TU Clausthal

Rundschreiben des Rechenzentrums

Erzstraße 51
D-38678 Clausthal-Zellerfeld
Tel.: 05323/72-2045

Beide Fakultäten,
sämtliche Fachbereiche und Institute,
Zentrale Einrichtungen,
Verwaltung der TU Clausthal

h i e r

06.10.2004

Rechnersicherheit

In immer stärkeren Maße werden auch die Computer an der TU Clausthal von "Malware" (Viren, Würmer, Trojaner, ...) heimgesucht. Dabei ist das Internet eine mögliche Infektionsquelle, aber auch auf anderen Wegen (Mail-Anhänge, Disketten, CDs, ...) werden Computersysteme häufig kompromittiert. Ziel der Angreifer ist es meist, Daten auszuspähen, zu verändern, zu löschen oder Systeme z.B. für den Austausch illegaler Daten zu missbrauchen (im Rechenzentrum sehen wir das in der Netzstatistik, wenn ein Computer viele Gigabyte von Daten sendet und/oder empfängt).

Überwiegend werden Computer mit Microsoft Windows Software befallen, aber andere Systeme sind ebenso betroffen.

Zu den allerersten und wichtigsten Gegenmaßnahmen gehört es, die eigenen Systeme auf dem aktuellsten "Patch-Level" zu halten. Das wird z.B. durch den Software Update Service (SUS) unterstützt. Siehe dazu die Informationen über den SUS-Server im Rechenzentrum:
http://www.rz.tu-clausthal.de/system+netz/sus-server.shtml.

Ebenso wichtig ist es, die Virenerkennungssoftware immer aktuell zu halten. Zur Erinnerung:
Die TUC ist an die Sophos-Landeslizenz angeschlossen, und hier kann ebenfalls ein automatischer Update-Service eingerichtet werden:
http://www.rz.tu-clausthal.de/software/sophos/.

Als weitere Maßnahme ist inzwischen angeraten, eine **Personal Firewall** zu aktivieren. Bei den Windows-Systemen sollte man, wann immer es geht, der Empfehlung folgen und **Windows XP mit dem Service Pack 2** einsetzen. Dort ist

eine Firewall standardmäßig integriert. Ansonsten gibt es im Netz Systeme, die in der Regel für die private Nutzung sogar kostenlos sind.

Solche Maßnahmen können eine Kompromittierung von Computern durch Ausnutzung von Sicherheitslücken weitestgehend verhindern. Weitere Empfehlungen zur „Härtung von Betriebssystemen“ finden Sie beim DFN-CERT:
http://www.dfn-cert.de/infoserv/bibliothek/betriebssysteme.html

Gelegentlich stellt sich die Frage: warum keine Firewall am Eingang zum Hochschulnetz oder zum Subnetz des Instituts?
Die Antwort ist, dass es für eine Hochschule mit ihren vielfältigen wissenschaftlichen Anwendungen keine Standardkonfiguration gibt, mit der alle leben bzw. arbeiten können. Vor allem aber wird das Problem dadurch nicht beseitigt, denn das große Gefahrenpotential bleiben Angriffe von Computern in der Hochschule selber, die durch Mail-Anhänge, den Internet Explorer, etc. infiziert wurden. Ein einziger infizierter Computer in der Hochschule / in einem Subnetz reicht meist aus, damit sich Viren (auch hinter einer Firewall!) ungestört fortpflanzen und ihr Unwesen treiben können.
Deshalb betonen wir nochmals, wie wichtig es ist, dass die Systemadministratoren/Nutzer in den Instituten **jeden einzelnen Computer absichern**.

Auch Maßnahmen wie NAT (Network Address Translation) sind wenig effektiv. Ursprünglich als Notlösung für den begrenzten IP-Adressraum gedacht, wird NAT heute oft zweckentfremdet, um Rechner mit privaten Adressen zu „verstecken“. Die Folge ist, dass viele normale Netzdienste und insbesondere das Netzmanagement nicht mehr richtig funktionieren. Wir empfehlen deshalb eindringlich, dieses Mittel **nicht** zu verwenden und werden es aus technischen Gründen nicht unterstützen.

Natürlich haben wir (ergänzend zu den Update-Services) **zentrale Sicherheitsvorkehrungen** getroffen. So sind am zentralen Router zwischen Wissenschaftsnetz/Internet und dem Hochschulnetz Ports gesperrt, die als Einfalltore bekannt sind. Weiterhin blockt der zentrale Mail-Server sehr effektiv E-Mails mit Viren und filtert Spam-Mails. Ferner können wir anhand unserer Netzstatistiken Auffälligkeiten feststellen und die betroffenen Institute bzw. Nutzer informieren. Muss dabei einmal ein Computer „abgeklemmt“ werden, so geschieht das, um die anderen Netzteilnehmer zu schützen und den Nutzer selbst bzw. das Institut vor rechtlichen Konsequenzen zu bewahren, falls der betroffene Computer z.B. für einen illegalen Datenaustausch missbraucht wird.

Schutzmaßnahmen an den einzelnen Computern und die zentralen Schutzmaßnahmen durch das Rechenzentrum können ein gutes Niveau an Sicherheit gewährleisten. Trotzdem arbeiten wir – mit Blick auf und in Abstimmung mit anderen Hochschulrechenzentren, dem DFN-CERT und einschlägigen Herstellern – weiter an Sicherheitsempfehlungen und zentralen Sicherheitsmaßnahmen. Dazu gehören Weiterentwicklungen der Netzinfrastruktur und eine Intensivierung der

Netzwerk-Überwachung. Dabei ist immer zu berücksichtigen, dass die wissenschaftliche Arbeit der Nutzer im und mit dem Netz nicht behindert werden darf, und nicht zuletzt sind gesetzliche Auflagen (z.B. das Telekommunikationsgesetz) und Datenschutzbelange zu beachten.
Gleichwertig neben den technischen Maßnahmen steht immer die Unterstützung durch die Mitarbeiter des Rechenzentrums:

Operating/Service-Theke – Tel.: 2626, E-Mail: support@rz.tu-clausthal.de

und die aktuelle Information auf der Webseite des Rechenzentrums:

http://www.rz.tu-clausthal.de.

Gez. Dr. G. Lange, Dipl.-Math. Ch. Strauf