Auch Ihr Rechner ist gefährdet

Rechner am Internet sind vielfältigen Gefährdungen ausgesetzt.

- **Viren und Würmer** gefährden die Stabilität und Integrität der Rechner und Netze.
- **Trojanische Pferde** werden von Viren und Würmern hinterlassen und von Internetseiten unbeabsichtigt heruntergeladen und spähen vertrauliche Informationen (Kennwörter, Kreditkarteninformationen, Banktransaktionen, …) aus.
- Einbrecher (**Hacker**) dringen über Schwachstellen im Betriebssystem oder über schon vorhandene Trojanische Pferde in Rechner ein, um dort vorhandene Daten auszuspähen oder Rechner zu missbrauchen.

Auch Teilnehmer im Universitätsnetz erleben immer öfter böse Überraschungen, wenn ihr Rechner wegen solcher Kompromittierungen nicht mehr funktionsfähig ist, der Rechner nicht mehr genutzt werden kann und die Wiederherstellung viel Zeit kostet.

Weitergehende Schäden haben die bisherigen Angriffe glücklicherweise nicht verursacht. Aber schon

- **die nächste Virenattacke** könnte nicht nur Netze und Mailserver überlasten, sondern zu Totalverlusten von Daten führen,
- **das nächste Trojanische Pferd** könnte Zugriff auf sensible Daten erlauben,
- **der nächste Einbrecher** könnte Ihren Rechner nicht nur als illegale Tauschbörse für Filme und Software, sondern auch als Server für Kinderpornographie missbrauchen und Sie müssen beweisen, dass Sie den nicht selbst eingerichtet haben.

Nachstehend wollen wir Ihnen Informationen geben, die Ihnen helfen, Ihren Rechner vor solchen Gefahren zu schützen.

Denken Sie daran: Wenige Minuten genügen, um Ihren Rechner zu schützen.

Sichere Konfiguration und Umgang

Stellen Sie das Betriebssystem und Anwendungen so ein, dass Ihr Rechner Schadprogrammen und Angreifern möglichst **wenig Angriffsfläche** bietet! Installieren Sie nur die benötigten Dienste!

Stellen Sie sicher, dass für alle Benutzer, insbesondere aber für Benutzer mit Administrationsrechten nicht zu erratende **Kennwörter** verwendet werden! Ein Angreifer kann tausende Kennwörter in Sekundenbruchteilen ausprobieren.

Konfigurieren Sie **Netzwerkanwendungen** wie **Internetbrowser** oder **Mailprogramm** so, dass auf WWW-Seiten oder in Mails enthaltene Programme nicht ungewollt und unbemerkt ausgeführt werden können! Hinweise, wie Sie die gängigen Programme (Mail-Clients) einrichten sollten, finden Sie unter http://www.rz.uni-freiburg.de/pc/app/mail/index.php oder http://portal.uni-freiburg.de/rz/dienste/email

Software-Update

Moderne Software ist so komplex, dass sie nicht fehlerfrei sein kann. Softwarefehler werden immer wieder von Viren und Würmern wie auch Hackern als Angriffpunkte genutzt.

Softwarehersteller veröffentlichen immer wieder Korrekturen für solche Fehler. Diese Korrekturprogramme (Patches) müssen so zeitig wie möglich installiert werden, um zu verhindern, dass neue Viren oder Angriffsprogramme diese Fehler innerhalb kürzester Zeit ausnutzen.

Für einige Betriebssysteme – insbesondere für die neueren Windows-Versionen – bieten die Hersteller automatische Installationen dieser Korrekturen über das Internet an. **Nutzen Sie diesen Service und aktualisieren Sie regelmäßig Betriebssystem und Software!**

Microsoft Windows Betriebssysteme können Sie auf Aktualität prüfen unter http://update.microsoft.com (für den Aufruf ist der Internet Explorer gefordert). Dort finden Sie auch Hinweise, wie Sie die Updates automatisieren können.

Viren, Würmer, Trojanische Pferde

Die Universität Freiburg hat **Sammellizenzen für Antivirensoftware** erworben. Die entsprechende Software kann daher auf allen dienstlich genutzten Rechnern sowie auf den Rechnern aller Studierenden der Universität eingesetzt werden.

Schützen Sie sich, indem Sie dieses Angebot nutzen!

Neue Schädlinge werden fast täglich in Umlauf gesetzt. Nur ständig aktualisierte Antivirensoftware kann daher den nötigen Schutz bieten.

Halten Sie Ihre Antivirensoftware aktuell!

Die vom Freiburger Universitätsrechenzentrum lizenzierte Software sowie Beschreibungen für die Installation und Aktualisierung derselben finden Sie unter http://portal.uni-freiburg.de/rz/rat_und_hilfe/virenschutz/sophos-antivirus/. Informationen zur Installation von Sophos finden Sie unter http://portal.uni-freiburg.de/rz/rat_und_hilfe/virenschutz/sophos-installation/

Viele Viren werden über Massenmails verteilt. Gehen Sie **vorsichtig mit Mailanhängen** um! Öffnen Sie diese nur, wenn Sie sich über die Herkunft und den Inhalt im Klaren sind!

Der **Mailserver des Rechenzentrums** filtert alle mit bekannten Viren behafteten Mails aus. Nutzen Sie den Mailserver des Rechenzentrums oder einen anderen Mailserver, der Sie vor Viren schützt! Infos zum RZ-Mailserver und zum Virenschutz dort finden Sie unter: http://portal.uni-freiburg.de/rz/dienste/email

Manche Würmer dringen über von Virenscannern nicht überwachte Schnittstellen in den Rechner ein. Lassen Sie den Virenscanner daher **regelmäßig die Festplatte nach Viren durchsuchen**!

Nicht alle Internetseiten sind seriös. Wegen eines unsicher konfigurierten Browsers können Sie sich daher Trojanische Pferde und andere Schädlinge einhandeln. Viele dieser Schädlinge kann ein regelmäßiger Virenscan finden. Noch wichtiger ist, einen sicheren bzw. sicher konfigurierten Browser zu benutzen. Hinweise dazu finden Sie beispielsweise unter http://www.gwdg.de/service/sicherheit

Personal Firewall

Angreifer aus dem Internet schlagen oft schneller zu, als die Nutzer die nötigen Softwarekorrekturen (gerade bei neuen Rechnern) aus dem Netz herunter laden können. Hier – und generell als zusätzliche Verteidigungslinie – hilft ein „Personal Firewall“ genanntes Filterprogramm, das Zugriffe aus dem Netz heraus abwehrt.

Mit Windows Vista, Windows XP und Windows 2003 wird eine solche Firewall mitgeliefert. Für ältere Windows-Versionen gibt es frei verfügbare Firewalls. Auch andere Betriebssysteme bieten entsprechende Filterprogramme an.

Anleitungen und weitere Informationen zu Microsoft Produkten finden Sie unter http://www.microsoft.com/germany/sicherheit/default.mspx

Nutzen Sie die verfügbaren Firewallfunktionalitäten, um eine Grundsicherung der Rechner zu erreichen!

Private IP-Adressen

Nutzen Sie die Netzanbindungen Ihres Rechners zum E-Mail-Lesen und Internetsurfen, benötigen darüber hinaus aber keine spezielleren Internetdienste?

Für die meisten Rechner trifft das zu. Dann können auch Sie so genannte „private IP-Adressen“ für Ihren Rechner verwenden. Diese Adressen bieten den Vorteil, dass sie prinzipbedingt nicht aus dem Internet angegriffen werden können. Diese Funktion wird seit geraumer Zeit auch in Freiburg von der Netzwerk-Truppe zur Verfügung gestellt. Bitte kontaktieren Sie das Rechenzentrum über die Mail-Adresse technik@fun.uni-freiburg.de, wenn Sie Ihren Arbeitsplatzrechner auf „private IP-Adressen“ umstellen wollen.

Notebooks und mobile Rechner

Rechner, die zeitweise innerhalb und zeitweise außerhalb des Netzes der Universität Freiburg am Netz betrieben werden, haben wiederholt zu schweren Sicherheitsproblemen im Universitätsnetz geführt, weil durch solche Rechner Schädlinge „durch die Hintertür“ ins Netzwerk eingeschleppt wurden, die am Internetzugang eigentlich blockiert wurden.

Prüfen Sie Notebooks und mobile Rechner auf ihre Integrität, bevor Sie diese an das Universitätsnetz anschließen!

Eine Publikation mit Sicherheitshinweisen und nützlichen Tipps speziell für Rechner, die über VPN und WLAN ans Netz gehen, ist in Vorbereitung.

Herausgeber:
Rechenzentrum der Universität Freiburg
Hermann-Herder-Str. 10
79104 Freiburg
Leiter des Rechenzentrums: Prof. Dr. Gerhard Schneider
Redaktion Dr. Helmut Schyle

Dies ist eine an Freiburger Bedingungen angepasste Version eines Faltblatts der
Gesellschaft für wissenschaftliche
Datenverarbeitung mbH Göttingen
Am Fassberg
37077 Göttingen

Internetadresse der Göttinger Vorlage:
http://www.gwdg.de/service/sicherheit/info/faltblatt.pdf

Das Rechenzentrum der Universität Freiburg bedankt sich für die freundliche Genehmigung zur Nutzung der Göttinger Vorlage und Publikation an der Universität Freiburg.

rz

rechenzentrum
universität freiburg

Sicherheit im Netz

Sicherheitshinweise für Netzteilnehmer im Universitätsnetz Freiburg

Version: 2.0
Stand: Juli 2010