Sicherheit im Internet

Vor einiger Zeit führte der »ILoveYou«-Virus mit Hilfe des Microsoft E-Mail-Programms Outlook weltweit zum Zusammenbruch von Millionen von Rechnern und beeinträchtigte vor allem den E-Mail-Verkehr. Täglich erscheinen Meldungen über neue Viren und Sicherheitslücken. Da aber nur selten über verursachte Schäden berichtet wird, scheint der gewöhnliche Endanwender mit dem Satz »Ich bin drin« nur all zu oft zu vergessen, dass mit der Internetverbindung der eigene Rechner auch Angriffen aus dem Internet ausgesetzt ist. Das Internet ist keine Einbahnstraße. Daten verlassen den Computer, und Daten werden auf den Rechner heruntergeladen. Wenn dieser Datenaustausch ungewollt passiert, ist das mehr als ärgerlich. Ausspionierte Zugangsdaten für den Online-Account werden missbraucht, um auf fremde Rechnung kostenlos zu surfen. Sogenannte Trojaner (Programm, das neben seiner eigentlichen Funktion, die dem Anwender bekannt ist, noch weitere Funktionen ausführt, von denen der Anwender nichts weiß und deren Ausführung er im Regelfall auch nicht bemerkt, beispielsweise das Verschicken von Passwörtern via E-Mail ins Internet) wählen ohne Kenntnis des PC-Users teure 0190-Nummern und verursachen auf diese Weise finanzielle Schäden. Für viele Sicherheitslücken gibt es Lösungen, und so ziemlich jeder Virus lässt sich durch entsprechende Antivirenprogramme vom Rechner verbannen. Leider bemerken die Betroffenen zu selten, dass der heimische Rechner Unbefugten Zutritt gewährt oder Viren ihr unsägliches Spiel im Hintergrund treiben. Richtig ist aber auch, dass nicht jeder Virus die Festplatte formatiert und jede Sicherheitslücke zu folgenreichen Angriffen führt.

Dennoch geht der Download von Software von unsicheren Quellen aus dem Netz zu leicht von der Hand. Indes wird nicht beachtet, dass jedes ausführbare Programm vollen Zugriff auf den eigenen Rechner genießt und Hintertüren öffnen kann. Viel zu oft werden Word-Dateien arglos geöffnet, auch wenn sie als E-Mail-Attachment von unbekannten Absendern stammen. Dabei gehen seit geraumer Zeit die meisten Virusinfektionen auf Word-Makros zurück. Dieser unbekümmerte Umgang führte im letzten Jahr zur massenhaften Verbreitung des Word-Makro-Virus »Melissa«. Nur die wenigsten Anwender benötigen Makros, dennoch sind sie aktiviert.

Wer aber vor Angriffen aus dem Internet gleich schwere Geschütze wie eine Personal Firewall (Programm, das den ein- und ausgehenden Datenverkehr zum Internet überwacht und unerwünschte Verbindungen verhindert) einsetzt, tut den zweiten Schritt vor dem ersten. Zunächst einmal sollten das vorhandene Betriebssystem und die installierten Anwendungen im Rahmen ihrer Möglichkeiten konfiguriert werden.

Einen umfassenden Schutz beim Surfen im Internet kann man sicherlich nicht erreichen, aber mit den nachfolgenden Tipps ist der nächste Webausflug von weniger Risiken für den eigenen Rechner begleitet.

Gerade der Internet-Browser und das E-Mail-Programm sind zumeist nach der Installation betriebsbereit und gewähren unproblematischen Zugang zum Internet. Dies verleitet zum sofortigen Lossurfen, wenngleich die von den Programmen voreingestellten Standardkonfigurationen bedenklich offen gegenüber Angriffen aus dem Internet sind. Beim Internet-Browser sollte die Sicherheitsstufe so hoch wie möglich eingestellt werden. Insbesondere sollten aktive Inhalte (Daten, die beim Empfänger aktiv Veränderungen am Zustand des Rechners vornehmen können) wie ActiveX, JAVA und Javascript deaktiviert werden. Diese Inhalte ermöglichen es, dass Angreifer beispielsweise Nutzerkennungen und Passwörter oder auch lokal gespeicherte Daten des Internet-Nutzers ausspionieren können. Der weitaus größte Teil dieser aktiven Inhalte dient meistens nur für optische Spielereien, wie dem Einblenden von Werbebannern. Allerdings sind zahlreiche Seiten ohne die aktiven Inhalte nur noch eingeschränkt darstellbar, so dass der sicherheitsbewusste Internet-Nutzer von vielen Angeboten ausgesperrt wird und für ihn das Surfvergnügen geschmälert wird. Höhere Sicherheit bedeutet hier, Einbußen am Komfort hinzunehmen. Es sollte gerade für das Betriebssystem sowie für den Internet-Browser und das eingesetzte E-Mail-Programm regelmäßig nach sicherheitsrelevanten Updates geschaut werden.

Viele Benutzer haben unzählige Hintergrundanwendungen auf dem eigenen Rechner zu laufen – Augen, die dem Mauszeiger folgen, Programme, die im eingestellten Zeittakt das Hintergrundbild auswechseln. Alle schön anzusehen, aber wenig wirkungsvoll gegenüber Spionen im Netz. Effektvoll und meist weniger rechenintensiv sind speicherresidente Antiviren-Programme, die bei bekannten Viren Alarm schlagen. Diese sollten mindestens einmal monatlich auf den aktuellen Stand gebracht werden, da die Entwicklung neuer Viren genau so rasant voranschreitet wie die Computertechnik selbst. Viele Antiviren-Programme bieten dafür eine bequeme Update-Funktion an.

Bereits im BIOS des Computers lassen sich wirksame Einstellungen vornehmen. Dazu gehört zum einen, dass die Bootreihenfolge der Laufwerke auf C:, A: gestellt wird. So wird beim Start des Computers verhindert, dass Viren auf einer Diskette aktiviert werden. Zum anderen ist der Viren-Schutz des BIOS selbst zu aktivieren.

Grundsätzlich gilt, nur das zu installieren, was wirklich gebraucht wird. Jedes ungenutzte Programm und jede unnötige Funktion vergrößert die Gefahr eines unberechtigten Zugriffs auf die heimische Festplatte. Wer die Möglichkeit besitzt, Software erst auf einem nicht vernetzten älteren Rechner auszuprobieren, sollte dies tun. Bei dauerhaft genutzten Anwendungen sollten nur diejenigen Funktionen aktiviert sein, die auch benötigt werden. In den Officeanwendungen wie WORD, EXCEL oder POWERPOINT ist der Makro-Viren-Schutz zu aktivieren.

Eingehende E-Mails sind das größte Einfalltor für Computerviren. Der Angreifer kann sein Ziel direkt anwählen und muss nicht warten, bis der Internetnutzer eine bestimmte Seite anwählt und ein bestimmtes Programm herunterlädt, wie es die meisten Attacken über das Internet erfordern. Ferner lässt sich die Absenderadresse unproblematisch fälschen, so dass der Absender der E-Mail fast unmöglich identifiziert werden kann. Zum besseren Schutz sollten daher offensichtlich unsinnige E-Mails ungelesen in den Papierkorb wandern. Bei vermeintlich bekannten oder vertrauenswürdigen Absendern sollten E-Mail-Attachments vor dem Öffnen auf Viren überprüft werden. Sicherer ist die Kommunikation via E-Mail mit Verschlüsselungsprogrammen wie dem bekannten PGP (www.pgp.com). Auf diese Weise lässt sich die Herkunft der elektronischen Post überprüfen. Zudem können gesendete Nachrichten nicht von anderen Personen als dem beabsichtigten Empfänger abgefangen und gelesen werden.

Neben E-Mails ist ein weiterer Hauptverbreitungsweg von Computerviren der Abruf von Daten und Programmen aus dem Internet. Programme sollten nur von vertrauenswürdigen Seiten heruntergeladen werden, also insbesondere von den Originalseiten des Erstellers. Anonyme Webspace-Provider, die jeder Privatperson Speicherplatz zur Verfügung stellen, sollten unbedingt als Quelle gemieden werden. Heruntergeladene Programme sollten vor ihrer Installation auf Viren überprüft werden. Achtlosigkeit beim Umgang mit E-Mail-Attachments und Programmen aus dem Netz führte auch zur Verbreitung des wohl bekanntesten trojanischen Pferdes »Back Orifice«. Dieses Programm erlaubt es durch die Hintertür, den heimischen Rechner komplett auszuforschen. Der Angreifer erhält einen be-

quemen und vollständigen Zugriff, als säße er selbst an unserer Tastatur.

Fazit: Wer mit einem gesunden Maß an Zurückhaltung und Misstrauen in die Welt des Internet eintaucht und nicht jedes x-beliebige Programm auf seinem Rechner startet, der bietet Einbrechern aus dem Internet nur eine geringe Chance, den eigenen Computer zu sabotieren oder auszuspionieren. Falsch wäre es auch, sich allein auf die Technik zu verlassen. Jeder neue Virus kann auch von einem Anti-Viren-Programm anfangs nicht erkannt werden. Passiert doch einmal der Gau und wichtige Daten sind verloren, so ist es immer sinnvoll, alle notwendigen Dateien regelmäßig gesichert zu haben, um sie im Ernstfall wiederherstellen zu können.

stud. iur. André Felgentreu
Andre@Felgentreu.de