

PERSONAL FIREWALL

Auch unterwegs gut geschützt

In der Ausgabe 6/2010 wurde das Thema zentrale (Firmen-)Firewall näher beleuchtet. Aber nicht nur in einem Firmennetzwerk verhindert eine Firewall, dass Fremde auf den eigenen Rechner zugreifen können, auch Private müssen sich schützen.

AUTOR: ANDREAS WISLER

Im Gegensatz zu einer klassischen Netzwerk-Firewall ist eine Personal Firewall kein eigenständiges Gerät, welches den Verkehr zwischen zwei Netzwerken untersucht und filtert. Sie filtert nur zwischen dem Rechner, auf dem sie installiert ist, und dem angeschlossenen Netzwerk.

Das deutsche Bundesamt für Sicherheit in der Informationstechnik wie auch die Schweizerische Vereinigung InfoSurance empfehlen den Einsatz einer persönlichen

Firewall. Gerade in fremden Netzen (beispielsweise am Flughafen oder Bahnhof) ist der Betrieb einer aktuellen, lokalen Firewall Pflicht.

Ein Vorteil einer Personal Firewall ist, dass sie ermitteln kann, welche Applikation bei der ein- und ausgehenden Kommunikation beteiligt ist. Auf diese Weise sind applikationsspezifische Filter möglich, sodass man einigen Programmen den Datenverkehr erlauben kann und anderen nicht. Gerade in der heutigen Zeit gibt es viele Softwareprodukte, welche nach Hause telefonieren, also Informationen an eine entfernte Stelle

schicken. Oft ist dies auch gewünscht, beispielsweise für automatische Updates, es kann aber auch im Versteckten erfolgen und so möglicherweise das eigene (Kauf-)Verhalten übermitteln.

Der Hauptbestandteil einer Personal Firewall ist ein Paketfilter. Dieser Paketfilter ermöglicht es, eingehende oder ausgehende Datenpakete nach vorgegebenen Regeln zu blockieren. Filterkriterien können Quell- und Zieladresse, Protokoll sowie Quell- und Zielport sein, wie dies bereits im letzten Artikel genauer aufgezeigt wurde. Ergänzt wird dieser Filter durch das dynamische Zuweisen an eine Applikation. So kann konfiguriert werden, dass das Programm A ins Internet darf, die Software B hingegen nicht.

Mit Windows XP Service Pack 2 hat Microsoft «flächendeckend» eine Firewall eingeführt. Diese war zwar fehleranfällig, leistete aber bereits passable Dienste. Diese Personal Firewall überwachte als grosser Nachteil nur den Verkehr, welcher von «ausser» auf den eigenen PC auftraf. Nur wenn das Paket von intern angefordert (beispielsweise eine Webseite) wurde, wurde dieses an die interne Applikation (Internet Explo-

ZUM AUTOR



Andreas Wisler (Tel.: 052 320 91 20,) Dipl. Ing. FH, CISSP, ISO 27001 Lead Auditor, ist Geschäftsführer der GO OUT Production GmbH, welche sich mit ganzheitlichen und produktneutralen IT-Sicherheitsüberprüfungen und -beratungen auseinandersetzt. Regelmässig veröffentlicht er einen informativen Newsletter zu aktuellen Sicherheitsthemen, der kostenlos und unverbindlich auf www.gosecurity.ch (INFONEWS) heruntergeladen werden kann. Im Rahmen des Swiss Security Days ist er für die Schulungen an der Klubschule Winterthur.

rer, Firefox, o.ä.) weitergereicht. War ein Schädling aber erst einmal drinnen (durch einen USB-Stick, eine verseuchte CD, ...), konnte er ungefragt ins Internet kommunizieren und den PC übernehmen. Erst mit Windows Vista wird auch der nach aussen gehende Netzwerkverkehr untersucht. Dabei wurden gleichzeitig auch die bekannten «Kinderkrankheiten» behoben und das kostenlose Produkt macht einen guten Job.

Zugelassene Programme unter Windows 7 mit den drei möglichen Netzwerkzonen

Natürlich kann die integrierte Firewall auch durch ein anderes Produkt ersetzt werden. Dazu muss aber zwingend die Windows Firewall deaktiviert werden, da es ansonsten zu massiven Problemen kommen kann. Eines der bekanntesten Produkte ist hier sicherlich ZoneAlarm. In dieses Programm wurde beispielsweise eine Liste bekannter Software, welche als vertrauenswürdig eingestuft wird, integriert. Nach der Installation werden diese gesucht und automatisch in die Liste der erlaubten Programme hinzugefügt. Möchte eine Applikation, ein Dienst oder eine Software, welche sich nicht in dieser Liste befindet, mit dem Internet kommunizieren, wird der Benutzer zuerst um Erlaubnis gefragt. Und genau hier ist das grösste Problem einer Personal Firewall. Für unerfahrene Benutzer wirkt es oft verwirrend, wenn für unbekannte Prozesse nach einer Regel verlangt wird. Manche dieser Prozesse gehören zum Betriebssystem und sind für Internetverbindungen notwendig. Eine mögliche Grundhaltung ist, zunächst so wenige Prozesse wie möglich freizugeben. Funktioniert danach eine Software nicht mehr wie erwartet, so kann das Log nach gesperrten Verbindungen durchsucht werden, um den zu der behinderten Software gehörenden Prozess freizugeben. Ist der Prozess nicht bekannt, gilt es im Internet danach zu forschen. Dies bedeutet aber einen grossen Zeitaufwand und garantiert nicht, dass auch eine Lösung respektive Antwort gefunden wird. Daher empfehlen viele Sicherheitsprofis, kein weiteres Produkt zu verwenden und stattdessen auf die integrierte Windows-Firewall zu vertrauen.

Eine Firewall ist aber heute Pflicht und gehört auf jeden PC, welcher mit dem Internet verbunden wird. Sehr schnell kann es geschehen, und eine Schadsoftware hat unerlaubt Zugriff auf den Rechner erlangt. Die Firewall verhindert, dass dies passiert und minimiert dadurch das Infektionsrisiko. Wichtiger Hinweis zum Schluss: eine Firewall ersetzt aber nie ein gut gepflegtes Antivirenprogramm. Sollte ein USB-Stick oder eine CD-ROM verseucht sein, hilft auch die beste Firewall nicht. Beide Produkte ergänzen sich daher optimal.

Videoanleitungen zur Aktivierung der Windows Firewall finden Sie auf der Homepage www.infosurance.ch unter dem Punkt «5 Schritte für Private». ◆



MENTOR ist eine vollständig integrierte Softwarelösung für kleine und mittlere Unternehmen

Wenn Sie mehr Effizienz und Übersicht in Ihrem Unternehmen wünschen...

MENTOR unterstützt Sie z.B. mit folgenden Funktionen:
Kundenschichte, Kundenpreise
Fremdwährungen, PDF-Archiv,
Stücklisten, Staffelpreise, VOC-
Berechnung, Abonnemente,
WIR-Verrechnung u.s.w.

Software die "mitdenkt" ...
Die richtigen Papiere je Kunde
druckt, den Preis dieses Kunden
anzeigt...etc.

Interessiert?

Wir senden Ihnen gerne unsere
Dokumentation.
Informationen finden Sie auch
unter: www.usc.ch

FON: +41 (0)56 676 63 88
E-MAIL: info@usc.ch

topsoft
Messe für Business Software
10. - 12. Mai 2011 | Messe Zürich
Halle 3 | Stand 46 a | 9:00 - 17:00