Gnadenloser Türsteher

In wenigen Minuten zerstört ein Konkurrent den Firmenserver und verschafft sich dadurch die bessere Position am Markt – oder liest unbemerkt sensible Daten. Mythos und Wahrheit über Angriffe auf Netzwerke. Und wie sich Unternehmen effektiv schützen.

Die IT-Verantwortlichen eines Unternehmens schlafen schlecht. Fast täglich tauchen neue Sicherheitslücken auf, die unberechtigten Personen die Kontrolle über fremde Computer verschaffen. Die allgemeine Haltung lautet: „Wir haben Vorkehrungen getroffen. Es gibt eine Firewall, es gibt Virenscanner, die regelmäßig aktualisiert werden. Und außerdem: Man hört so selten, dass mal jemand Opfer eines Angriffs geworden ist, das ist doch alles nur Panikmache. Und was sollten wir schon groß tun? Absolute Sicherheit gibt es ohnehin nicht.“ Sind die Warnungen der Sicherheitsexperten wirklich nur Panikmache? Durch Angriffe auf Firmennetzwerke kleinerer und mittelständischer Unternehmen wurde in der europäischen Wirtschaft in 2003 ein Schaden von 22 Milliarden Euro verursacht*. Natürlich werden eher selten konkrete Fälle bekannt. Wer gibt schon gerne zu, dass er sich nicht ausreichend um die Sicherheit seines Netzwerkes gekümmert hat. Es gibt noch zu viel Unsicherheit bei vielen Unternehmen in Sachen Sicherheit. Zu viele Halbwahrheiten kursieren. Wie die Daten effektiv geschützt werden, bleibt dagegen Expertenwissen.

Halbwahrheiten

Mythos Firewall: Entgegen dem weit verbreiteten Irrglauben, eine Firewall würde alle Gefahren abwehren, schützt sie in Wirklichkeit nur vor einem gewissen Anteil der Gefahren. Eine Firewall ist zwar unverzichtbar. Sie ist aber nur ein Teil eines Sicherheitskonzeptes. Mythos Virenscanner: Auch ein Virenscanner erkennt nur einen Teil der Schadenssoftware. Neue und vor allem individuell angefertigte Schadenssoftware können Virenscanner dagegen prinzipbedingt nicht entdecken. Es gibt inzwischen sogar kommerziell arbeitende Firmen, die gegen Bezahlung einen Trojaner erstellen, der garantiert von Virenscannern „entdeckt“ wird. Aber auch ohne die Hilfe von Anbietern fragwürdiger Dienstleistungen ist es recht einfach, bestehende Trojaner zu modifizieren und gegen die Erkennung von Virenscannern zu manipulieren. Einschlägige Anleitungen gibt es im Internet.

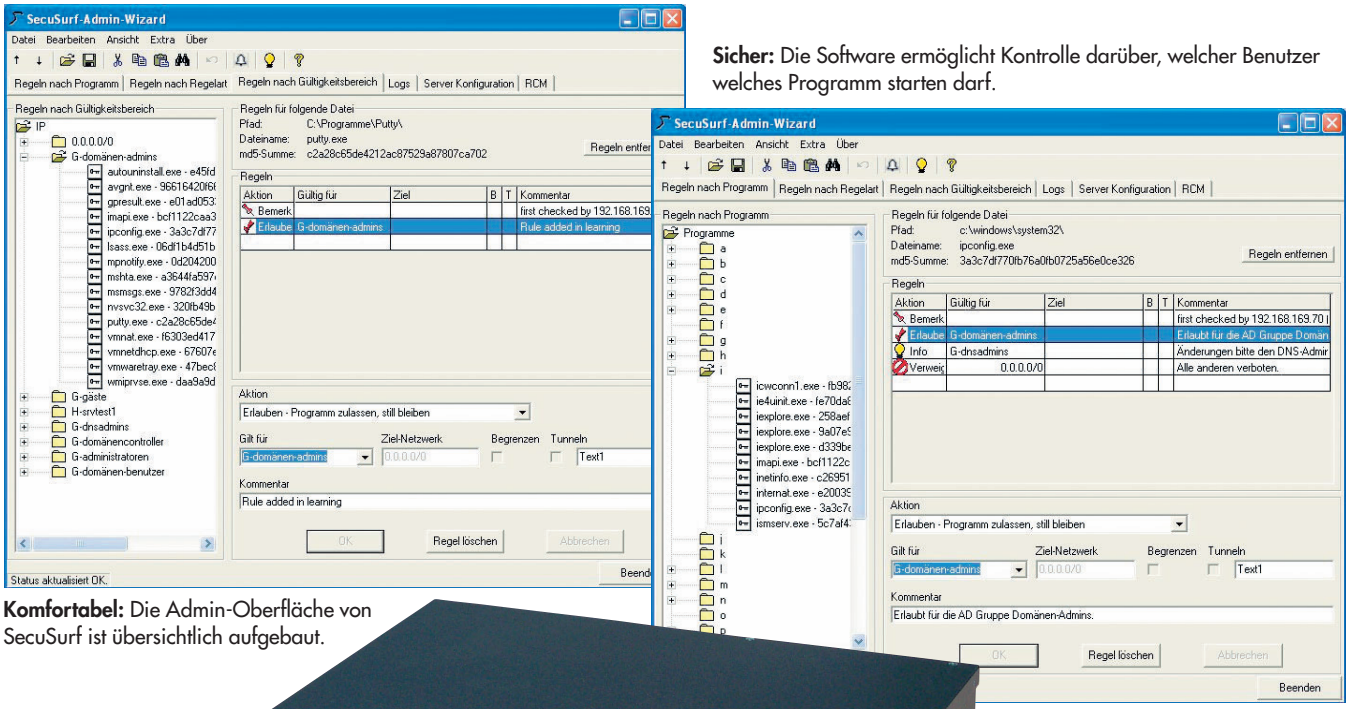
Auf diese Weise instruiert, muss der Angreifer seine vor Virenscannern versteckte Schadenssoftware nur noch irgendwie auf einen Rechner seines Opfers bringen. Möglichkeiten gibt es genug: Eine gut aufgemachte CD, die mit Begleitschreiben per Post ankommt oder ein Angriff über eine Sicherheitslücke im Browser etc. So wurde 2004 eine Si-

Der lüfterlose SecuSurf-SoHo-Server.

cherheitslücke in Microsoft-Produkten bekannt, die es ermöglicht, dass ein beliebiges Programm (zum Beispiel Trojaner des Angreifers) nur durch reines Anschauen eines entsprechend manipulierten Bildes gestartet wird. Am 9. Februar dieses Jahres meldete Microsoft, dass ein ähnlicher Fehler erneut aufgetreten ist. Folge: Der Angreifer muss nur noch dafür sorgen, dass sein Opfer sich das Bild anschaut. Ein Besuch auf einer manipulierten Webseite reicht aus, um die Schadenssoftware auszuführen.

Lösungen

Einmal auf dem Rechner des Angegriffenen ausgeführt, baut die Schadenssoftware über in der Firewall erlaubte Dienste, zum Beispiel normales Surfen, eine Verbindung zum Angreifer auf und nimmt von die-



Sicher: Die Software ermöglicht Kontrolle darüber, welcher Benutzer welches Programm starten darf.

Komfortabel: Die Admin-Oberfläche von SecuSurf ist übersichtlich aufgebaut.

Doppelpack: Zwei SecuSurf-Server der Enterprise Edition mit automatischer Redundanz.

sem Befehle entgegen. Die Folge ist die vollständige und vom Angegriffenen unbemerkte Kontrolle über das Netzwerk. Am Ende ist es selbst für Laien verblüffend simpel, die Kontrolle über ein fremdes, vermeintlich ausreichend gesichertes Netzwerk zu erhalten.

Doch was tun? Ist jedermann schutzlos ausgeliefert? Seit einigen Jahren bereits gibt es Lösungen, die beschriebenen Gefahren abzuwenden. Einen interessanten Ansatz verfolgt zum Beispiel das Produkt „SecuSurf“ des deutschen Herstellers SecuLution. SecuSurf macht sich zu Nutze, dass jeder Angriff auf ein Netzwerk immer voraussetzt, dass ein Programm des Angreifers (Virus, Wurm, Trojaner oder andere Schadenssoftware) auf einem Rechner des Angegriffenen zum Laufen kommen muss. SecuSurf erlaubt es festzulegen, welche Programme auf einem Rechner gestartet werden können. Alle nicht auf diese Weise explizit freigegebenen Programme können technisch nicht gestartet werden. Ein Virenscanner dagegen versagt nur solchen Programmen die Ausführung, die ihm bereits als schadhaft bekannt sind. Das fast simple Prinzip von SecuSurf hat weit reichende Konsequenzen: Jegliche unbekannten Programme, also auch alle noch unbekannten Viren, Trojaner oder andere Schadenssoftware, werden automatisch und ohne Update irgendwelcher Definitionsdateien in der großen Gruppe der unbekannten Programme und damit als unerlaubt eingestuft. Folge: Sie können schlicht-weg nicht ausgeführt werden, so lange ein Administrator das Programm nicht als vertrauenswürdig einstuft.

Praxistest

Das Evangelische Krankenhaus in Hamm etwa setzt bereits seit 2001 SecuSurf ein. „Eine besondere technische Herausforderung ist die Heterogenität unserer gewachsenen EDV-Struktur“, erklärt EDV-Leiter M. Raus. „Dank SecuSurfs Lernmodus war die Implementierung aber ohne großen Aufwand realisiert“, fügt er hinzu. SecuSurf läuft auf allen Windows-Systemen und sorgt dafür, dass nur die von der EDV-Abteilung freigegebenen Programme gestartet werden können. Das vereinfacht die Administration und Wartung der Systeme.

Das Unternehmen i-Tech, Partner der SecuLution und erfahrenes Unternehmen im Bereich IT-Security, hat sehr gute Erfahrungen beim Einsatz der Software in Unternehmen gemacht, die nicht ganz so sensible Daten wie ein Krankenhaus zu verwalten hatten. „Wir setzen SecuSurf bei Kunden ein, die die Sicherheit und Stabilität eines Netzwerkes nicht dem Zufall überlassen wollen. Die Resonanz ist hervorragend. Denn SecuSurf hilft, Geld zu sparen“, erklärt Marcell Oleff, Geschäftsführer der i-Tech. Neben dem enormen Zuwachs an Sicherheit bietet SecuSurf Features, die die Effizienz der Mitarbeiter erhöhen. Die Software ermöglicht eine bisher unerreichte Kontrolle darüber, welcher Benutzer welches Programm starten darf, und detaillierte Informationen darüber, welcher Benutzer wann welches Programm gestartet hat.

Torsten Valentin

*Quellen-Info: www.i-tech-online.de/facts

i-Tech
IT solutions for your business

INFO + INFO + INFO + INFO + INFO + INFO + INFO

i-Tech GmbH & Co. KG
Niederkasseler Lohweg 185
40547 Düsseldorf

Kontakt: Thomas Sammer
Telefon: +49 211-520668-0
Telefax: +49 211-520668-68
E-Mail: info@i-tech-online.de
Internet: www.i-tech-online.de