

Viren, Würmer, Trojaner, Spam: So heissen die Ungeziefer und der Müll, mit denen der Internetnutzer auf seinem Weg durch das Internet rechnen muss. Die Gefahren sind weitgehend bekannt, und auch die Massnahmen, mit welchen sich der Anwender schützen kann. Das erreichbare Mass an Sicherheit hängt aber nicht nur von den technischen Hilfsmitteln ab, sondern vor allem vom Verhalten und der Disziplin des Anwenders. SolNet gibt Ihnen Hinweise, wie Sie sich schützen können.

Mit einem Zugang zum Internet verbindet sich der Anwender an ein weltumspannendes und offenes Netz mit einer unüberschaubaren Anzahl angeschlossener Maschinen und Menschen. Darunter befinden sich zahlreiche Elemente mit mehr oder weniger kriminellen Absichten und Machenschaften. Wer sich in diesem Raum ahnungslos und ohne Vorkehrungen bewegt, wird früher oder später ein Opfer mit mehr oder weniger dramatischen Folgen. Dabei nutzen die Täter sowohl die Sicherheitslücken in weit verbreiteten Programmen, als auch die Naivität und Bequemlichkeit der Anwender. Der „Erfolg“ der Täter zeigt, dass diese Kombination tatsächlich sehr wirksam ist.

Von Viren, Würmern und anderen Schädlingen

Unter dem Begriff „Virus“ werden heute in der Umgangssprache praktisch alle Arten von Schädlingen bezeichnet. Das ist zwar nicht ganz richtig, denn ein „Virus“ ist ein Schädling mit speziellen Eigenschaften. Daneben gibt es noch andere, die wegen ihrem spezifischen Verhalten anders genannt werden, beispielsweise „Würmer“ oder „Trojanische Pferde“. Aber heute treten Schädlinge meistens als Mischformen auf, welche die verschiedenen Eigenschaften vereinen. Allen ist eines gemeinsam: Sie verbreiten sich über E-Mail in ausführbaren Attachments (der E-Mail angehängte Datei) oder beim Besuch von zweifelhaften Internetseiten.

Virus

Mit Virus bezeichnet man ein Programm, welches sich in andere Dateien einnistet und diese infiziert. Die infizierte Datei dient dabei als „Wirt“ mit dem der Virus weiterverbreitet wird.

Makro-Virus

Viele Produkte aus dem Microsoft-Office-Paket verwenden eine Makro-Sprache um Dateien zu interpretieren. Ein Makro-Virus bedient sich dieser Sprache und führt einen Code aus und infiziert damit möglicherweise andere Dateien. Am häufigsten sind Excel-Tabellen und Word-Dokumente betroffen.

Wurm

Würmer benötigen im Unterschied zu Viren keinen Wirt um sich zu verbreiten. Es sind eigenständige Programme, die sich auf andere Rechner kopieren können. Der übliche Verbreitungsweg für Würmer sind E-Mails: Als Attachment verschicken sich die Würmer selber an E-Mail-Adressen, welche sie auf dem infizierten Rechner vorfinden. Auch der Absender wird von diesem Rechner genommen. Zur Aktivierung eines Wurms muss der Anwender in der Regel das Attachment ausführen. Einige Würmer benutzen Sicherheitslücken von E-Mail Programmen, um bereits beim Betrachten der E-Mail aktiv zu werden.

Trojanisches Pferd

So nennt man ein Programm, das dem Anwender eine nützliche Anwendung vorgaukelt. Tatsächlich verbirgt sich dahinter ein gefährlicher Schädling. Diese Programme nisten sich vom Anwender oft unbemerkt im System ein und ermöglichen die Kontrolle des Rechners von aussen. So ist es für Angreifer möglich, Dateien zu lesen und zu Informationen zu gelangen, die der Anwender eigentlich lieber für sich behalten möchte.

Spam

Spam werden E-Mails genannt, welche in Massen verschickt werden. Es handelt sich meistens um unerwünschte Werbemails. Experten gehen davon aus, dass bereits mehr als die Hälfte der E-Mails Spam sind. Dieser „Werbemüll“ fügt in der Regel keinen direkten Schaden an, verstopfen aber das Netz und kosten den Anwender Speicherplatz und viel Zeit für das Aussortieren und anschließende Löschen. Es gibt aber auch Botschaften, welche den Anwender zum Besuch einer Webseite auffordern, auf welcher schlussendlich die Gefahr eines Schädling lauert.

Die technischen Hilfsmittel

Vor den genannten Gefahren und Unannehmlichkeiten des Internets kann man sich schützen. Es gibt zahlreiche mehr oder weniger wirksame Mittel gegen Ungeziefer und Müll. Allen gemeinsam ist, dass sie für den Benutzer mit zusätzlichem Aufwand verbunden sind und von ihm ein konsequentes Handeln verlangen.

Neueste Software Versionen benutzen

Installieren Sie grundsätzlich immer die aktuellste Version von Betriebssystem, Browser und E-Mail-Programm. Die Hersteller bieten in der Regel die neuesten Updates auf dem Web zum kostenlosen Download an. Sie sollten diese sofort nach Bekanntgabe installieren. Und damit Sie diese Arbeit nicht vergessen: Windows XP kann so konfiguriert werden, dass es regelmässig und automatisch nach entsprechenden Updates sucht und den Anwender auffordert, diese zu installieren.

Alternative Produkte einsetzen

Microsoft hat einen überwältigenden Marktanteil an PC-Betriebssystemen und Applikationen. Es ist daher kein Wunder, wenn sich Übeltäter jeglicher Art auf diese Produkte konzentrieren. Die zahlreichen Sicherheitslücken von Microsoft-Produkten machen es ihnen auch relativ einfach. Zudem sind Internet Explorer und Outlook eng mit dem Betriebssystem und weiteren Applikationen verknüpft. Das bringt dem Anwender zwar einen aussergewöhnlichen Bedienungskomfort, erhöht aber gleichzeitig die Gefahr, dass vorhandene Sicherheitslöcher sehr effizient ausgenutzt werden können.

Wer also aus dem Schussfeld der Täter treten will, kann sich nach einem alternativen Produkte für Browser und E-Mail-Programm umsehen. Viele gute Programme stehen kostenlos zum Download im Internet bereit.

Mozilla (Browser und E-Mail)	www.mozilla.org
Firefox (Browser)	www.mozilla.org
Opera (Browser)	www.opera.com
Thunderbird (E-Mail Client)	www.mozilla.org

Virenschutz

Die E-Mail-Boxen von SolNet verfügen über einen Virenschutz. Trotzdem empfehlen wir die Installation eines aktuellen Virenschanners auf jeden Rechner. Diese Programme untersuchen die PC-Laufwerke und E-Mails nach Schädlingen. Wird ein Schädling identifiziert unterstützen diese Programme den Anwender beim Entfernen.

AntiVir	www.antivir.de
Norton Antivirus	www.symantec.com
McAfee	de.mcafee.com

NAT-Router statt Modem

Wer seinen PC über einen NAT-Router mit ADSL verbindet, ist vor Zugriffen von aussen geschützt. Der Rechner hat nämlich eine interne IP-Adresse, die ihn von aussen nicht ansprechbar machen. Diese Geräte sind in der Regel etwas teurer als ein einfaches USB-Modem.

Firewall

Eine Firewall erlaubt, den Rechner für den Zugriff von aussen abzuschotten. So lassen sich Dienste (Ports), die nicht zwingend gebraucht werden, und eine potenzielle Gefahr darstellen können, blockieren. Die Installation einer Firewall schützt auch vor den Gefahren von innen. Erkennt ein Virens Scanner einen Trojaner nicht, dann kann eine Firewall die Infektion zwar nicht verhindern. Sie kann aber unterbinden, dass der Trojaner Verbindungen in das Internet aufbaut oder eine Hintertür im System für den Zugriff vom Internet öffnet.

Mit Windows XP wird eine Firewall ausgeliefert. Der Anwender muss diese nur aktivieren. Im Internet gibt es auch zahlreiche Produkte, welche für den kostenlosen Download bereitstehen.

Kerio Personal Firewall	www.kerio.com
Outpost Personal Firewall	www.agnitum.com
Sygate Personal Firewall	www.soho.sygate.com
Zone Alarm	www.zonelabs.com

Wer den Aufwand für die Installation, Konfiguration und andauernde Pflege einer eigenen Firewall scheut, kann den optionalen SolNet Firewall Service abonnieren.

Spam-Filter

Solche Filter erkennen typische Merkmale von unerwünschten E-Mails. Gute Produkte verwenden einen effektiven und selbstlernenden Filter. Bei korrekter Einstellung hilft ein solcher Filter, den grössten Teil der unerwünschten E-Mails zu erkennen und zu löschen. SolNet hat auf seinen E-Mail-Servern einen solchen Spamfilter installiert. Diese stehen allen Kunden kostenlos zur Verfügung. Es gibt auch Mail-Programme, welche Spamfilter bereits mitbringen. Der kostenlose E-Mail-Client von Mozilla oder Thunderbird haben selbstlernende und effektive Filter dabei.

Mozilla (Browser und E-Mail)	www.mozilla.org
Thunderbird (E-Mail-Client)	www.mozilla.org

Der Faktor Mensch

Die Benutzung von Produkten mit bekannten Sicherheitslöcher, ein Virens Scanner, der nur Schädlinge vom letzten Jahr kennt, eine falsch konfigurierte Firewall oder der unkritische Umgang mit Attachments in E-Mails von unbekanntem Absendern: In einer solchen Umgebung fühlen sich die Schädlinge so richtig wohl.

Als Internetnutzer müssen Sie das Thema Sicherheit selbst in die Hand nehmen. Die Kombination von technischen Hilfsmitteln, das Befolgen von ein paar Regeln und der Einsatz des gesunden Menschenverstandes schützen Sie weitgehend vor den Gefahren des Internets. Dazu gehört auch Ihr eigenes Verhalten, dass sich beim Surfen und der Benutzung von E-Mail durch eine gewisse Vorsicht und Zurückhaltung äussern sollte. **Schlussendlich bestimmt der Anwender den erzielbaren Grad an Sicherheit.**

Einen 100%-igen Schutz gibt es auch bei richtigem Verhalten nicht. Durch weitere Massnahmen wie regelmässiges Sichern Ihrer Daten kann ein möglicher Schaden des verbleibenden Risikos noch einmal begrenzt werden.

Informieren Sie sich auch regelmässig über die aktuelle Gefahrenlage. Inzwischen sind die Auswirkungen von Schädlingen so gross, dass deren Auftauchen und Verbreitung in den Medien ein Thema sind. Beachten Sie solche Meldungen aus Presse, Fernsehen und Radio. Auch Fachzeitschriften informieren regelmässig zum Thema Sicherheit. Im Internet finden Sie weitere nützliche Informationen, insbesondere auch auf den Seiten von Firmen, welche Anti-Viren-Software anbieten.

Norton Antivirus	www.symantec.com
McAfee	de.mcafee.com
Technische Universität Berlin	www.tu-berlin.de/www/software/virus/aktuell.shtml
Heise-Verlag	www.heise.de