Netzwerkgruppe KaWo1 e.V.

Merkblatt zur Netzwerksicherheit

Stand: 01.12.2007

Dieses Merkblatt soll dir einen kurzen Überblick verschaffen, wie du deinen Rechner und deine Daten gegen unbefugten Zugriff und Malware (Schadprogramme) schützen solltest.

Würmer und andere Malware

Würmer sind schädliche Programme, die sich über Computernetzwerke verbreiten. Diese Programme können auf verschiedene Arten Schaden auf deinem oder auch anderen Computern anrichten. Viele Benutzer wissen leider nicht, dass ein großer Teil des Spam (unerwünschte E-Mails) von so manchem Privat-PC aus verschickt wird, ohne dass der Besitzer etwas davon wüsste. In anderen Fällen werden beispielsweise das Surfverhalten ausspioniert und/oder störende Popups erzeugt. Schlimmstenfalls kann ein Wurm sogar anderen Personen den Zugriff auf deinen Computer ermöglichen und ihn so über das Internet fernsteuerbar machen. *In vielen Fällen bemerkt der Benutzer dies nicht!*
Insbesondere ein *ungepatchtes* Windows-System kann ohne jegliche Interaktion bereits nach wenigen Minuten am Netz infiziert sein. Deshalb sind regelmäßige Sicherheitsupdates auch auf deinem PC unerlässlich.

Sicherheitsupdates

Unter Windows gibt es für die neueren Windows Versionen eine automatische Updatefunktion, die den Benutzer regelmäßig über neue Updates informiert und diese dann installiert. Diese Meldungen sollten *auf keinen Fall* ignoriert werden! Solltest du solche Meldungen über einen längeren Zeitraum vermissen, ist es ratsam, die Einstellungen zu Windows-Update in der Systemsteuerung zu überprüfen. Die Sicherheitsupdates sind für einen wirksamen Schutz vor Würmern und Hackerangriffen unerlässlich!
Außerdem gibt es für die meisten Windowsversionen sogenannte „Service Packs“, die eine Sammlung aller bis zum Erscheinungsdatum des Service Packs verfügbaren Updates darstellen, und im Falle von Service Pack 2 für Windows XP sogar erweiterte Sicherheitsfunktionen bieten. Die landläufigen „Personal Firewalls“ sind *nicht geeignet*, um Sicherheitslücken zu schließen oder deinen Rechner vor Würmern und Hackerangriffen zu schützen.
Bevor du deinen Computer ans Netz lässt, solltest du unbedingt prüfen, ob das neueste Service Pack auf deinem Computer bereits installiert ist. Ob und welches Service Pack installiert ist, kann in der Systemsteuerung unter System nachgelesen werden. Eine CD mit dem neuesten Service Pack für dein Windows kann bei der Softwareberatung ausgeliehen werden.
Für Windows 2000 ist derzeit Service Pack 4 und ein Rollup-Paket 1 mit weiteren Updates verfügbar. Für Windows XP ist Service Pack 2 aktuell und für Windows Vista gibt es bisher noch kein Service Pack.
Von der Benutzung älterer Windows Versionen raten wir dringenst ab, da Microsoft für diese keine Updates mehr herstellt.

E-Mail

Immer häufiger verbreiten sich Würmer als Anhänge in E-Mails in denen beispielsweise von einer Rechnung, einem Gewinn oder sogar einer Mahnung oder einer Anzeige die Rede ist. Aber auch durch andere Texte wird oft versucht, den Benutzer zum Öffnen des meist schädlichen E-Mail-Anhangs zu bewegen. Du solltest daher Anhänge nur dann öffnen, wenn du sie erwartet hast und sicher bist, dass sie keine Schadprogramme enthalten. Es genügt leider nicht den Absender zu kennen, da Absenderadressen leicht gefälscht werden können. *Anhänge von einem E-Mail-Programm automatisch öffnen zu lassen, ist verantwortungslos!* Häufig werden zur Infektion eines Computers auch zu niedrige Sicherheitseinstellungen oder Sicherheitslücken in der Software

ausgenutzt. Wir raten daher dringend davon ab, MS Outlook oder Outlook Express zum Lesen von E-Mails zu benutzen. Als Alternative empfehlen wir das in unserer Dokumentation beschriebene Mozilla Thunderbird (`http://www.mozilla-europe.org`).
Ein anderer Punkt sind die sogenannten Kettenbriefe, die niemals weitergeleitet werden sollten. Sie gehen oft jahrelang durch das Internet, verunsichern die Leser, kosten Zeit und sorgen in manchen Fällen sogar dafür, dass bestimmte Adressen oder Telefonnummern jahrelang mit Postkarten oder Anrufen gestört werden. Eine informative Seite zu solchen Hoaxes (Falschmeldungen) kannst du hier finden:
`http://www.tu-berlin.de/www/software/hoax.shtml`

Passwörter

Solltest du an deinem Computer kein Passwort oder ein schlechtes Passwort eingestellt haben, sei dir bewusst, dass es anderen Nutzern im Netzwerk ohne Veränderung deiner Konfiguration sehr leicht möglich ist, sich über das Netzwerk an deinem Computer anzumelden und ihn dann kontrollieren kann. Deshalb empfiehlt es sich unbedingt, *gute Passwörter* zu benutzen.
Ein gutes Passwort kennzeichnet sich durch eine Länge von mindestens acht Zeichen und enthält Sonderzeichen, Groß- und Kleinschreibung sowie Zahlen. So ist z.B. ein Name ein schlechtes Passwort, „Nd!bw4np“ wäre ein sehr starkes Passwort, und ließe sich mit folgendem Satz leicht merken: „Nach der Attacke brauchen wir vier neue Passwörter“. Passwörter sollten nicht aufgeschrieben, per E-Mail verschickt oder an den Monitor geklebt werden! Passwörter werden *niemals* an andere Personen weitergegeben, auch nicht an Administratoren.

Weitere Informationen und Ansprechpartner

Weitere Informationen findest du in der „Installationsanleitung“ und auf den Internetseiten des Vereins:
`http://www.kawo1.rwth-aachen.de/kawo1-net`.
Solltest du Fragen zur Sicherheit im Netz haben, so zögere nicht, deine Frage in der Newsgroup `kawo1.computer` zu stellen. Alternativ kannst du einen Administrator in seiner Sprechstunde aufsuchen, oder eine E-Mail an `admin@kawo1.rwth-aachen.de` schicken.