

IT-Sicherheitstipp: Hilfe beim Virenbefall

Es ist der Albtraum eines jeden Computernutzers: Man sitzt vor dem Bildschirm und merkt wie die Kontrolle über Vorgänge verloren geht. Anzeichen dafür können zum Beispiel ein verlangsamter Rechner, Computerabstürze, ungewollt gestartete Programme oder verdächtige Nachrichten auf dem Bildschirm sein. Es besteht dann der Verdacht, dass der Rechner mit Schadsoftware infiziert ist. Als Nutzer ist man in einer solchen Situation meist verunsichert und der PC ist zunächst nicht mehr zu gebrauchen.



Man fragt sich, wie man den Schaden begrenzen kann und das Gerät und die eigenen Daten wieder für den sicheren Betrieb bereit macht. Wie verhalten Sie sich, wenn Sie einen Hacker-Angriff vermuten? Folgende Hinweise aus dem Netzwerk Elektronischer Geschäftsverkehr [1] sollen Ihnen helfen, Licht ins Dunkel zu bringen.

► Erste Hilfe bei dem Verdacht einer Infektion

Wenn Sie den Verdacht hegen, dass Ihr PC mit Schadsoftware infiziert sein könnte, kommt es auf **schnelles, aber besonnenes Handeln** an. Sie sollten zunächst ruhig bleiben und Ihre Arbeit zügig am Computer beenden. Schließen Sie, sofern es möglich ist, alle Programme ordnungsgemäß, und schalten Sie den Computer aus. Schalten Sie Ihren Router bzw. das DSL-Modem ebenfalls aus, sodass keine Verbindung mit dem Internet mehr besteht.

► Selbst herausfinden, ob der PC infiziert ist

Es gibt verschiedene Möglichkeiten um herauszufinden, ob man Opfer von Schadsoftware geworden ist. Sofern sich der PC fehlerfrei hochfahren lässt und Programme noch gestartet werden können, sollten Sie eine **vollständige Systemüberprüfung** mittels einer Antiviren-Software durchführen. Dies ist wichtig, um den PC auf Viren und ähnliche Schädlinge zu durchleuchten. Aktualisieren Sie vor der Prüfung Ihre Antiviren-Software, denn nur wenn Sie die aktuellen Virendefinitionen benutzen, kann auch auf neu erkannte Viren geprüft werden. Für den Privat-

gebrauch gibt es kostenfreie Antiviren-Programme, wie AntiVir Personal oder AVG Free Antivirus, die den notwendigen Standard-Schutz abdecken.

Professionelle Programme und die Premium-Versionen der Freeware eignen sich sowohl für den Privathaushalt, als auch für Unternehmen. Sie verfügen über den üblichen Schutz und haben noch einige Zusatz-Anwendungen, wie eine Personal Firewall, die ein- und ausgehende Verbindungen überwacht. Einige Versionen verfügen auch über so genannte WebGuards, die Downloads überwachen oder Zusatzprogrammen zur Abwehr von Phishing-Angriffen oder zur Wiederherstellung von Daten.

► **Vorhandene Viren und Schädlinge entfernen**

Stellt sich bei der Systemüberprüfung heraus, dass der Computer infiziert ist, müssen die Schädlinge entfernt werden. Häufig macht die Antiviren-Software einen Vorschlag zum Umgang mit den Schädlingen oder entfernt diese automatisch. Kann man die betroffenen Daten nicht löschen, bieten die **Suchdatenbanken der Hersteller der Antiviren-Software** häufig Abhilfe. Unter Angabe der Bezeichnung des Schadprogrammes kann man in der Programmoberfläche oder auf der Website des Herstellers weitere Informationen und Handlungsempfehlungen erhalten. Eine Alternative dazu bietet das kostenlose Programm Hijackthis [1]. Hijackthis erstellt eine Liste der laufenden Anwendungen auf dem System und speichert diese in einer Textdatei, einer so genannten Log-Datei, ab. Auf der Homepage von Hijackthis kann die Log-Datei ausgewertet werden. Dabei werden die in der Textdatei genannten Prozesse auf Seriosität überprüft. Weichen Sie von seriösen Anwendungen ab, empfiehlt Hijackthis, wie weiter vorgegangen werden sollte.

► **In anderem Modus hochfahren und Daten retten**

Sollte sich der Computer im normalen Modus nicht mehr hochfahren lassen oder nach kurzer Zeit abstürzen, sind Ihre Dateien wahrscheinlich noch nicht verloren. Sie sollten zuerst versuchen, Ihren PC im **abgesicherten Modus** zu starten. Den abgesicherten Modus aktivieren Sie, indem Sie beim Hochfahren des Geräts eine bestimmte Taste, häufig F8, mehrmals hintereinander drücken, bis ein Bildschirm erscheint, der Sie den Modus auswählen lässt. Sofern der PC startet, lädt er nur die nötigsten Programme, sodass Sie in der Regel eine Systemüberprüfung durch Ihr aktuelles Antiviren-Programm ausführen können.

Sollten Sie auch im abgesicherten Modus nicht weiterkommen, so ist es ratsam, ein **mobiles Betriebssystem**, wie Knoppix oder Kanotix, herunterzuladen, auf eine CD zu brennen und von dieser CD zu starten, auch booten genannt. Standardmäßig bootet der Computer vom CD-ROM Laufwerk. Ist das einmal nicht der Fall, müssen Sie beim Hochfahren das so genannte BIOS starten (meistens mit der Taste F2 oder ENTF – siehe dazu Informationen auf dem Bildschirm beim Hochfahren), um einzustellen, dass Sie bevorzugt vom CD-ROM Laufwerk booten möchten.

Sichern Sie nach der Überprüfung auf Schädlinge Ihre ungesicherten Daten auf einem externen Datenspeicher. Bevor Sie die Daten auf einen anderen Rechner übertragen, prüfen Sie diese nochmals mit einem Antivirenprogramm. Um sich umständliche Datensicherungen bei einem Virenbefall zu ersparen, sollten Sie **regelmäßig Datensicherungen anfertigen**. Weitere Tipps dazu finden Sie in dem bereits veröffentlichtem IT-Sicherheitstipp „Sicheres Speichern und Löschen Ihrer Daten“ [2].

► Einen Computerexperten zurate ziehen

Scheuen Sie sich nicht, bei einem Sicherheitsvorfall im Privatbereich einen vertrauenswürdigen Computerexperten einzuschalten, sofern Sie selbst wenig oder keine Erfahrung beim Umgang mit Schadprogrammen haben. Ein Experte nimmt sich des Problems an und wird es meist schnell lösen. Überlegen Sie sich, wie Sie bei einem Sicherheitsvorfall an Ihrem Auto vorgehen würden. Bei einem Sicherheitsvorfall im Unternehmen sollten Sie sich umgehend an den Administrator des Systems und an den IT-Sicherheitsbeauftragten wenden, ohne eigene Schritte zu unternehmen.

Das Bundesamt für Sicherheit in der Informationstechnik empfiehlt, dass jedes Unternehmen, welches seinen Geschäftsprozess auf IT aufbaut, einen **IT-Sicherheitsbeauftragten** für die eigene Informationssicherheit benennt. Weitere Informationen erfahren Sie auf den Webseiten des BSI [3].

► Nach einer vollständigen Überprüfung wieder betriebsbereit machen

Nach der erfolgreichen Bereinigung von Viren, sollte(n) die Festplatte(n) und alle Datenträger erneut vollständig überprüft werden. Durch diese Prüfung besteht eine höhere Wahrscheinlichkeit, alle Schädlinge entfernt zu haben. Um auf Nummer sicher zu gehen, sollten Sie nach einem Virenbefall jedoch Ihr **gesamtes System neu installieren**. Sie können nämlich nicht wissen, was der Schädling alles unternommen hat, als Ihr Rechner nicht ausreichend geschützt war. Gegebenenfalls hat er weiterer Schadsoftware einfach nur die Tür geöffnet. Wochen später kann diese Sicherheitslücke ausgenutzt werden, da das Antivirenprogramm ausschließlich Schadsoftware beseitigt aber keine entstandenen Sicherheitslücken erkennen und schließen kann.

Spätestens nach einem Virenbefall ist es der richtige Zeitpunkt, um für alle schützenswerten Logins **neue, sichere Passwörter** zu vergeben. Vergeben Sie ein Passwort nicht mehrfach und nutzen Sie zur Verwaltung aller Passwörter einen Passwort-Manager. Weitere Informationen dazu finden Sie in unserem bereits erschienenen IT-Sicherheitstipp „Wie erstelle ich ein sicheres Passwort“ [2].

► Hacker-Angriffe der Polizei melden

Wenn Sie merken, dass Sie Opfer von **Wirtschaftsspionage** geworden sind, kappen Sie umgehend Ihre Internetverbindung. Melden Sie den Vorfall bei der Polizei. Sollte sich der Tatverdacht

verdichten, so sollten Sie bei der Polizei Anzeige erstatten. Möglicherweise müssen Sie Ihren Rechner komplett zur Verfügung stellen.

► **Durch Sicherheitsupdates und bewusstes Surfen besser schützen**

Halten Sie Ihre Rechner immer auf dem neuesten Stand. Laden Sie **regelmäßig Updates** des Betriebssystems herunter. Auch alle Programme, mit denen sie im Internet arbeiten, müssen ständig aktualisiert werden, einem Trend zufolge werden diese für Angreifer deutlich interessanter. Während in der Vergangenheit Sicherheitslücken in Betriebssystemen und Browsern eine sehr häufige Infektionsursache waren, konzentrieren sich viele Angreifer nun auf Zusatzsoftware für Browseranwendungen. Immer **mehr Malware für Anwendungen von Drittherstellern**, wie dem Adobe Reader, Flash-Plugins und Java werden in Umlauf gebracht. Der beste Schutz ist es, immer über aktuelle Sicherheitslücken informiert zu sein und sich bewusst im Internet zu bewegen. Einen hilfreicher Service sind die so genannten **securityNews** vom Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen. Melden Sie sich dazu einfach bei dem Online-Portal der Marktplatz IT-Sicherheit an und erhalten Sie automatisch eine E-Mail mit Hinweisen und Handlungsempfehlungen beim Erscheinen aktueller Sicherheitsupdates.

Autoren

Mark Thiel, FH Gelsenkirchen, Institut für Internet-Sicherheit

Dipl.-Inform.(FH) Sebastian Spooren, FH Gelsenkirchen, Institut für Internet-Sicherheit

B.Sc. Deborah Busch, FH Gelsenkirchen, Institut für Internet-Sicherheit

Prof. Dr. (TU NN) Norbert Pohlmann, FH Gelsenkirchen, Institut für Internet-Sicherheit

Bildquelle: © Spectral-Design - Fotolia.com

Weiterführende Informationen

[1] <http://www.ec-net.de>

[2] <http://www.hijackthis.de>

[3] <https://www.it-sicherheit.de>

[4] <http://www.bsi.bund.de>

Fachhochschule Gelsenkirchen, Institut für Internet-Sicherheit - if(is)

Das Institut für Internet-Sicherheit ist eine fachbereichsübergreifende wissenschaftliche Einrichtung der Fachhochschule Gelsenkirchen. Es forscht und entwickelt auf Basis innovativer Konzepte im Bereich der Internet-Sicherheit. 2005 gegründet, hat es sich unter der Leitung von Prof. Dr. (TU

NN) Norbert Pohlmann und in enger Zusammenarbeit mit der Wirtschaft innerhalb kurzer Zeit einen Ruf als eine der führenden deutschen Forschungsinstitutionen der IT-Sicherheit gemacht. Weitere Informationen finden Sie unter: <http://www.internet-sicherheit.de>

Das Netzwerk Elektronischer Geschäftsverkehr

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr, in 29 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business Lösungen. In dieser Zeit hat sich das Netzwerk mit über 30.000 Veranstaltungen und Einzelberatungen mit über 300.000 Teilnehmern als unabhängiger und unparteilicher Lotse für das Themengebiet „E-Business in Mittelstand und Handwerk“ etabliert. Das Netzwerk stellt auch Informationen in Form von Handlungsanleitungen, Studien und Leitfäden zur Verfügung, die auf dem zentralen Auftritt www.ec-net.de heruntergeladen werden können. Die Arbeit des Netzwerks wird durch das Bundesministerium für Wirtschaft und Technologie gefördert.

Sichere E-Geschäftsprozesse in KMU und Handwerk

Die Checkliste IT-Sicherheit wurde im Rahmen des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerks Elektronischer Geschäftsverkehr (NEG) erstellt. Das Verbundprojekt wird vom Bundesministerium für Wirtschaft und Technologie (BMWi) unterstützt und soll helfen, in kleinen und mittleren Unternehmen mit verträglichem Aufwand die Sicherheitskultur zu verbessern. Hier werden insbesondere kleine und mittelständische Unternehmen sowie das Handwerk zu wichtigen Aspekten der Informationssicherheit sensibilisiert und praxisnah informiert. Alle Details finden Sie unter: <http://www.kmu-sicherheit.de>