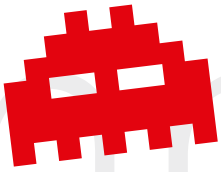
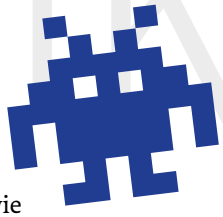
IT+Technik





Viren, **Malware** & Co.

Viren, Trojaner, Dial-In Programme, Botnetze – alles dies wird unter dem Begriff „Malware“ (zu deutsch: **Schadprogramme**) verstanden. Was es damit auf sich hat und wie man sich schützen kann, erfahren Sie hier.

Christian Kierdorf
IT-Sicherheitsbeauftragter Deutscher Hausärzteverband

Schnell ist es passiert und man hat sich ein Schadprogramm eingefangen – sei es durch einen eingelegten Datenträger, den geöffneten Anhang einer E-Mail oder den Aufruf einer Internetseite. Aber was ist ein Schadprogramm und woher kommt es? Vielleicht sagt Ihnen der „Michelangelo“-Virus noch etwas, Anfang der 90er Jahre.? Er hat die Festplatte damals so manipuliert, dass wichtige Informationen für das Betriebssystem nicht mehr auffindbar waren. Ein wirtschaftlicher Zweck wurde damals nicht verfolgt, trotzdem entstand bei den Betroffenen ein Schaden. Mittlerweile hat sich die Motivation derjenigen geändert, die Schadprogramme herstellen.

Informationsquellen und Hilfsmittel

Wenn Sie sich pro-aktiv informieren wollen, hilft Ihnen zum Beispiel die Seite des „AV-Test“-Instituts weiter (**www.av-test.org**). Das unabhängige Institut liefert hilfreiche Empfehlungen für die Auswahl von geeigneten Programmen gegen Schadprogramme.
Mit aktuellen Hinweisen rund um Sicherheit und aktuelle Bedrohungen versorgt Sie das Bürger-CERT des BSI (**www.buerger-cert.de**).
Vermuten Sie eine bösartige Datei auf Ihrem System, haben Sie unter **www.virustotal.com** die Möglichkeit, diese mit der Mehrzahl der derzeit verfügbaren Anti-Malware-Lösungen in der jeweils aktuellen Fassung prüfen zu lassen.
Liegt ein Befall vor, helfen womöglich die Tipps und Tricks von **www.botfrei.de**, um die Schadsoftware zu entfernen oder zumindest wichtige Daten zu sichern.

Die Malware blockiert die Nutzung des Systems und erpresst für die angebliche Freischaltung Geld – Sie sind gut beraten, das Geld nicht zu zahlen, denn eine Freischaltung erfolgt selbstverständlich nicht.

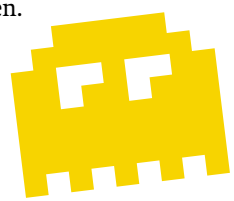
Andere Programme erlauben zwar weiterhin die Nutzung, die Angreifer nutzen jedoch die Kapazitäten des Rechners sowie des Netzwerks für eigene Zwecke – z. B. als sogenannte „Zombies“ von Botnetzen, mit denen dann Angriffe auf die IT-Infrastruktur von Unternehmen oder Regierungseinrichtungen durchgeführt werden.

Banking-Trojaner wie zum Beispiel „Zeus“ dienen dem Ziel, bestehende Sicherheitsmaßnahmen von Banken zu umgehen und so Zahlungsströme umzuleiten.

Für alle diese Gefahren bieten eine Vielzahl von Herstellern Programme – oftmals als „Security Suite“ deklariert – an, die genau so vielfältig aufgestellt sind wie die Bedrohungen, gegen die sie schützen sollen. Sie prüfen ein- und ausgehende E-Mails, bewerten die Reputation aufgerufener Internetadressen und suchen in ausführbaren Dateien nach gefährlichen Routinen.

Für den privaten Endkunden gibt es von einigen Anbietern auch kostenfreie Lösungen, die in der Regel aber im Funktionsumfang beschnitten sind oder mit Werbung für den Kauf der kostenpflichtigen Version werben. Hier sollten Sie abwägen und vor dem Einsatz solcher Versionen in der Praxis die Lizenzbedingungen hinsichtlich des gewerblichen Einsatzes prüfen.

Aber ein gutes Anti-Malware-Programm schützt nicht gegen alle Bedrohungen. Regelmäßige Updates von Betriebssystem und Anwendungen sind ebenso wichtig wie die regelmäßige Sicherung der Dateien – und ein aufmerksamer Umgang mit E-Mails und Internetseiten.



Illustrationen:fotolia