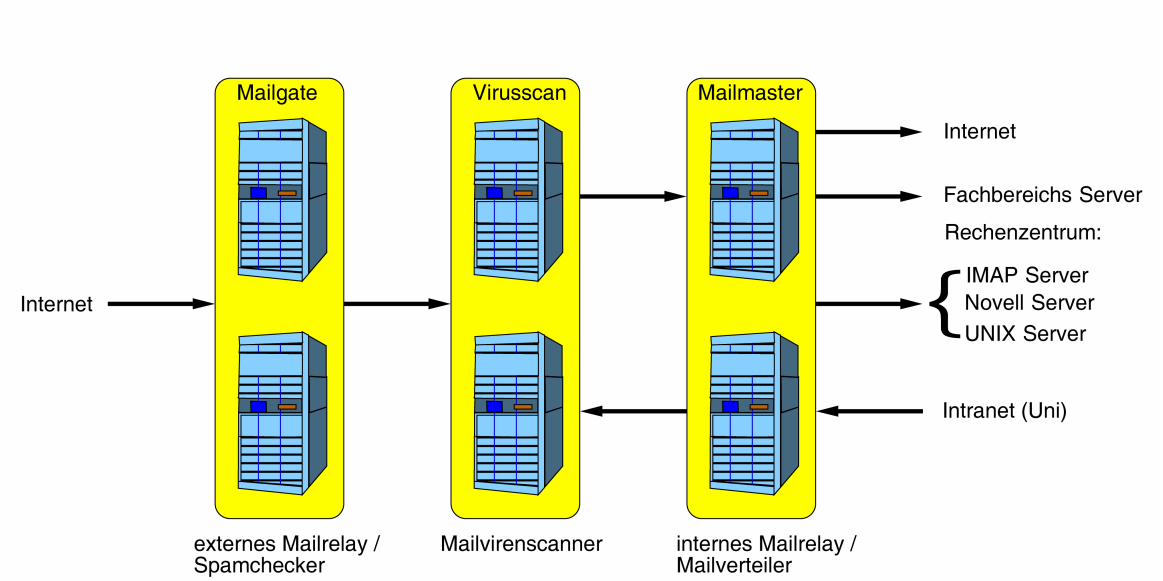

Abbildung 1: Das zentrale Mailsystem der Universität Würzburg.

Das interne Mailrelay (Mailmaster)

Mails, die den Mailviren-Scanner ohne Beanstandung passiert haben, werden von dort über ein weiteres Paar von Relay-Servern an die Mailserver der verschiedenen Fachbereiche oder an die zentralen RZ-Mailserver (IMAP, Novell, Unix) verteilt. Außerdem sind sie für die Auslieferung von Mails an Ziele außerhalb der Universität verantwortlich.

Neben ihrer Funktion als Mailverteiler nehmen diese Relay-Server die Mails von Benutzern aus dem Hochschulnetz entgegen. Dazu muss als *Smart-* oder *Relayhost* (auch Postausgangs-Server oder SMTP-Host genannt) im Mailprogramm des Benutzers „mailmaster.uni-wuerzburg.de“ eingetragen werden. Zum Zweck der Ausfallsicherheit und Lastverteilung wurde das interne Mailrelay ebenfalls redundant ausgelegt.

Damit auch der E-Mail-Verkehr innerhalb der Universität auf Viren überprüft wird, wird jede interne E-Mail, bevor sie endgültig ausgeliefert wird, an die Mailvirenscanner weitergeleitet. Von dort wird sie nach dem Passieren des Scan-Prozesses wieder an die Mailverteiler zurückgeliefert.

Da derzeit noch von jedem Rechner aus dem Universitätsnetz Mail ins Internet gesendet werden kann, ist die Verwendung des Mailrelays optional. Sie wird aber empfohlen, da mittelfristig geplant ist, ausgehenden SMTP-Verkehr durch eine Portsperre zu unterbinden. Ab diesem Zeitpunkt können Mails nach extern nur noch über die zentralen Relay-Server versendet werden. Auf diese Weise wird gewährleistet, dass nur auf Viren geprüfte E-Mails die Universität verlassen.

Der zentrale Spam-Checker

Die Belästigung durch Spam hat sich zu einem großen Ärgernis für die Benutzer entwickelt. Es stellt sich die Frage, warum die zentralisierte Mail-Infrastruktur nicht auch dazu verwendet werden kann, ungewollte Spam-Mails für den gesamten Bereich der Universität herauszufiltern. Dazu ist Folgendes zu bemerken: Im Gegensatz zu Viren in E-Mails, welche durch Mustervergleich gegen eine Virendatenbank eindeutig identifiziert werden können, gibt es keine allgemeingültigen Kriterien, was eine Spam-Mail ist. Es hängt von der persönlichen Einschätzung jedes einzelnen ab. Was für den einen lästiger Werbeschrott ist, beinhaltet für den anderen möglicherweise nützliche Verbraucherinformationen. Aus juristischer Sicht ist es zudem äußerst fragwürdig, E-Mails nicht zuzustellen, ohne hinreichenden Grund und ohne Benachrichtigung des Empfängers.

Aus den genannten Gründen ist es unmöglich, die Auslieferung von vermeintlicher Spam-Mail an zentraler Stelle zu unterbinden. Die Einrichtung eines Spam-Filters muss vom Anwender selbst geleistet und verantwortet werden. Er wird dabei allerdings vom Rechenzentrum unterstützt. Zu Beginn des Jahres 2003 wurde auf den beiden externen Mailrelay-Servern am Anfang der Kette ein *Spam-Checker* installiert, der den „Spam-Gehalt“ jeder einzelnen Mail überprüft. Die Mails werden verschiedenen heuristischen Tests unterzogen und aus den Ergebnissen eine Summe errechnet. Je größer die Summe, umso wahrscheinlicher handelt es sich um Spam-Mail.

Der Spam-Checker basiert auf dem Perl-Modul *SpamAssassin*. Er filtert keine Mail aus, sondern erweitert den Mail-Header, indem er Informationen über das Ergebnis der Spam-Bewertung hinzufügt. Einer dieser Header-Einträge hat die folgende Gestalt:

X-Spam-Level: *********

Dabei entspricht die Anzahl der Sternchen der berechneten Summe. Diese zusätzlichen Header-Zeilen können von den meisten modernen Mail-Programmen für die Konfiguration von Filterregeln verwendet werden. Eine solche Spam-Filterregel könnte lauten:

> Verschiebe alle Mails, deren Header-Feld „X-Spam-Level“ das Muster „********“ enthält, in den Ordner „Spam“.

Dadurch werden alle Mails mit einer Bewertung von acht Punkten oder mehr in den Ordner „Spam“ verschoben. Auf diese Weise ist es möglich, eine individuelle Grenze für Spam festzulegen. Es sei an dieser Stelle empfohlen, dass man als Spam markierte Mails nicht einfach löschen sollte. Es besteht immer die Gefahr, dass auch normale Mails als Spam eingestuft werden. Es ist besser, vermutliche Spam-Mails in einem separaten Ordner zu sammeln, der von Zeit zu Zeit manuell kontrolliert werden sollte.

Da trotz allem nicht jeder Mail-Client über eine geeignete Filtermöglichkeit verfügt, bietet das Rechenzentrum den Benutzern des IMAP-Servers einen einfach zu konfigurierenden Mail-Filter an. Die Vorgehensweise bei der Konfiguration des Spam-Filters wird im Artikel „Webmail – ein E-Mail-System für die Anforderungen von heute“ genauer beschrieben. Die Besonderheit ist, dass der Filter schon bei der Auslieferung der Mail wirksam wird. Er ist unabhängig vom Mail-Client, mit dem auf den IMAP-Server zugegriffen wird. Der Filter wird einmalig über das Webinterface des Webmailers eingerichtet. Für das Lesen der Mails kann jeder IMAP-fähige Mail-Client verwendet werden, der Webmailer ist dafür nicht mehr notwendig.

Bilanz

Ab Mitte März 2002 wurde die Mail für die ersten Institute über das zentrale Mailrelay geleitet und die Zentralisierung danach bis zum Ende des Sommersemesters sukzessive auf alle Fachbereiche ausgedehnt. Dies führte zu einem kontinuierlichen Anstieg des Mailaufkommens. Abb. 2 veranschaulicht die Entwicklung über das Jahr hinweg. Im Laufe des Wintersemesters stieg die Zahl der Mails weiter an und erreichte am Ende des Jahres ein Niveau von täglich etwa 45.000 Mails an einem normalen Tag.

Im Jahr 2002 wurden insgesamt etwa 44.000 mit Viren infizierte Mails abgefangen. Abb. 3 zeigt die jährliche Entwicklung des täglichen Virenaufkommens. Im Durchschnitt wurden täglich zwischen 100 und 200 Viren detektiert. An Spitzentagen wurden bis zu 1.200 Viren abgefangen.

Der sprunghafte Anstieg der detektierten Viren Mitte April ist auf den Ausbruch einer neuen Variante des Klez-Virus zurückzuführen. Seitdem ist Klez-H der häufigste Virus. Etwa jeder zweite Virenvorfall ist auf diesen Schädling zurückzuführen. Tatsächlich ist die Zahl noch höher, da die neue Variante bis zum nächsten monatlichen Update des Virenscanners als Klez-G identifiziert wurde. Abb. 4 stellt die zehn am häufigsten aufgetretenen Viren für das Jahr 2002 dar. Entgegen dem globalen Trend wurde die Universität Würzburg von Bugbear weniger stark getroffen. Bemerkenswert ist, dass sich Sircam auch nach vielen Monaten seit dem ersten Auftreten immer noch weit oben in der Rangliste halten kann.

Zu Beginn des Jahres 2003 wurde der neu ausgebrochene Virus Sobig-A am häufigsten abgefangen. Seit seinem Abflauen ist es an der Virenfront deutlich ruhiger geworden.

Seit Anfang 2003 ist der Spam-Checker in Betrieb. Im Moment werden mehr als 50% der Mails als Spam klassifiziert (Spam-Level acht Punkte und mehr), mit steigender Tendenz.

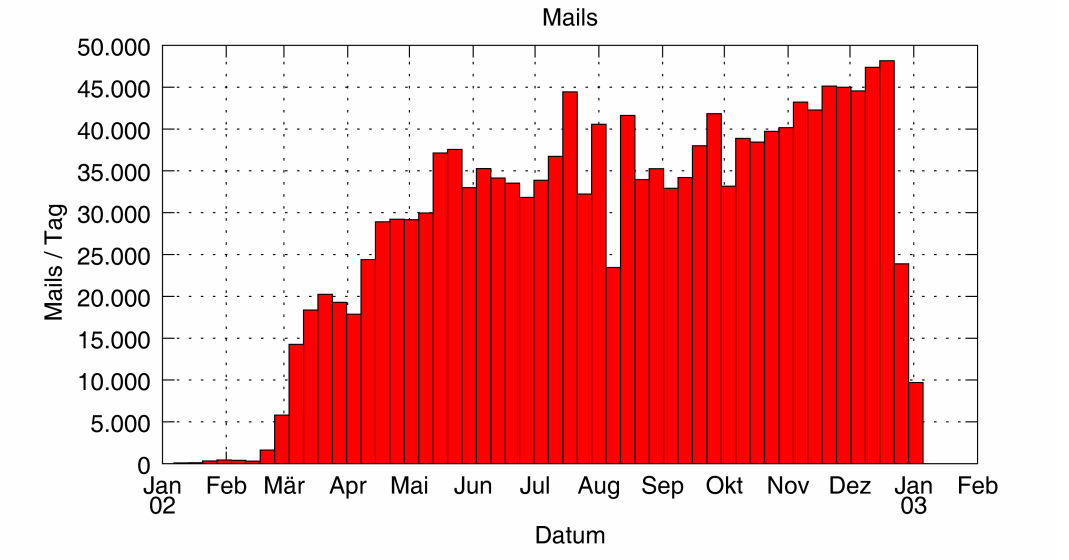

Abbildung 2: Jahresübersicht für das Jahr 2002 der Zahl der täglichen Mails, die über die zentralen Mailrelay-Server geschickt wurden. Die Balken zeigen die über eine Woche gemittelte Anzahl von Mails.

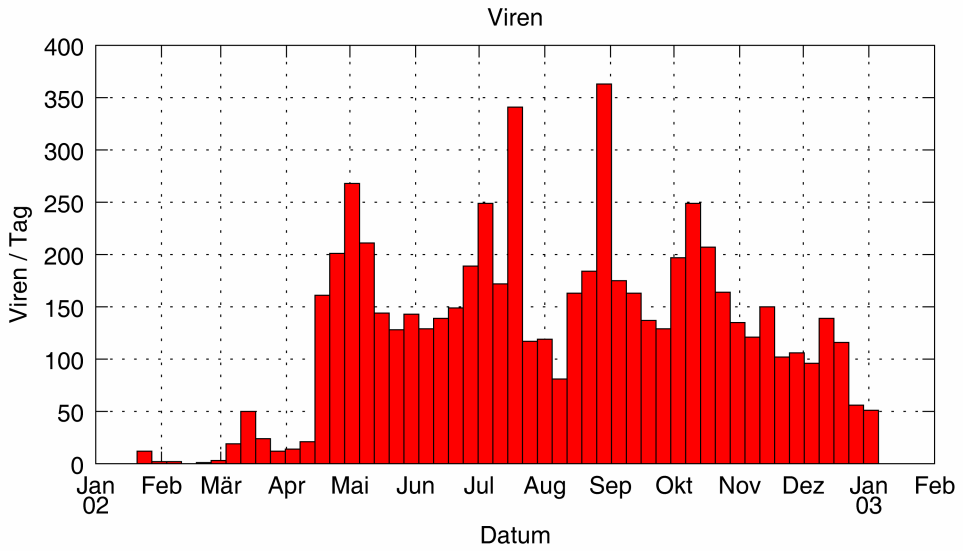

Abbildung 3: Jahresübersicht für das Jahr 2002 der Zahl der täglich von den zentralen Virenscannern entdeckten Viren in E-Mails. Die Balken zeigen die über eine Woche gemittelte tägliche Anzahl abgefangener virenverseuchter Mails.

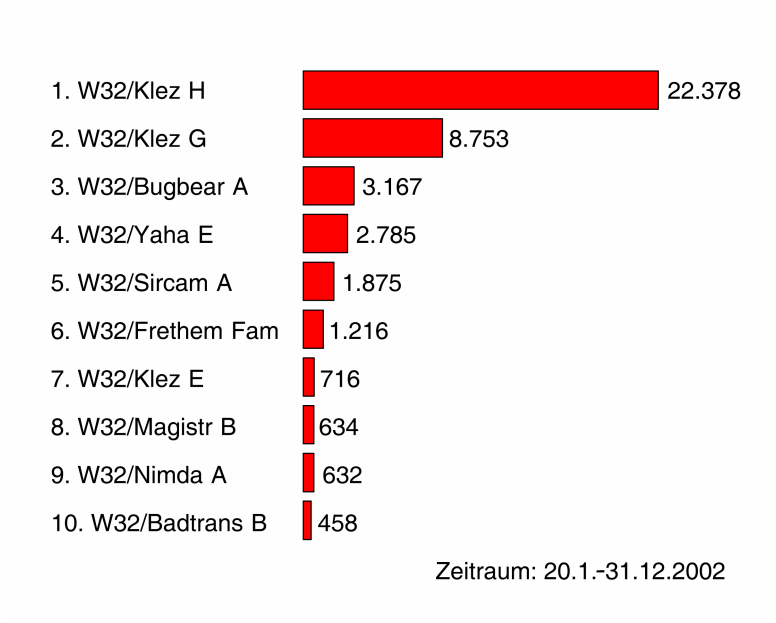

Abbildung 4: Top Ten der am häufigsten vom Virenscanner abgefangenen Viren für das Jahr 2002.

Sicherheit in Netzwerken – die Secure Shell

Ulrich Plödereder

Für viele Mitarbeiter der Universität gehört es zur Selbstverständlichkeit von unterschiedlichen geographischen Orten aus an verschiedenen Rechnern arbeiten zu wollen oder zu müssen. Sei es, dass sie von zu Hause Abläufe auf ihren Rechnern in den Instituten steuern, sich von einem Kongress oder einer Arbeitskreissitzung auf ihren eigenen Arbeitsplatzrechner einwählen oder Berechnungen auf einem Spezialrechner einer anderen Einrichtung durchführen wollen. Allen aufgezeigten Szenarien gemeinsam ist das Anmelden an einem entfernten System von einer lokalen Arbeitsstation aus und der Transfer von Daten über das Netzwerk von einem Rechner zum anderen. In den meisten Fällen werden dazu immer noch Protokolle und Programme eingesetzt, welche vom sicherheitstechnischen Aspekt aus betrachtet sehr bedenklich sind. Im Folgenden soll das Programmpaket Secure Shell als eine sichere Alternative vorgestellt werden.

Problematik

Viele Internetdienste wie *telnet*, *ftp* und die r-Kommandos *rexec*, *rlogin*, *rcp* haben, historisch bedingt, gravierende Sicherheitslücken. Bei ihrem Einsatz läuft die gesamte Kommunikation unverschlüsselt ab, so dass Daten und insbesondere die Anmelde-Informationen wie die Benutzerkennung und das Passwort unverschlüsselt im Klartext über das Netzwerk übertragen werden. Für einen potentiellen Angreifer ist es daher ein Leichtes, mit bestimmten Programmen (z. B. Paket-Sniffern) den Verkehr im Netzwerk abzuhören und so an vertrauliche Daten und Kennwörter zu gelangen. Programme zur Netzwerkadministration, die für derartige Angriffe missbraucht werden können, gehören heutzutage zum Standard-Lieferumfang jeder Linux-Distribution oder werden frei zugänglich im WWW angeboten.

Ziel des Rechenzentrums ist es, in Zusammenarbeit mit den Fachbereichen und Einrichtungen der Universität die Nutzungsmöglichkeit von unsicheren Protokollen möglichst bald in der gesamten Universität zu blockieren und stattdessen die Verwendung der sicheren *Secure Shell* zu erreichen.

Was ist die Secure Shell?

Die Secure Shell ist ein Paket an Protokollen und Programmen zur sicheren Kommunikation innerhalb eines Netzwerks. Jegliche Daten und ausgetauschte Informationen zwischen Client und Server werden verschlüsselt über das Netzwerk transportiert. Die Verschlüsselung auf der Seite des Senders und die Entschlüsselung auf der Seite des Empfängers erfolgt völlig transparent für den Nutzer. Es ist keine grundlegende Änderung der gewohnten Arbeitsweise erforderlich. Die dabei verwendeten Verschlüsselungsmethoden sind, wenn die Schlüssellänge geeignet gewählt wird, nach heutigem Erkenntnisstand und mit endlichem Aufwand an Rechenleistung und Rechenzeit nicht angreifbar. Neben dem Schutz der Daten, wie Verhinderung der Kenntnisnahme durch Dritte, stellt die Secure Shell zusätzliche Mechanismen bereit, welche die Integrität der Daten auf dem Weg vom Sender zum Empfänger gewährleisten.

Zum einen erfolgt vor einer Datenübertragung eine gegenseitige Überprüfung der Identität von Sender und Empfänger, um das Szenario eines *man-in-the-middle-Angriffs* auszuschließen, zum anderen werden durch die Verwendung von *Hash-Funktionen* als so genannter elektronischer Fingerabdruck Manipulationen an den Daten verhindert.

Was kann die Secure Shell ersetzen?

Die Secure Shell ist ein sicherer Ersatz für die unter UNIX bekannten r-Kommandos sowie weiterer Standard-Anwendungen wie telnet oder ftp. Anstatt wie gewohnt eine Sitzung auf einem entfernten Rechner via rsh oder telnet zu starten, verwendet man bei Secure Shell in analoger Weise das *ssh* Kommando. Der Transfer von Dateien zwischen Rechnern erfolgt nicht mehr durch das rcp Kommando oder per ftp, sondern durch die sichere Varianten *scp* oder *sftp* (Secure Copy bzw. Secure FTP). Die Bedienung der Kommandos erfolgt in gewohnter Weise mit analoger Syntax. Der Aufruf der sicheren Kommandos kann entweder von der Kommando-Eingabeaufforderung erfolgen, oder unter Windows mit dem gewohnten Komfort einer grafischen Benutzer-Oberfläche.

Was bietet die Secure Shell noch?

Die Möglichkeiten der Secure Shell (SSH) reichen aber weit darüber hinaus, nur ein Ersatz für ältere und unsichere Befehle zu sein. Für fortgeschrittene Anwender ersetzt die Authentifizierung über einen public-key Mechanismus in Verbindung mit dem SSH-Agenten z. B. die Notwendigkeit, ständig sein Passwort beim Anmelden eingeben zu müssen. Darüber hinaus ist es möglich, beliebige, unsichere Netzwerk-Anwendungen, für die es derzeit keine sicheren Alternativen gibt, über SSH zu *tunneln* und somit gegenüber Dritten abzusichern (*Port Forwarding*). Ein wichtiges Beispiel dafür ist das *X11 Protokoll* (X Window System), das aufgrund seiner besonderen Bedeutung für den Benutzer aus dem Anwendungsangebot nicht wegzudenken ist und das von SSH standardmäßig abgesichert werden sollte (X forwarding). Das Tunneln von X11 Verbindungen ist über SSH nicht nur weitaus sicherer, sondern für den Anwender auch mit weniger Konfigurationsaufwand verbunden als bei der Verwendung der bei X11 implementierten Authentifizierungsmechanismen (xhost, xauth). Eine weitere gebräuchliche Anwendung des Port Forwarding ist die Möglichkeit, gesicherte Verbindungen durch eine Firewall zu gestatten, ohne die Schutzwirkung der Firewall dabei zu kompromittieren. Als konkretes Beispiel sei hier wieder das X Window System genannt: Die zum X11 Protokoll zugehörigen Standard-Ports werden in der Regel aus Sicherheitsgründen an der Firewall zum Kliniknetz geblockt. Das Tunneln durch den offenen SSH Port 22 ermöglicht X11-Verbindungen, ohne die Notwendigkeit die Sperrungen der assoziierten Ports aufzuheben. Daher ist es Benutzern aus dem Kliniknetz möglich, vom Rechenzentrum bereitgestellte X11 Programme zu verwenden, ohne die Sicherheit zu beeinträchtigen. Als Beispiele dafür seien die wissenschaftlichen Anwendungen SPSS und SAS (Statistik), Mathematica und Matlab (analytische Mathematik) oder GCG Seqlab (Gen-Sequenzierung) genannt.

Wo finde ich das Secure Shell Programmpaket?

Für die Secure Shell existieren sowohl zahlreiche kommerzielle als auch nicht kommerzielle Implementierungen für die unterschiedlichsten Betriebssysteme und Rechnerplattformen. Bei den UNIX-Derivaten sowie unter den verschiedenen Linux Distributionen kommt im Allgemeinen die freie Variante *OpenSSH* des OpenBSD Projekts zum Einsatz. Bei Microsoft Windows kann die für Universitäten kostenlose, nicht kommerzielle Version *SSH Secure Shell for Workstations* der SSH Communications Security auf den Arbeitsplatzrechnern eingesetzt werden oder aber das freie Programmpaket *PuTTY* von Simon Tatham. Die SSH Clients für Windows können Benutzer im Novell-Netz direkt aus dem Novell Application Launcher

(NAL) aufrufen. Benutzer von neueren Apple Macintosh Rechnern können beim Unix basierten MacOS X standardmäßig das mitgelieferte OpenSSH verwenden. Für das klassische MacOS 9 und darunter gibt es alternativ die Freeware *NiftyTelnet 1.1 SSH* oder *MacSSH*.

Schlussbemerkung

Das Rechenzentrum empfiehlt dringend jedem Anwender, sowohl aus Gründen der Sicherung der eigenen IT-Ressourcen als auch aus der Verantwortung gegenüber Dritten, die Verwendung unsicherer Programme und Dienste möglichst umgehend einzustellen und als Alternative die Secure Shell zu verwenden. Bei Fragen und Problemen stehen Mitarbeiter des Rechenzentrums über die Hotline (Tel. 5050) jederzeit zur Verfügung.

Literatur und andere Quellen

Daniel J. Barret and Richard E. Silverman: "SSH – The Secure Shell", O'Reilly 2001

Die SSH-Implementierung des OpenBSD-Projekts: www.openssh.org

Homepage der SSH Communications Security: www.ssh.com

PuTTY: A free Win32 Telnet/SSH Client: www.chiark.greenend.org.uk/~sgtatham/putty

MacSSH: Secure Shell Support for Macintosh: www.macssh.com

Maßnahmen zur Erhöhung der IT-Sicherheit an der Universität Würzburg

Hartmut Plehn, Matthias Reichling, Christian Rossa

Macht man sich einerseits die zentrale Rolle deutlich, die der Informationstechnologie in der Universität zukommt und andererseits die Gefahren und Risiken bewusst, denen die IT-Ressourcen ausgesetzt sind, dann stellt sich die berechtigte Frage: Was unternimmt die Universität bereits jetzt zum Schutz und was müsste sie noch unbedingt tun?

Einleitung

Die Bedrohungen und Gefahren, denen die IT-Ressourcen der Universität täglich aus dem Internet aber auch aus dem Hochschulnetz ausgesetzt sind, sind nach den Beobachtungen des Rechenzentrums gewaltig. Dringend erforderlich wäre es umfassende Schutzmaßnahmen sowohl in den Fachbereichen und Einrichtungen als auch im Rechenzentrum zu veranlassen. Doch für die Planung und Umsetzung von IT-Sicherheitsmaßnahmen benötigt man Personal. Dieses Personal steht derzeit zumindest im Rechenzentrum nicht zur Verfügung. Die wahrzunehmenden zentralen Kernaufgaben lassen leider keinen personellen Spielraum dafür.

Legt man die Erfahrungen der letzten Jahre zu Grunde, dann muss man davon ausgehen, dass auch in Zukunft die Bemühungen um die Sicherheit der IT-Ressourcen ein permanentes Reagieren auf die aktuellen Entwicklungen sein werden. Das bedeutet, dass man IT-Sicherheit nicht durch einen einmaligen Kraftakt erreichen kann, vielmehr werden die Anstrengungen, die IT-Ressourcen der Universität zu schützen, eine für das Wohl der Universität sehr wichtige Daueraufgabe sein. Einerseits muss man sich darüber im Klaren sein, dass es keinen hundertprozentigen Schutz geben kann, andererseits muss aber alles dafür getan werden, um die IT-Sicherheit auf ein definiertes Niveau zu bringen.

Der Schutz der IT-Systeme und der Schutz der Daten – Werkzeuge der Wissenschaftler und Fundament der Forschungsarbeit – sollten einen entsprechenden Aufwand gerechtfertigt erscheinen lassen. Doch eine Lösung des Personalproblems ist derzeit nicht in Sicht. Andererseits erscheint es extrem gefährlich so lange zu warten, bis alle Rahmenbedingungen erfüllt sind. Es ist sehr wichtig, möglichst umgehend alles Denkbare und Machbare zum Schutz der IT-Ressourcen im Hochschulnetz zu tun. Die unten angeführten Sicherheitsmaßnahmen kann das Rechenzentrum derzeit gerade noch mit dem vorhandenen Personal abdecken. Es ist wichtig darauf hinzuweisen, dass sie keinen perfekten Schutzschild darstellen, sondern lediglich die Breite der Angriffsfront ein klein wenig reduzieren.

Nicht zu unterschätzen ist dagegen das deutliche Mehr an IT-Sicherheit, das man erreicht, wenn die Fachbereiche/Institute und Einrichtungen der Universität das dezentrale Betreuungskonzept ganz konsequent umsetzen. Denn gut gepflegte IT-Systeme lassen einen Großteil der Angriffe ins Leere laufen.

Sofortmaßnahmen

Auf Grund der dramatischen Entwicklung im Sicherheitsumfeld hat das Rechenzentrum bereits vor etwa zwei Jahren damit begonnen, IT-Sicherheitsmaßnahmen schrittweise zu testen, in Betrieb zu nehmen und im Betrieb zu pflegen. Im Einzelnen sind es:

- Durchführung von uni-internen Rechner-Scans
  Das Rechenzentrum führt in Abstimmung mit den Netzverantwortlichen etwa einmal pro Jahr einen Rechner-Scan über die IP-Adressen der Universität durch und unterrichtet die Einrichtungen über die Ergebnisse.

- Zentralisierung von Diensten
  Die vom Rechenzentrum durchgeführten Rechner-Scans zeigten deutlich, dass auf zahlreichen Rechnern im Hochschulnetz häufig unbeabsichtigt eine umfangreiche Dienstepalette (z. B. WWW-, SMTP- oder FTP-Server) angeboten wird, auf die in der Regel weltweit zugegriffen werden kann. Durch eine weitgehende Rezentralisierung ist es möglich, diese Dienste ohne nennenswerte Einschränkungen für den Benutzer lediglich auf einer überschaubaren Reihe von Servern anbieten zu können.

- Mailvirenscanner
  Um zu verhindern, dass sich über E-Mails eingeschleppte Viren innerhalb der Universität verbreiten, wurde ein zentraler Mailviren-Scanner installiert (siehe Artikel „Zentrale Maßnahmen des Rechenzentrums gegen Viren und Spam“).

- Ersetzen unsicherer Dienste durch sicherere
  Normalerweise wird für die Authentifikationsprüfung ein Passwort benötigt. Bei einer Reihe von Diensten erfolgt die Übertragung von Benutzerkennung und Passwort im Klartext. Solche Dienste (z. B. telnet, POP3) sollten möglichst umgehend flächendeckend durch sicherere Dienste ersetzt werden. Das Rechenzentrum stellt diese alternativen Dienste zur Verfügung (siehe Artikel „Sicherheit in Netzwerken – die Secure Shell“ und „Webmail – ein E-Mail-System für die Anforderungen von heute“).

- Sperren bzw. Einschränken von Diensten
  Am Zugang vom Internet zum Hochschulnetz wird der Zugang zu einer Reihe von Diensten aus dem Internet ohne Ausnahme gesperrt (z. B. nfs, ntp). Darüber hinaus wird der Zugriff auf eine Reihe weiterer Dienste aus dem Internet grundsätzlich blockiert und nur für einige wenige Server explizit geöffnet (z. B. smtp).

- Sperren von IP-Adressen
  IT-Systeme, die generell nicht aus dem Internet erreicht werden sollen (z. B. Netzwerkkomponenten, Netzwerkdrucker), werden über Access Control Lists (ACLs) bereits am Zugang zum Hochschulnetz gesperrt.

- Sonderbehandlung bestimmter Subnetze
  Soweit technisch realisierbar, werden öffentlich zugängliche Rechner (z. B. CIP-Pools) und Netzanschlüsse (u. a. auch Funknetz) in eigenen Subnetzen zusammengefasst, um die Mitarbeiternetze vor Abhören zu schützen.

Diese Sofortmaßnahmen werden am Zugang vom Internet zum Hochschulnetz durchgeführt. Daraus ergibt sich, dass darüber nur ein partieller Schutz gegen Angriffe von „außen“ erreicht werden kann. Demzufolge können diese Sicherheitsmaßnahmen nicht gegen Angriffe von „innen“ schützen, die von so genannten „Innentätern“ ausgehen. Zum Innentäter wird auch ein Hacker, dem es gelungen ist, einen Rechner im Hochschutznetz in seine Gewalt zu bringen und dieses System als Sprungbrett für weitere Angriffe zu benutzen.

Weitere technische Maßnahmen

Momentan sind alle Endgeräte an der Universität Würzburg standardmäßig aus dem Internet uneingeschränkt erreich- und angreifbar, wenn ihre IP-Adressen am Wingate, dem Anschluss-Router ans Internet, nicht besonders behandelt wird. Man spricht im Firewall-Jargon in diesem Fall von einer so genannten *Black List* für die Liste der nicht erreichbaren Rechner. Es wäre zur Verkleinerung der Angriffsfläche dringend erforderlich, die Grundstrategie am Wingate auf eine *White List* umzustellen. Bei einer White List sind alle Endgeräte im Hochschulnetz von außen zunächst nicht erreichbar. Alle Server, die Dienstleistungen nach außen bereitstellen sollen, müssen aktiv in die White List aufgenommen und explizit am Wingate frei geschaltet werden.

Die Wirksamkeit einer solchen Maßnahme hängt sehr stark davon ab, dass gleichzeitig die danach noch öffentlich erreichbaren Server über andere Mechanismen geschützt werden. Zum einen muss dazu die kompetente Administration der Server im Rahmen der Umsetzung des dezentralen Betreuungskonzepts erreicht werden. Zum anderen müssen die Server in Zonen niedrigerer Sicherheitsniveaus, so genannten DMZs (siehe Artikel „Sniffer, Hacker, Firewalls“), gesammelt werden, damit sie im Falle eines erfolgreichen Einbruchs nicht als Sprungbrett für weitere Angriffe auf interne Rechner verwendet werden können.

Weiterhin ist zu beachten, dass die Fachbereiche zum Teil sehr unterschiedliche Anforderungen im Hinblick auf Sicherheit und Betrieb von eigenen Servern haben. Es werden daher bis zu einem gewissen Grad auch Maßnahmen benötigt, die die Teilnetze verschiedener Fachbereiche voreinander schützen.

Der aus Sicht eines Fachbereichs mit eigenem EDV-Personal verlockende Lösungsansatz, eine Firewall vor das eigene Teilnetz zu platzieren, hat einige gravierende Nachteile:

- Firewalls sind von ihrer Konzeption und Leistungsfähigkeit dafür gedacht, am relativ langsamen Übergang zu einem Internet-Provider eingesetzt zu werden. Die Gebäude der Universität sind meist mit Übertragungsraten von 622 Megabit oder neuerdings 1 Gigabit pro Sekunde angebunden. Nur sehr leistungsfähige und teure Firewalls können solche Datenraten weitervermitteln, ohne die Kommunikation stark „auszubremsen“.

- Bei der strukturierten Verkabelung der Gebäude mit Lichtwellenleitern werden am Übergabepunkt vom Gebäude- zum Backbone-Netz Hunderte von Anschlüssen auf einer vom Rechenzentrum administrierten Komponente zusammengeführt. Es gibt daher keinen technisch sinnvollen Einsatzort für eine Firewall, da nirgends im Gebäude eine einzelne Verbindung existiert, in welche die Firewall eingehängt werden könnte. Die Beschaffung einer eigenen Netzkomponente zur Aufnahme der Lichtwellenleiterstrecken durch einen Fachbereich würde hohe zusätzliche Kosten verursachen.

- Eine hohe Verfügbarkeit des Datennetzes gewinnt zunehmend an Bedeutung, weswegen künftig jedes Gebäudenetz mit mindestens zwei voneinander unabhängigen Glasfaserstrecken angebunden werden soll. Eine Firewall könnte nur eine Strecke überwachen, so dass eine ausfallsichere Anbindung nicht möglich wäre. Die Firewall selbst würde noch eine zusätzliche Fehlerquelle in der Gebäudeanbindung darstellen.

- Eine Firewall vor einem Fachbereichs-Teilnetz versetzt alle anderen Bereiche der Universität, insbesondere zentrale Einrichtungen wie die Universitätsbibliothek und das Rechenzentrum, nach „außen“. Das Management der Netzkomponenten und die Unterstützung des Fachbereichs bei der Fehlersuche durch das Rechenzentrum sind in diesen Netzen nur noch eingeschränkt möglich. Bei sehr vielen Diensten, u. a. Mail-Nutzung bei Modem-/ISDN-/DSL-/VPN-Einwahl oder in Rechner-Pools, Remote-Administration, Videokonferenzen, Software- und Datenbank-Bereitstellung, sind Behinderungen durch eine Firewall nur schwer zu vermeiden, weil sie tief in die interne Kommunikation eingreift.

- In den Bereichen finden sich zwar einige fest angestellte IT-Spezialisten oder auch die einen oder anderen technisch versierten Assistenten bzw. Hilfskräfte, die in der Lage sind, eine Firewall einzurichten und zu administrieren. In den wenigsten Fällen ist aber eine kompetente Urlaubs- und Krankheitsvertretung oder eine Kontinuität in der Betreuung der Firewall zu gewährleisten.

- Die Einrichtung eigener Firewalls durch einige Fachbereiche bringt die Universität als Ganzes in Sachen IT-Sicherheit nicht weiter. Der Aufwand zum Betrieb einiger weniger Fachbereichs-Firewalls würde an zentraler Stelle gebündelt allen Bereichen den gleichen großen Nutzen bringen.

- Wie im Artikel "Sniffer, Hacker, Firewalls" dargelegt wird, gibt es momentan eine sehr starke Tendenz, fast beliebige Anwendungen über WWW-Server und die dort verwendeten Ports 80 bzw. 443 abzuwickeln. Dies könnte dazu führen, dass einerseits die derzeitige Bedeutung von Firewalls abnimmt, da eine Firewall nur bedingt unterscheiden kann, ob gerade öffentliche Informationen abgerufen werden oder ob Online-Banking genutzt wird. Andererseits werden Maßnahmen zur Sicherung der DMZ und der darin befindlichen Server immer wichtiger werden.

Die einzig sinnvolle Lösung, die bei geringst möglichem Aufwand den größten Nutzen für die Universität bringen würde, ist in Abb. 1 dargestellt. Am Wingate käme eine Firewall mit einer White List zum Einsatz. Die Netze der Fachbereiche würden voreinander geschützt werden, indem an den vier zentralen Netzknoten Hubland, Sanderring, Röntgenring und Kliniken direkt auf den dortigen Routern entsprechende ACLs definiert werden.

Das Netz würde primär in drei Sicherheitszonen eingeteilt werden. Die reinen Arbeitsplatzrechner in Zone C sind vom Internet und von anderen Teilnetzen nicht mehr erreichbar. In Zone B werden alle internen Server (z. B. zentrale Server in der Universitätsbibliothek oder im Rechenzentrum) gesammelt. Alle aus dem Internet öffentlich erreichbaren Server werden in der

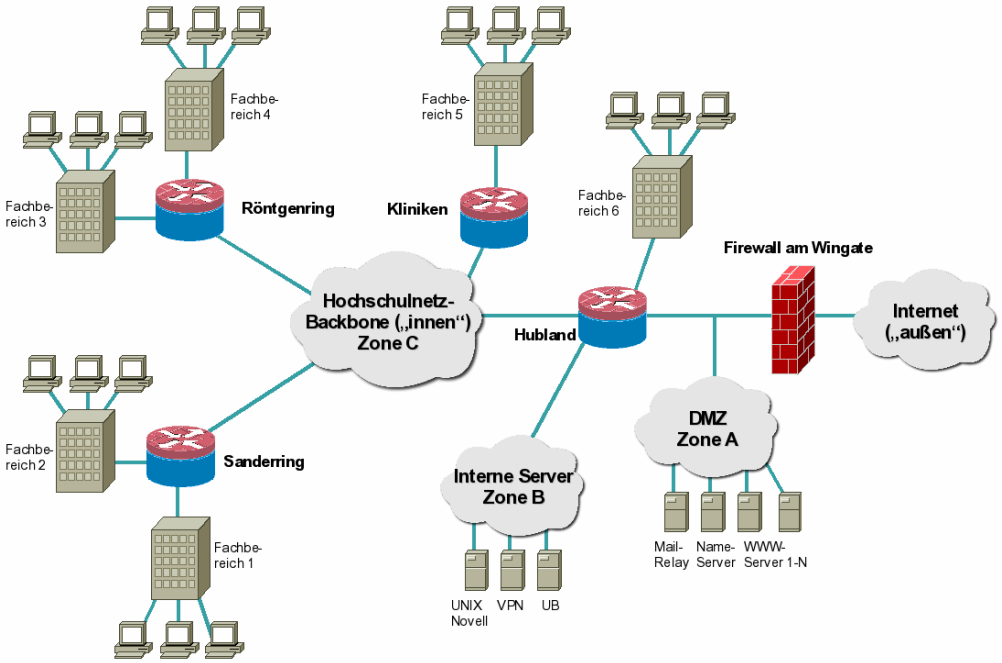

Abbildung 1: Die Heterogenität des Hochschulnetzes erfordert ein Konzept, bei dem neben einer DMZ und dem klassischen Einsatz einer Firewall am Verbindungspunkt zum Internet weitere Sicherheitszonen definiert werden können, die die unterschiedlichen Sicherheitsbedürfnisse der verschiedenen Einrichtungen berücksichtigen lassen. Die Server in Zone A und Zone B müssen sich nicht physikalisch an einem Ort befinden, sondern können in den Fachbereichen aufgestellt bleiben. Sie werden über VLANs virtuell in die entsprechenden Netzzonen eingebunden.

DMZ (Zone A) untergebracht. Über Virtuelle LANs würde gewährleistet werden, dass diese Server sich netztechnisch in der DMZ befinden, obwohl sie physikalisch im Rechnerraum eines Fachbereichs stehen, siehe auch Abschnitt 3.3.8.2 im Bericht des Arbeitskreises „Security-Management“.

Es würden nur wenige Bereiche der Universität mit ganz speziellen Anforderungen an die Datensicherheit wie z. B. die Zentralverwaltung oder die klinische Versorgung verbleiben, die im Rahmen dieses Konzepts besonders behandelt werden müssten.

Die Realisierung des vorgestellten Firewall-Konzepts in der gesamten Universität hängt von der zügigen Fertigstellung des Lichtwellenleiter-Datennetzes ab. Ein Beginn wäre kurzfristig möglich, erfordert aber gemeinsame Anstrengungen aller Bereiche der Universität.

Organisatorische Maßnahmen

Die qualifizierte und kompetente Betreuung aller IT-Systeme in der Universität ist die tragende Säule einer durchdachten IT-Sicherheitspolitik. In diesem Bewusstsein setzte die ständige Kommission für Angelegenheiten des Rechenzentrums bereits Mitte 2000 einen Arbeitskreis mit dem Namen „Betreuungskonzept“ ein und beauftragte ihn, ein Konzept zur Verbesserung der Betreuung dezentraler Rechner in der Universität Würzburg zu erarbeiten. Das Konzept wurde im Februar 2001 der Kommission vorgelegt. Noch im gleichen Monat wurde es der Hochschulleitung überreicht.

Die Kernaussagen des Konzeptpapiers sind die Entwicklung und Umsetzung eines *kooperativen Betreuungskonzepts,* nach dem grundsätzlich vor Ort kompetente IT-Betreuer eingesetzt werden sollen, sowie in jeder Fakultät/Einrichtung mindestens ein hauptamtlicher IT-Bereichsmanager die internen IT-Belange koordinieren soll. Außerdem sind an zentraler Stelle IT-Experten anzusiedeln, die die IT-Spezialisten in den Fachbereichen und Einrichtungen schulen und unterstützen. Wichtig ist, dass dieses Konzept in der Universität Würzburg möglichst zügig umgesetzt wird.

Der ausführliche Bericht des Arbeitskreises ist zu finden unter http://www.rz.uni-wuerzburg.de/infos/benutzungso/betreuung.html.

Außerdem setzte die ständige Kommission für Angelegenheiten des Rechenzentrums Mitte 2000 einen Arbeitskreis mit dem Namen „Security-Management“ ein und beauftragte ihn, eine Sicherheitspolitik für die Informationsverarbeitung im Bereich Lehre und Forschung an der Universität Würzburg zu erarbeiten. Der Arbeitskreis, in dem neben IT-Experten des Rechenzentrums auch Vertreter der Fachbe--reiche und der Zentralverwaltung beteiligt waren, legte seinen Bericht „Konzept für IT-Sicherheit im Bereich Lehre und Forschung der Universität Würzburg“ im April 2002 der Kommission vor. Die Kommission hält die in dem Bericht vorgestellte IT-Sicherheitspolitik für geeignet, der wachsenden Bedrohung der gesamten Informationsverarbeitung in der Universität Würzburg entgegenzuwirken und ein hohes Maß an IT-Sicherheit herzustellen. Der Bericht wurde im Herbst 2002 der Hochschulleitung vorgelegt und erläutert. Im Folgenden werden die zentralen Ergebnisse des Berichts zusammengestellt:

- IT-Sicherheit ist für die Universität Würzburg unverzichtbar. Es ist eine Aufgabe, die nur in großer Solidarität zu meistern ist, wenn sie von allen Fachbereichen und Einrichtungen der Universität gemeinschaftlich getragen wird.

- IT-Sicherheit ist für die Universität Würzburg so wichtig, dass sie als Aufgabe direkt von der Hochschulleitung wahrgenommen wird.

- Die Hochschulleitung muss ein IT-Sicherheitsmanagement-Team (SMT) mit einer operativen Gruppe (OG) einsetzen. Die Hauptaufgabe des SMT und der OG wird das Umsetzen und Fortschreiben des IT-Sicherheitskonzepts sowie das Bearbeiten von IT-Sicherheitsvorfällen sein.

- Die operative Gruppe (OG) ist für das Koordinieren aller technischen und organisatorischen IT-Sicherheitsmaßnahmen zuständig. Aus Synergiegründen soll die operative Gruppe im Rechenzentrum angesiedelt werden

- Die Fachbereiche und Einrichtungen müssen IT-Sicherheitsbeauftragte ernennen und mit der erforderlichen Kompetenz ausstatten. Ihre Aufgabe ist das Koordinieren und Umsetzen der IT-Sicherheitsmaßnahmen im jeweiligen Zuständigkeitsbereich.

- Das Rechenzentrum soll im Rahmen der personellen Möglichkeiten unverzüglich unbedingt benötigte Maßnahmen zum Schutz vor Angriffen aus dem Internet ergreifen.

- Es ist darauf zu achten, dass IT-Sicherheitsmaßnahmen die Lehre und Forschung nicht unnötig einengen bzw. behindern. Aber die Aufgaben der Lehre und Forschung sind kein Freibrief für überzogene Forderungen nach ungehinderter IT-Nutzung auf Kosten der Sicherheit.

Der komplette Bericht des Arbeitskreises ist zu finden unter
http://www.rz.uni-wuerzburg.de/infos/sicherheit/AK_Sec_Konzept.pdf.

Webmail – ein E-Mail-System für die Anforderungen von heute

Hartmut Plehn

Mit der zunehmenden Verbreitung von häuslichen Arbeitsplatzrechnern, mobilen Geräten im WLAN oder auch Internet-Terminals bei Kongressen und sonstigen Veranstaltungen wird der mobile Zugriff auf die Electronic Mail überall und jederzeit immer wichtiger. Anders als beim WWW, wo ein mehr oder weniger beliebiger Browser zur Informationsbeschaffung ausreicht, erfordert die E-Mail-Nutzung normalerweise ein vertrautes Mail-Programm, das bei der Einrichtung mit den nötigen Einstellungen konfiguriert werden muss. Auf einem „fremden" Internet-Terminal ist dieses in den seltensten Fällen verfügbar. Die Sicherheitseinstellungen der beteiligten Netzbetreiber schränken außerdem oft den direkten E-Mail-Versand oder -Abruf ein. Das Rechenzentrum hat daher ein kombiniertes Webmail-/IMAP-System entwickelt und eingerichtet, um die mobile Nutzung von E-Mail zu vereinfachen.

E-Mail unterwegs

Für dieses System wird eine WWW-Schnittstelle verwendet, die den Zugriff auf die eigene Mailbox (Abb. 1) und den Versand von E-Mails mit Hilfe eines WWW-Browsers ermöglicht (Abb. 2). Die Nutzung erfordert neben einem https-fähigen und ansonsten beliebigen WWW-Browser nur die Kenntnis der Startseite https://webmail.uni-wuerzburg.de/ sowie der eigenen Login-Daten zur Authentifizierung. Einige wesentliche Einstellungen wie z. B. die Einrichtung einer Weiterleitungsadresse oder einer Abwesenheitsnachricht können ebenfalls über das Webmail-Interface vorgenommen werden. Darüber hinaus sind ein Adressbuch und ein einfacher Kalender integriert.

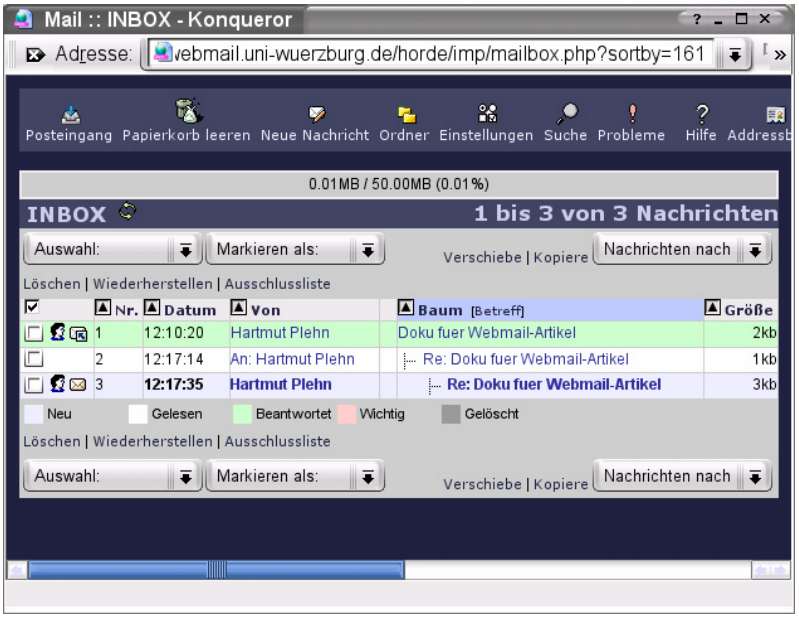

Abbildung 1: Im Webmail-Interface werden die eingegangenen E-Mails mit Status-Informationen und auf Wunsch hierarchisch gruppiert angezeigt.

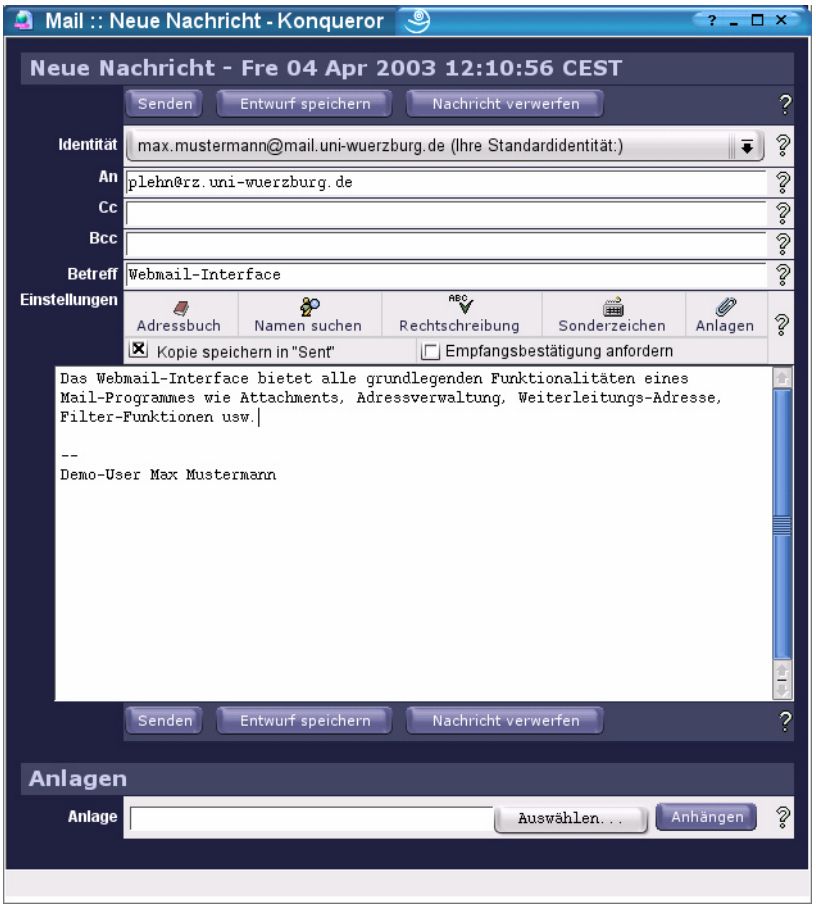

Abbildung 2: Eigene Mail-Texte werden in einem WWW-Formular eingegeben und per https zum Webmail-Server übertragen. Dort werden daraus dynamisch E-Mails erzeugt, die zum Adressaten versendet und im eigenen „Sent“-Ordner auf dem IMAP-Server abgelegt werden.

Der im Hintergrund des Webmail-Systems arbeitende IMAP-Server (Internet Mail Access Protocol) bietet gegenüber den früher für Mailboxen primär eingesetzten POP3-Servern den Vorteil, die empfangenen und versendeten E-Mails in einer hierarchischen Ordnerstruktur ablegen zu können. Somit sind im Webmail-Interface auch alle früheren und von unterwegs versendeten E-Mails wohlgeordnet immer und überall im Internet verfügbar. Die Vorteile des IMAP-Protokolls gegenüber dem POP3-Protokoll sind in Abb. 3 und Abb. 4 dargestellt.

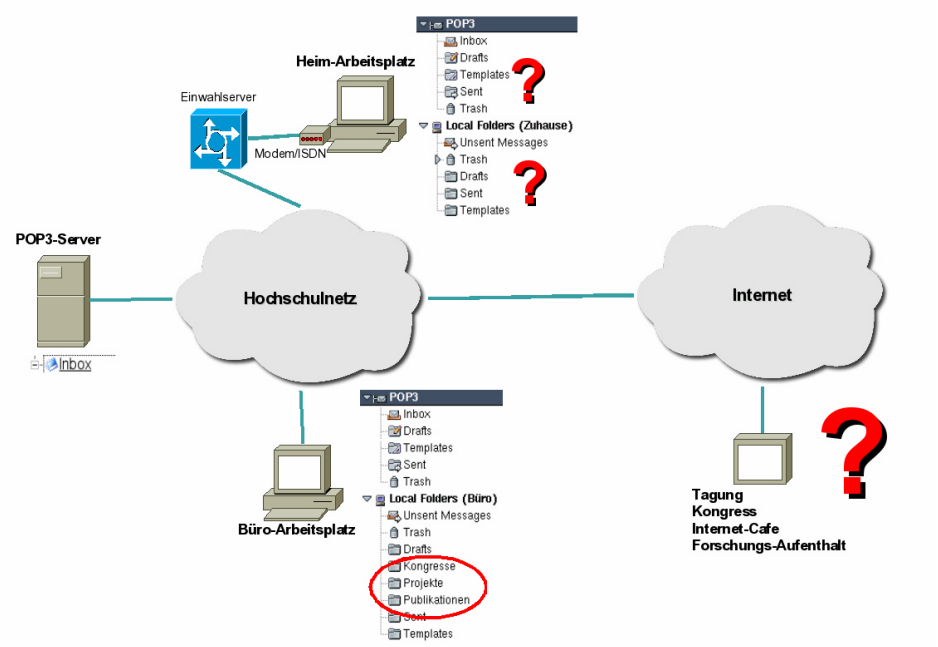

Abbildung 3: Bei der Nutzung eines POP3-Servers stehen an den verschiedenen Arbeitsplätzen immer nur die dort angelegten Ordner zur Verfügung. Im gezeigten Beispiel sind die E-Mails in den lokal am Büro-Arbeitsplatz vorhandenen Ordnern „Kongresse“, „Projekte“ und „Publikationen“ am Heimarbeitsplatz und im Internet nicht zugreifbar. Auf dem POP3-Server werden eingegangene E-Mails in dem einzigen vorhandenen Ordner „Inbox“ abgelegt und zum Abruf bereitgehalten. An entfernten Internet-Stationen ist es aufwändig oder sogar unmöglich, das vertraute Mail-Programm richtig konfiguriert zu installieren.

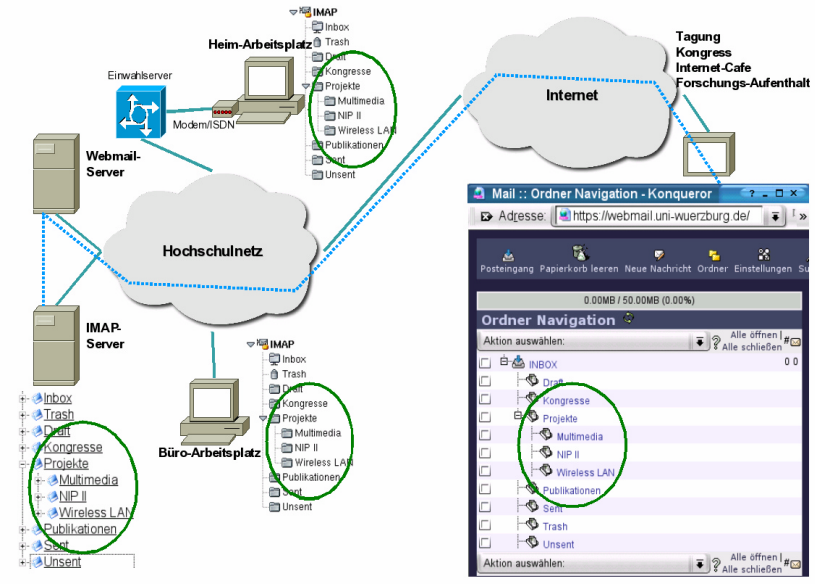

Abbildung 4: Beim IMAP-Protokoll befinden sich alle Ordner und E-Mails auf dem Server, so dass von überall darauf zugegriffen werden kann. Bei der Verwendung des Webmail-Interfaces wird per https, der verschlüsselnden Variante von http, eine Verbindung zum Webmail-Server aufgebaut, der seinerseits die Kommunikation zum IMAP-Server übernimmt. Der Webmail-Server wandelt dynamisch die vom Nutzer in WWW-Formularen eingegebenen Texte in E-Mails und die auf dem IMAP-Server befindlichen E-Mails in WWW-Seiten um.

E-Mail am Arbeitsplatz

Für den mobilen Einsatz bietet das Webmail-Interface zwar große Vorteile, in mancherlei Beziehung kann es aber für einige Nutzer mit einem für die E-Mail-Bearbeitung speziell programmierten E-Mail-Client nicht mithalten. Es ist hierbei weniger die Funktionalität, die eingeschränkt wäre, sondern die Bequemlichkeit der Benutzerschnittstelle. Der IMAP-Server kann aber auch unabhängig vom Webmail-Interface mit jedem beliebigen Mail-Programm verwendet werden, welches das IMAP-Protokoll unterstützt. Auch in diesem Fall bietet der IMAP-Server gegenüber POP3-Servern den großen Vorteil, dass frühere E-Mails in einer Ordnerhierarchie zentral auf dem Server verwaltet und nicht auf den jeweiligen Arbeitsplatz übertragen werden. Somit sind auch alle früheren E-Mails sowohl am Arbeitsplatz als auch zuhause verfügbar, ohne dass man sich selbst um einen Abgleich der Ordnerstruktur kümmern müsste. Das Rechenzentrum empfiehlt, für die Kommunikation zwischen Mail-Client und IMAP-Server die verschlüsselnde Variante des IMAP-Protokolls zu verwenden, die in vielen der gängigen Mail-Programme inzwischen gewählt werden kann (Stichwort IMAPS oder SSL).

Die Kombination aus IMAP- und Webmail-System bietet am normalen Arbeitsplatz die Bequemlichkeit des bevorzugten Mail-Programms mit den genannten Vorteilen gegenüber POP3 sowie die Möglichkeit zur Erledigung der E-Mail von beliebigen Internet-Terminals unterwegs, ohne dort einen Mail-Client installieren oder gar konfigurieren zu müssen. Der einzige Nachteil entsteht dadurch, dass die Benutzung des Webmail-Interfaces und die Verfügbarkeit der vollen Funktionalität des IMAP-Servers (zum Beispiel zum Verschieben von Mails) eine permanente Online-Verbindung voraussetzen.

Kampf dem Spam

Im Zusammenwirken mit der zentralen Spam-Markierung (siehe Artikel „Spam-Mail – mehr als nur ein Ärgernis“) spielt das System seine größte Stärke aus. Über ebenfalls mit dem Webmail-Interface konfigurierbare Filter kann der Schwellwert eingestellt werden, ab dem eine E-Mail als Spam behandelt werden soll (Abb. 5). Das Rechenzentrum empfiehlt, derartige Mails zumindest in der Anfangsphase nicht direkt zu löschen sondern in einen Ordner verschieben zu lassen, den man gelegentlich prüfen und von Hand leeren kann. Diese Spam-Filterung wird schon bei der Zustellung der Mail an den IMAP-Server vorgenommen und nicht erst beim Abruf der E-Mails mit dem Mail-Programm. Sie ist somit unabhängig davon, welcher Mail-Client normalerweise für die alltägliche Arbeit verwendet wird.

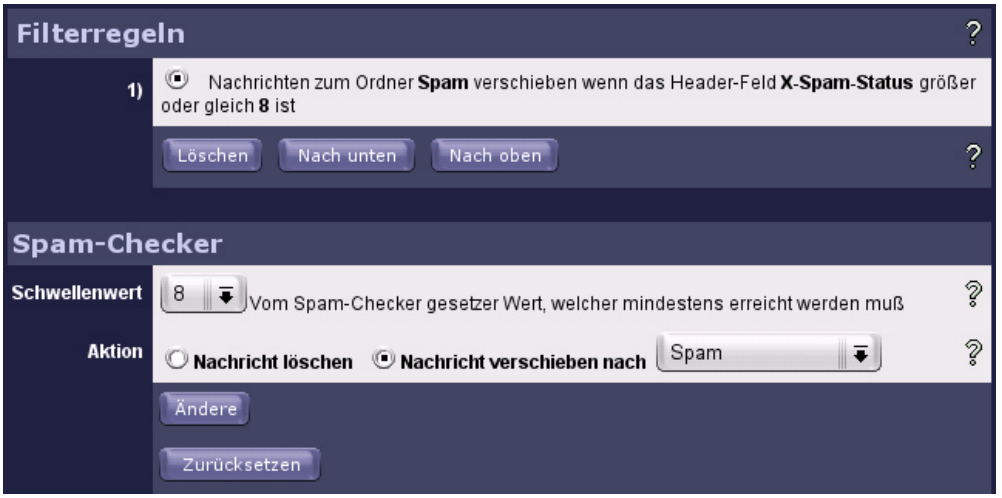

Abbildung 5: Im Webmail-Interface wird der Schwellwert, ab dem zuvor zentral als Spam bewertete Mails gefiltert werden sollen, eingestellt. Im Beispiel werden Mails mit einem Spam-Status von mindestens 8 in den Ordner „Spam“ verschoben. Dies geschieht schon bei der Auslieferung der Mails und ist somit unabhängig vom verwendeten Mail-Programm.

Ausstattung und Nutzung

Das Webmail-/IMAP-System besteht aus zwei identisch ausgestatteten Linux-PCs und einem 140 Gbyte großen Festplatten-RAID-System. Jeder der beiden Rechner kann nach administrativem Eingriff sowohl den Webmail- als auch den IMAP-Dienst alleine übernehmen, falls einmal einer der Rechner ausfallen sollte. Beide Rechner laufen seit der letzten Betriebssysteminstallation im Mai 2002 ununterbrochen durch. Die Verfügbarkeit der Dienste wurde höchstens gelegentlich durch das Einspielen der erforderlichen Sicherheits-Patches nur sehr kurzzeitig und in der Regel vom Benutzer unbemerkt eingeschränkt.

Es kommen die Open Source-Software-Produkte Cyrus IMAP (www.cyrusoft.com) sowie IMP, Kronolith und Turba aus dem Horde-Projekt (www.horde.org) zum Einsatz. Die Anpassung an lokale Gegebenheiten sowie die Programmierung der Schnittstelle zur zentralen Benutzerdatenbank und des Spam-Filters wurden nach Vorgaben des Rechenzentrums extern vergeben.

Seit dem Sommersemester 2002 werden Mitarbeiter auf Wunsch und alle neu immatrikulierten Studierenden standardmäßig auf diesem System eingetragen. Fachbereiche mit eigener Mail-Domäne können unter Beibehaltung der Mail-Adressen auch vollständig auf den Webmail-/IMAP-Server umziehen. Derzeit versorgt das System knapp 4.000 Benutzer.

Nähere Informationen zur Umstellung auf den IMAP-Sever und zur Konfiguration verschiedener Mail-Programme finden sich unter http://www.rz.uni-wuerzburg.de/dienste/email/.

Authentifizierung und Sicherheit im WLAN

Markus Krieger, Hartmut Plehn

Funkwellen machen an Gebäudegrenzen nicht Halt. Ein Funknetz wie das universitätsweite Wireless Local Area Network (WLAN) stellt besondere Anforderungen an Zugriffskontrolle und sonstige Sicherheitsmaßnahmen, weil es anders als gewöhnliche Netzanschlussdosen für jedermann zugänglich ist, der sich in die Nähe einer WLAN-Basisstation, eines so genannten Access Point (AP), begibt. Wie auch mehrfach in der Presse zu lesen war, sind die im WLAN-Standard vorgesehenen Techniken nur bedingt geeignet, um ein WLAN vor unautorisierter Nutzung zu schützen. Das Rechenzentrum hat eine Lösung entwickelt, bei der man sich als Universitätsangehöriger authentifizieren muss, bevor man vom WLAN auf das Hochschulnetz und das Internet zugreifen kann.

Zugriffskontrolle

Das WLAN ist als Gebäude übergreifendes Virtuelles LAN aufgebaut (Abb. 1). Es verwendet zwar im Netzwerk-Backbone dieselben physikalischen Leitungen wie das normale Hochschulnetz, für die Datenpakete gibt es aber nur eine einzige logische Verbindung zum Rest des Hochschulnetzes. Diese Verbindung ist über eine Firewall abgesichert, die zunächst den Datenverkehr von im WLAN neu eingebuchten Endgeräten blockiert. Der Nutzer kann über die in Abb. 2 gezeigte Eingabemaske seine Zugangsdaten übermitteln und damit die Firewall für seinen Rechner frei schalten. Nach erfolgreicher Anmeldung wird die Verbindung offen

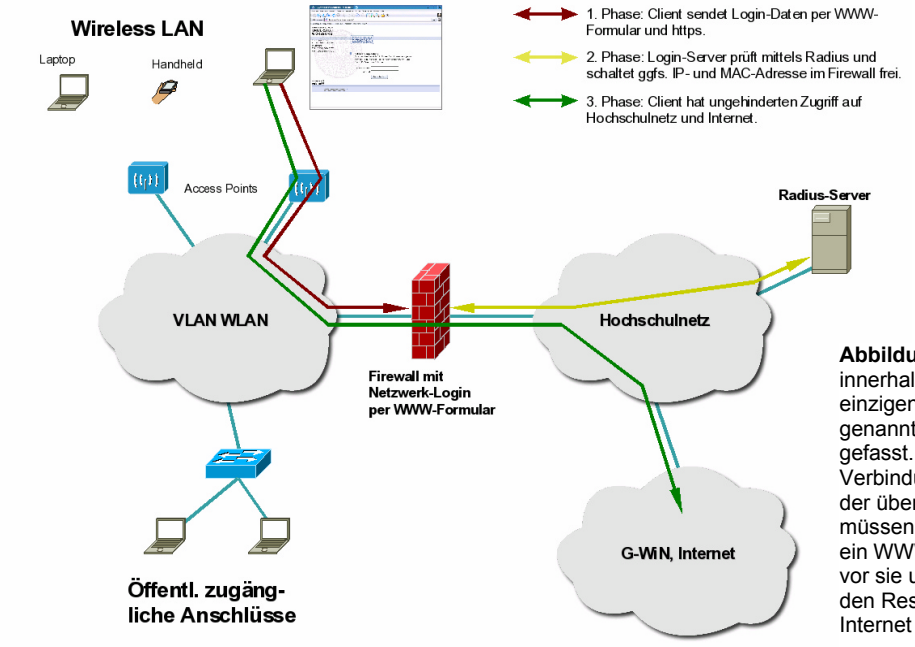

Abbildung 1: Alle WLAN-Bereiche innerhalb der Universität sind zu einem einzigen logischen Netzwerk, einem so genannten Virtuellen LAN, zusammengefasst. Dieses VLAN hat nur einen Verbindungspunkt zum Hochschulnetz, der über eine Firewall gesichert ist. Dort müssen sich berechtigte Benutzer über ein WWW-Formular authentifizieren, bevor sie uneingeschränkten Zugriff auf den Rest des Hochschulnetzes und das Internet erhalten.

gehalten bis sich der Benutzer entweder aktiv abmeldet oder bis er nach 15 Minuten Inaktivität automatisch abgemeldet wird. Die Anmeldedaten werden verschlüsselt per https zur Firewall übertragen, so dass ein „Abhören“ des Passworts durch andere WLAN-Benutzer dabei nicht möglich ist. Die identische Methode zur Authentifizierung wird auch bei einigen öffentlich zugänglichen Netzanschlussdosen im Rechenzentrum und in der Informatik sowie in den an das Hochschulnetz angeschlossenen Wohnheimen verwendet.

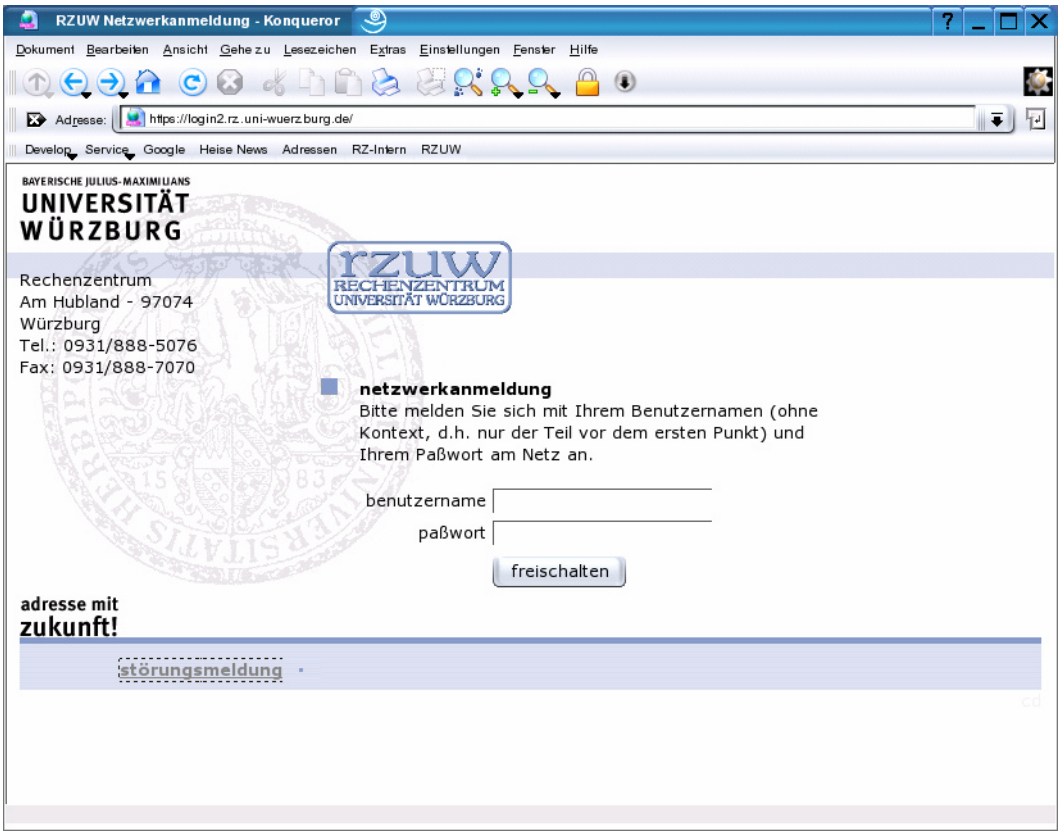

Abbildung 2: Die Eingabemaske für die Authentifizierung im WLAN. Erst nachdem berechtigte Benutzer sich mit ihrem Benutzernamen und Passwort authentifiziert haben, wird ihnen der ungehinderte Zugriff auf das Hochschulnetz und das Internet gewährt.

Sicherheit im WLAN

Im Artikel „Sniffer, Hacker, Firewalls“ wird dargelegt, wie leicht Datennetze abgehört werden können, wenn der Angreifer direkten Zugang zum Netzwerk hat. Bei einem Funknetz hat man diesen direkten Zugang aber überall in einem Umkreis von bis zu 300 m um einen Access Point und unabhängig davon, ob man Zutritt zu dem Gebäude hat, in dem sich der Access Point befindet. Daher ist die Abhörgefahr im WLAN deutlich größer als im kabelgebundenen Netz. Ein Angreifer benötigt lediglich ein Notebook mit WLAN-Karte und spezielle aber überall verfügbare Programme. Eine Anmeldung am Netz wie im vorigen Abschnitt beschrieben ist für derartige Angriffe nicht notwendig.

Im WLAN ist es unbedingt erforderlich, für alle Anwendungen, bei denen sicherheitsrelevante Daten übertragen werden, nur solche Protokolle zu verwenden, bei denen die Datenpakete verschlüsselt werden. Insbesondere muss darauf geachtet werden, dass bei allen eCommerce-Anwendungen die Daten mit https und dass Benutzerdaten mit Passworten nur verschlüsselt übertragen werden.

Ausblick

Die optimale technische Methode, um sowohl die Zugangskontrolle als auch die Sicherheit der übertragenen Daten zu gewährleisten, bietet ein VPN. Dort wird über ein asymmetrisches Schlüsselverfahren eine verschlüsselte Pseudoverbindung in Form eines Tunnels aufgebaut, die sowohl ein Abhören als auch das Einschleusen gefälschter Pakete effektiv verhindert. Ein VPN hat gegenüber der oben skizzierten Methode zur Authentifizierung aber den Nachteil, dass der Aufwand zur Installation und richtigen Konfiguration des VPN-Client-Programms nicht zu unterschätzen ist.

Der im nachfolgenden Artikel behandelte VPN-Concentrator soll auch für das WLAN eingesetzt werden. Möglicherweise wird es dem Benutzer überlassen werden, ob er die bisherige Anmeldemethode ohne Verschlüsselung auf Netzwerkebene oder das VPN verwendet.

Nutzungszahlen

Es sind derzeit 36 Access Points über 12 Gebäude der Universität verteilt installiert. Sie versorgen über 500 verschiedene Benutzer, von denen im Durchschnitt an jedem Werktag ca. 60 aktiv sind. In Spitzenzeiten waren schon bis zu 50 Benutzer gleichzeitig eingeloggt. Nähere Informationen über das WLAN finden sich unter http://www.rz.uni-wuerzburg.de/dienste/kommunikation/wlan.html.

Elektromagnetische Verträglichkeit

Obwohl dieser Artikel primär die Sicherheit der IT-Resourcen und weniger die Sicherheit der sie nutzenden Personen zum Thema hat, sollen hier einige Daten und weiterführende Quellen zur potentiellen Schädlichkeit von WLAN-Funknetzen für Menschen genannt werden, um unbegründeten Ängsten vor einer Gefährdung durch das WLAN vorzubeugen.

Eine umfassende Untersuchung zur Elektromagnetischen Verträglichkeit Umwelt (EMVU) von WLANs findet sich in dem von der Universität Bremen in Auftrag gegebenen Gutachten unter http://www.dmn.tzi.org/wlan/wlan-emvu-gutachten-bremen.pdf . Gemäß diesem Gutachten geht von einem WLAN keine gesundheitliche Gefährdung aus, da nicht nur die gesetzlichen Grenzwerte sondern auch die nach der Empfehlung des nova-Instituts sehr viel niedriger liegenden Vorsorgewerte deutlich unterschritten werden.

Das Thema WLAN wurde auf Betreiben des Personalrats auch bei einer Sitzung des Arbeitsschutzausschusses der Universität Würzburg behandelt. Der Sicherheitsingenieur hat dargelegt, dass die elektromagnetischen Wellen im WLAN nicht ionisierend sind und dass die verwendeten Strahlungsleistungen weit unter den Grenzwerten und unter den Werten vergleichbarer haushaltsüblicher Geräte (z. B. Schnurlostelefone) liegen. Es wurde daher einstimmig festgestellt, dass im Zusammenhang mit dem Betrieb von WLAN-Komponenten keine besonderen Maßnahmen zum Schutz der Beschäftigten erforderlich sind.

„Virtueller“ Zugang zum Hochschulnetz – VPN

Markus Krieger, Hartmut Plehn

Im Zuge der vom Rechenzentrum umgesetzten Sofortmaßnahmen am Internetzugang der Universität, dem Wingate, wurden Access Control Lists (ACLs) mit dem Ziel definiert, die Angriffsfläche im Hochschulnetz zu verkleinern. Dadurch ist eine Reihe von Diensten nicht mehr von außerhalb der Universität ansprechbar. Mit weiteren aus Sicherheitsgründen notwendigen Einschränkungen am Wingate droht sich das Problem, dass Universitätsangehörige von außen nicht mehr ungehindert auf benötigte Dienste zugreifen können, zu verschärfen. Durch die zunehmenden Mobilität, alternative Einwahl-Provider und neue Zugangsformen wie DSL wird der Zugriff von außen auf das Hochschulnetz immer wichtiger. Aus diesem Grund beschafft das Rechenzentrum eine Komponente zum Aufbau eines Virtual Private Networks (VPN), welches die an beliebigen Orten im Internet befindlichen Rechner berechtigter Benutzer „virtuell“ an das Hochschulnetz anbinden lässt.

Bisheriger Zustand

Bei der Verwendung einer Firewall bzw. von Filterregeln (ACLs) entsteht das Problem, dass die externen IP-Adressen von Uni-Angehörigen nicht von denen unberechtigter Benutzer unterschieden werden können, da es keine Zuordnung von IP-Adressen zu Personen gibt. Alle Regeln, die den Zugriff von außen auf das Hochschulnetz aus Sicherheitsgründen einschränken, würden somit auch die berechtigten Benutzer behindern, wenn sich diese beispielsweise über einen günstigen Internet-by-Call-Provider oder T-DSL ins Internet einwählen (Abb. 1). Außerdem gibt es eine Reihe von Diensten, die nur mit einer IP-Adresse aus dem Adressbereich der Universität aufrufbar sind, wie z. B. Datenbanken der Universitätsbibliothek. Eine interne IP-Adresse kann ein Benutzer zuhause derzeit bei einer Einwahl nur erhalten, wenn er sich über den Modemzugang des Rechenzentrums oder über DFN@Home bzw. DFN@Home-DSL einwählt. Benutzer mit analogem oder ISDN-Modem haben die Möglichkeit, nach Bedarf verschiedene Zugangsprovider zu verwenden, und werden genau für diese Einwahl vom jeweiligen Provider abgerechnet. Benutzer einer DSL-Flatrate haben diese Wahlmöglichkeit nicht, da sie eine von Dauer und Anzahl der Einwahlvorgänge unabhängige Monatspauschale entrichten müssen. Da der Zugang mit DFN@Home-DSL nach der Benutzungsordnung für das Hochschulnetz vorrangig nur für studienrelevante bzw. dienstliche Zwecke genutzt werden darf, müssen Benutzer für private Zwecke u. U. einen weiteren Provider verwenden. Gerade bei Benutzern mit einem geringen Verkehrsaufkommen zur Universität tragen sich diese Kosten nicht.

Der Zugriff aus dem Internet auf Dienste im Hochschulnetz erfolgt zudem häufig unverschlüsselt. Da der Datenaustausch durch das Internet über unbekannte Wege und somit potenziell auch unsichere Netze abgewickelt wird, könnte eine Verbindung mitgehört werden. Die Problematik der Klartextprotokolle stellt sich zwar auch im lokalen Hochschulnetz, dort hat aber die Universität selbst Möglichkeiten einem Missbrauch entgegenzuwirken.

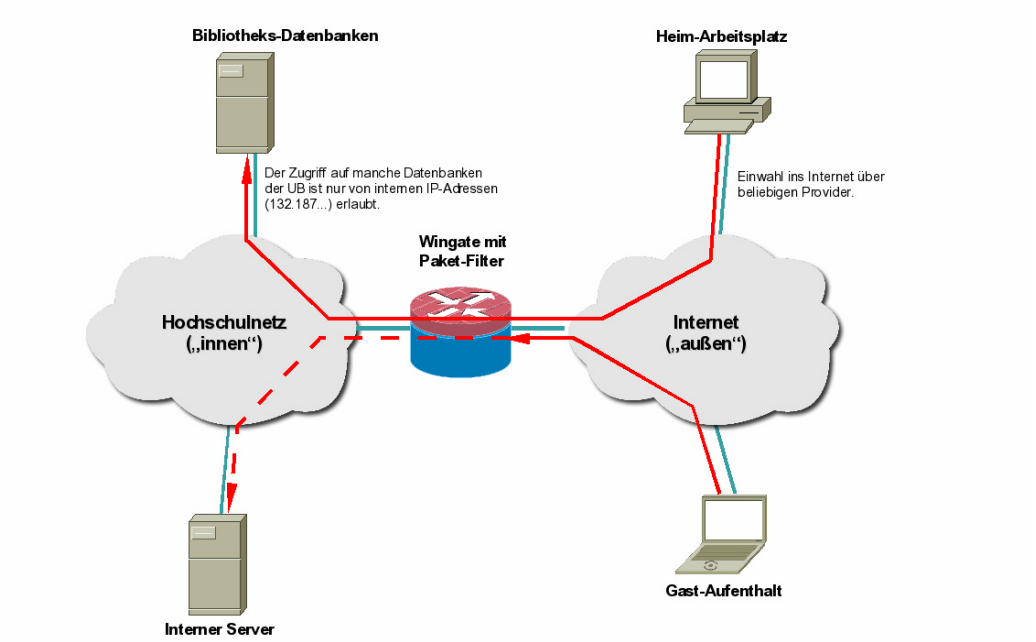

Abbildung 1: Falls sich ein Universitätsangehöriger von seinem Heim-Arbeitsplatz über einen beliebigen Provider oder DSL ins Internet einwählt, kann er bestimmte Dienste im Bereich der Universität (z. B. Datenbanken der Bibliothek) nicht abrufen, da deren Verfügbarkeit aus Lizenzgründen auf Rechner mit IP-Adressen aus dem Adressbereich der Universität Würzburg eingeschränkt sind (rechts oben). Aus Sicherheitsgründen wird zukünftig der Zugriff auf „interne Server“ vermehrt mit Hilfe von ACLs am Wingate-Router blockiert werden. Diese ACLs würden aber z. B. auch einen Mitarbeiter während eines Gast-Aufenthalts auswärts behindern (rechts unten).

Virtual Private Network

Die oben genannten Probleme können durch die Einrichtung eines VPN gelöst werden. Bei diesem tauscht der Rechner des Benutzers nicht mehr mit den jeweiligen Servern direkt Datenpakete über das Internet aus, sondern diese werden durch einen verschlüsselten Tunnel von einem VPN-Clienten auf dem Benutzerrechner an ein VPN-Gateway im Hochschulnetz geschickt. Dieses nimmt die Pakete in Empfang und kann sie ohne die Einschränkungen durch die Filterregeln am Wingate an den Zielserver im Hochschulnetz weiterschicken. Das VPN-Gateway nimmt auch die Antwortpakete des Servers entgegen und reicht sie durch den Tunnel an den VPN-Client weiter (Abb. 2).

Das VPN-Gateway befindet sich innerhalb des Hochschulnetzes der Universität. Es ist über eine extern zugängliche IP-Adresse von außerhalb des Hochschulnetzes erreichbar. Je nach verwendeter VPN-Technologie muss ein Client das Gateway auf einem festgelegten Port ansprechen. Die ACLs am Wingate sind so konfiguriert, dass das VPN-Gateway von beliebigen externen IP-Adressen erreicht werden kann. Der Benutzer muss sich mit seinen persönlichen Zugangsdaten am VPN-Gateway anmelden, bevor er im internen Hochschulnetz befindliche Server ansprechen kann.

Um von einem Rechner das VPN nutzen zu können, muss auf diesem eine Zugangssoftware, ein VPN-Client, installiert und konfiguriert werden. Dieser wird im System wie eine zweite, virtuelle Netzwerkkarte angesprochen, der eine eigene von der Einwahl ins Internet unabhängige IP-Adresse aus dem Adressbereich der Universität zugeteilt wird. Im VPN-Client muss primär die öffentlich erreichbare IP-Adresse des VPN-Gateways konfiguriert werden.

Nach der erfolgreichen Installation muss sich der Benutzer zunächst über einen beliebigen Provider ins Internet einwählen. Danach kann er sich unter Angabe seines Benutzernamens und -passworts am VPN-Gateway authentifizieren. Ist die Anmeldung erfolgreich, wird ein Tunnel aufgebaut, und dem Tunnelende auf

Clientseite, d. h. der virtuellen Netzwerkschnittstelle, wird eine IP-Adresse aus dem Adressbereich der Universität zugeteilt.

Jeglicher Datenverkehr zum Universitätsnetz wird nun nicht mehr direkt über die zur Einwahl ins Internet verwendete Schnittstelle übermittelt. Vielmehr werden die Datenpakete über die virtuelle Netzwerkschnittstelle und durch den dort endenden Tunnel verschickt. Dazu nimmt der VPN-Client die Datenpakete, verschlüsselt sie und baut eine Hülle mit zusätzlichen Informationen um sie herum. Die resultierenden Datenpakete werden durch den Tunnel an das VPN-Gateway geschickt. Dort werden die Pakete ausgepackt und an den Zielrechner im Hochschulnetz weitergeleitet. Die Antwortpakete werden in umgekehrter Richtung entsprechend bearbeitet.

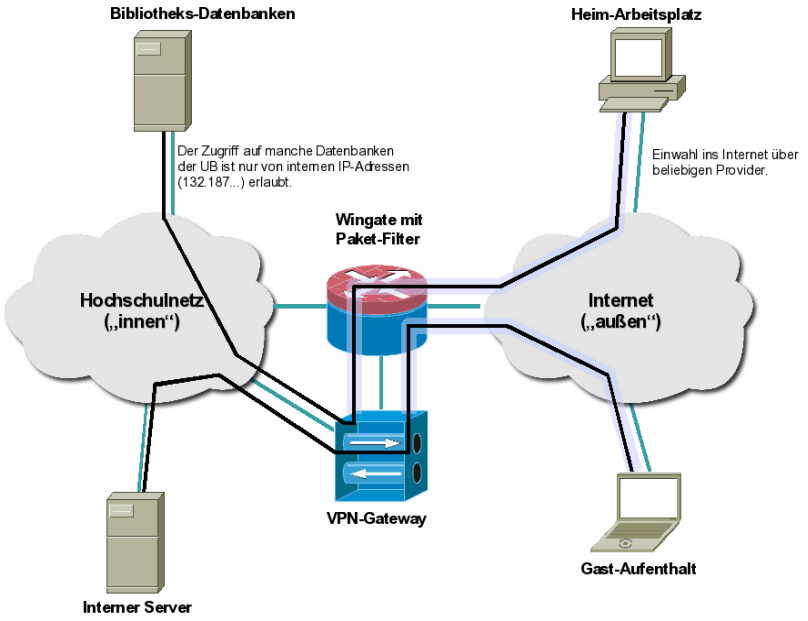

Abbildung 2: Bei der Nutzung des VPN „wählt“ sich der irgendwo im Internet befindliche Rechner in das Hochschulnetz ein, wobei die Verbindung zum Einwahl-Server, dem VPN-Gateway, nicht über Telefonleitungen von Punkt zu Punkt geschieht, sondern über die öffentliche Internet-Infrastruktur. Der Rechner befindet sich „virtuell“ mit einer IP-Adresse der Uni Würzburg im lokalen Hochschulnetz, obwohl er sich real an beliebigen Orten im Internet befinden kann. Die „reale“ IP-Adresse, die der Rechner vor Ort hat, wird nur für die Kommunikation durch den Tunnel zwischen VPN-Client und VPN-Gateway verwendet.

Einsatzgebiete

VPNs werden in Zukunft für verschiedene Szenarien an der Universität Würzburg eingesetzt werden. Zum einen ist ein VPN in Vorbereitung, mit dem sich Benutzer über das Internet ins Netz der Universität einwählen können, um auf interne Dienste zuzugreifen. Zum anderen wird ein VPN für das universitätsweite Wireless LAN aufgebaut, da dort ein hoher Bedarf an einer verschlüsselten Übertragung der Daten über die Funkschnittstelle vorhanden ist. Weitere Einsatzgebiete sind überall dort denkbar, wo sichergestellt werden muss, dass nur berechtigte Benutzer das Hochschulnetz verwenden können, z. B. in Wohnheimen oder an öffentlich zugänglichen Netzanschlussdosen.

Es ist geplant, einen VPN-Concentrator der Firma Cisco mit dem Verschlüsselungsprotokoll IPSec einzusetzen. Für die gängigsten Betriebssysteme (Windows, Linux, MacOS X, Solaris 8) wird für Angehörige der Universität Würzburg ein VPN-Client-Programm der Fa. Cisco frei erhältlich sein. Ob die IPSec-Client-Programme anderer Hersteller ebenfalls problemlos mit dem VPN-Concentrator zusammenarbeiten, muss noch getestet werden.

Die Client-Software und eine Installationsbeschreibung werden über den WWW-Server des Rechenzentrums verfügbar gemacht, sobald der VPN-Concentrator in den Wirkbetrieb geht.