Beirat des Leitungsgremiums
der Universität der Bundeswehr München
für Informations- und Kommunikationsinfrastruktur (IKIS)
Der Vorsitzende

22.11.2001

Maßnahmen zur Eindämmung von „Malware-Funktionen“

Mit der Zunahme der Internetnutzung steigt auch das Risiko, dass von den angeschlossenen Rechnern (von den Administratoren zumeist unbeabsichtigt) „Malware-Funktionen“ ausgehen. Darunter versteht man die negativen Auswirkungen von Viren, Würmern, Trojanern und sonstiger unerwarteter Software-Funktionalität auf andere Rechner und Netzteilnehmer.

Das Bestreben, bestmögliche Arbeitsbedingungen für alle Nutzer des Universitäts-Datennetzes zur Verfügung zu stellen, führt zur Konsequenz, dass

1. alle Teilnehmer möglichst viele Sicherheitsvorkehrungen treffen, damit von „ihrem“ Rechner keine „Malware-Funktionen“ ausgehen können.
2. wenn eine „Malware-Funktion“ eingetreten ist, schnellstmöglich alle Maßnahmen zur Eindämmung und Beseitigung des Schadens ergriffen werden.

Das RZ als Netzbetreiber initiiert nach Kenntnis von „Malware-Funktionen“ an den Subnetzgrenzen (Router) nachfolgende Maßnahmen:

– Information des zuständigen Subnetz-Administrators (seines Vertreters) mit der Bitte um umgehende Fehlerbehebung (Gerät vom Netz nehmen, Abschalten des Gerätes, Fehlerbehebung)
– ist nach maximal 4 Stunden weder ein Ansprechpartner zu erreichen noch Abhilfe erkennbar und gemeldet, so wird das betroffene Subnetz bis auf folgende Funktionen
  - Erreichbarkeit des „kommsrv“ via telnet, ssh und Email-Abruf von dort
  - Erreichbarkeit des „gatesrv“ (WWW, News, DNS)
  - Erreichbarkeit des „sweepsrv“ (Virenschutz)

  vom Hochschuldatennetz abgehängt (Eindämmung durch Konfigurationsmaßnahme auf dem jeweiligen Router des RZ). Insbesondere muss dann zum Versenden von Email der „kommsrv“ benutzt werden.
– ist die Software-Konfigurationsmaßnahme am RZ-eigenen Router aus nachvollziehbaren Gründen nicht möglich, so kann das gesamte betroffene Subnetz vollständig vom Hochschuldatennetz abgetrennt werden (Hardware-Eingriff).

Die eindämmenden Maßnahmen werden nach der durch den zuständigen Subnetzadministrator gemeldeten Behebung der „Malware-Funktion“ vom RZ unverzüglich rückgängig gemacht.

gez. Prof. Dr. Helmut Rzehak

IKIS-Beschluss B 25-10/01 vom 24.10.2001, genehmigt vom Leitungsgremium am 12.11.2001