Sicherheit in Rechnernetzen

Dieses Heft der RZ-Mitteilungen ist überschrieben mit „Sicherheit in Rechnernetzen“. Warum ein solches Thema zur gegenwärtigen Zeit?

Im Sommer 1990 wurde im Rechenzentrum (RZ) der Humboldt-Universität das erste lokale Netz installiert und der Zugang zum Deutschen Wissenschaftsnetz über eine 9,6-kbit/s-Leitung zur Zentraleinrichtung Datenverarbeitung (ZEDAT) der Freien Universität realisiert. Wir waren froh, in so kurzer Zeit den Anschluß an weltweite Netze ermöglichen zu können und richteten unsere Bemühungen in der Folgezeit auf den schnellen Ausbau des universitären Rechnernetzes. Unter dem Namen SERVUZ (**SERV**erbasiertes **U**niversitätsrechnernet**Z**) wurde ein Projekt kreiert, das uns in der Zwischenzeit dazu geführt hat, daß die rund 4000 PC und 500 Workstations der Universität in 130 lokale Netze integriert sind und über das Universitätsbackbone der Zugang zum Deutschen Breitbandwissenschaftsnetz (B-WiN) und damit zum Internet ermöglicht wird. Aus der Freude der Nutzer über die raschen Fortschritte ist in der Zwischenzeit eine selbstverständliche Forderung nach Verfügbarkeit und Stabilität des Netzes geworden. Mit der steigenden Zahl der lokalen Netze, der zunehmenden Verflechtung zwischen den Netzen und vor allem den immer komplizierter werdenden Diensten auf diesen Netzen wird die Umsetzung dieser Forderungen jedoch nicht einfacher. Die beeinflussenden Faktoren und die Komplexität sind um ein vielfaches gestiegen.

Während zu Beginn der Netznutzung alle Beteiligten von dem neuen Medium begeistert, an einer sinnvollen umsichtigen Nutzung interessiert, mit Unzulänglichkeiten zu leben bereit waren und sich selbst Regeln des Umganges (Netiquette) auferlegten, ist die Netznutzung heute zu einer „Massenbewegung“ geworden. In vielen Fällen gehört es zum guten Ton, eine Mailadresse zu haben und im Internet zu surfen. Mit dieser breiten Nutzung entwickelten sich neue Dienste wie das World Wide Web, die Netnews u. a., aber auch nicht zu übersehende negative Erscheinungen. In der Millionen zählenden Schar der Nutzer findet man ebenso die „schwarzen Schafe“, die unbewußt unter Mißachtung der Netiquette, aus „sportlichem“ Selbstbestätigungsdrang oder mit bösartigem Hintergrund, fremde Daten ausspähen, verändern oder gar zerstören.

Aus der mehr sporadischen experimentellen Nutzung ist die „Arbeit im Netz“ für viele zu einer Hauptform des wissenschaftlichen Arbeitens geworden. Der vernetzte Computer, ob am universitären Arbeitsplatz oder zu Hause, ist nicht mehr wegzudenken. Nahezu sämtliche Daten, ob der wissenschaftliche Artikel, die Studienarbeit, das Vorlesungsmanuskript oder die Ergebnisse einer Testreihe, sind im Computer gespeichert. In vielen Fällen leider ohne jede weitere Sicherung. Der Wissenschaftler ist von diesem Arbeitsinstrument abhängig geworden und unterstellt die korrekte Funktionsfähigkeit. Havarien, ob im eigenen Rechner oder einem zentralen universitären Fileserver, können heute verheerende Folgen haben, die Arbeit von Monaten oder Jahren zerstören. Mit der zunehmenden Nutzung und der steigenden Abhängigkeit vom Computer ist allein die Existenz des Netzes nicht mehr der bestimmende Faktor, sondern dessen Verfügbarkeit, Stabilität und Korrektheit, d. h. die Sicherheit des Computernetzes und seiner Bestandteile.

Die Gewährleistung der Sicherheit ist durch eine Vielzahl von Faktoren beeinflußt, von denen wir in diesem Heft einige näher erläutern wollen. Dabei beginnen wir mit solchen Themen, die dem Einfluß des einzelnen Nutzers unterliegen und durch seinen bewußten Umgang mit der Problematik schon wesentlich zur Sicherheit des Gesamtsystems beitragen können.

So geben wir Hinweise zur Sicherung des eigenen PC oder zur Vorbeugung gegen den nicht zu unterschätzenden Virenbefall. Wir wollen Ihre Sensibilität dafür wecken, daß sich mit dem Anschluß Ihres Rechners an ein Rechnernetz auch Ihre Verantwortung erhöht. Bei Nichtbeachtung der Grundregeln, z. B. des Paßwortschutzes, kann nicht nur Ihr Computer Schaden nehmen, sondern auch die übrigen Rechner im Netz. Leider haben wir an der Humboldt-Universität schon die negative Erfahrung machen müssen, daß sich Hacker auf die Paßwortdatei gestürzt, allzu triviale Paßwörter geknackt und dann unter falschem Namen ihr Unwesen getrieben haben.

Wir machen darauf aufmerksam, daß auch die z. Z. verfügbaren Programme zur Nutzung des World Wide Web Sicherheitslücken aufweisen können und vor allem, daß Sie erkennen, daß die elektronische Post zwar eine sehr verbreitete und relativ bequeme Kommunikationsart ist, jedoch erhebliche Datenschutzprobleme aufweist. Sicher ist bekannt, daß man die unverschlüsselte E-Mail am ehesten mit der Vertraulichkeit einer Postkarte vergleichen kann.

Zum einen geht es darum, Gefahren aufzuzeigen, denn nur so kann man ihnen am besten begegnen, und zum anderen, Sie mit dem Rüstzeug zu versehen, daß Sie durch Ihr Handeln zur allgemeinen Netzsicherheit beitragen können. In einigen Artikeln des Heftes beschreiben wir die im RZ der Universität eingesetzten Verfahren, um den Grad der Netzsicherheit möglichst hoch zu halten. Eingeleitet wird dieses Heft jedoch durch einen Beitrag eines häufigen Gesprächspartners des RZ, des Behördlichen Datenschutzbeauftragten der Universität, mit dem wir gemeinsam in vielen Fällen nach akzeptablen Lösungen zur Wahrung des Datenschutzes und gleichzeitig eines rationellen Netzbetriebes gesucht haben.

Peter Schirmbacher