Check: Spioniert mein Computer mich aus?

25.03.2016 | 10:01 Uhr | Arne Arnold – PC-WELT

Sicherheit per Firewall - © Fotolia: MK-Photo

Schon bei einem einfachen Windows-PC nehmen oft 20 oder mehr Programme Kontakt mit dem Internet auf. Welche das sind und wie Sie den Datenfluss kontrollieren, erfahren Sie hier.

Sie glauben, Ihr PC versendet insgeheim Daten ins Netz? Mit diesen Tipps finden Sie es heraus und behalten die volle Kontrolle über alle Ihre Tools. Das geht mit einer lokalen Firewall wie Zonealarm, Comodo Firewall oder Sphinx.

Warum Firewalls für den Desktop groß in Mode kamen

Im Jahr 2003 machte der Wurm Blaster die Runde, gefolgt vom Schädling Sasser im Mai 2004. Beide verbreiteten sich massenhaft. Sie konnten sich auf Windows-XP-PC's einschleusen, sobald der Rechner per Modem mit dem Internet verbunden war. Eine damals noch weit verbreitete Einwahlmethode. Beide Würmer nutzten Sicherheitslücken im Windows-Komponenten. Eine Desktop-Firewall hätte das verhindern können. Doch die in Windows XP integrierte Firewall war standardmäßig deaktiviert. Erst mit dem Service Pack 2 für Windows XP schaltete Microsoft die Firewall ein.

Das Service Pack erschien allerdings erst im August 2004. Zu diesem Zeitpunkt war das Vertrauen in die Sicherheitstechnik von Microsoft schon arg geschrumpft. Das lag zum einen an den vielen Sicherheitslücken, zum anderen an den Funktionen von XP, die automatisch und im Hintergrund Kontakt mit Microsoft-Servern aufnahmen. „Nach Hause telefonieren" wurde das damals genannt.

COMODO Internet Security Pro 8 DE Win

Die meisten Anwender wollten deshalb lieber eine Firewall von einem anderen Hersteller. Das war die große Zeit der kostenlosen Firewall Zonealarm Free und von anderen ähnlichen Tools. Die meisten dieser Programme sind heute verschwunden oder werden nicht mehr weiterentwickelt. Das trifft etwa auf die Sygate Firewall zu, die von Symantec aufgekauft und eingestellt wurde, oder die McAfee Firewall, die es nicht mehr als eigenständiges Dektop-Programm gibt.

Warum Firewalls nicht mehr wichtig erschienen

Desktop Firewall sind allerdings alles andere als einfach zu handhaben, und sie gingen mit ihren häufigen Meldungen den meisten Anwendern auch bald auf die Nerven. Außerdem gewöhnen sich die meisten Nutzer an die vielen Tools, die selbstständig den Kontakt mit dem Internet herstellten. In der Regel waren es ja Update-Programme, die nach neuen Sicherheits-Patches suchten – was ja eine durchaus erwünschte Aktion ist. Viele wechselten auch zu DSL und setzten einen DSL-Router ein. Dieser kann alleine schon durch seine NAT-Funktion sehr effektive Angriffe aus dem Internet abwehren.

Außerdem zeigten sich gängige Desktop-Firewalls gegenüber Trojanern und anderen Schädlingen oft machtlos. Denn hatte ein Trojaner das Antivirenprogramm bereits ausgetrickst, dann konnte er auch recht simpel die Firewall umgehen. Entweder er zerstörte die Firewall gleich weitgehend oder er verpackte seine Daten in den Datenstrom einer erlaubten Online-Anwendung, meist in die des Internet-Explorers. An dieser Verwundbarkeit von Desktop-Firewalls hat sich bis heute wenig geändert. Zur Abwehr von Viren, die bereits auf dem PC sind, tragen sie eher wenig bei. Diese Aufgabe muss auf einem Dektop-PC die Antiviren-Software leisten, schließlich hat sich die Windows-Firewall als Abwehrprogramm gegen unaufgeforderte Verbindungen von außen als sehr zuverlässig und auch performant erwiesen. Einige Internet-Sicherheitspakete nutzen heute etwa keine eigene Firewall mehr, sondern greifen auf die Funktion der Windows Firewall zurück, etwa F-Secure Internet Security oder Avira Antivirus Pro.

Warum es sich lohnt, eine Firewall für den Desktop zu installieren

Viele Anwendungen für den PC lassen sich heute überhaupt erst sinnvoll nutzen, wenn sie Kontakt zum Internet herstellen dürfen. Doch längst nicht alle. Wenn Sie wissen möchten, welches Programm eine Online-Verbindung aufbaut und wohin diese geht, dann hilft eine Desktop-Firewall. Sich eine solche zu installieren und damit die rudimentäre Windows-Firewall zu ersetzen, ist durchaus empfehlenswert. So bekommen Sie etwas Einblick in alle Programme mit Internetzugriff und entdecken vielleicht auch Tools, denen Sie den Online-Zugang lieber verweigern möchten.

Zugegeben: Einen raffinierten Spionage-Virus mit Rootkit-Funktion (Unsichtbarkeitsmodus) werden Sie mit der Desktop-Firewall nicht aufdecken. Dafür benötigen Sie auch weiterhin Ihr Antivirenprogramm, etwa die Freeware Avira Antivirus Free. Trotzdem wird sich eine Desktop-Firewall als sehr informativ erweisen. Sie müssen das Tool ja nicht für immer installiert lassen. Wenn Sie sich einen Eindruck von Ihren Online-Verbindungen gemacht haben, können Sie zur eingebauten Windows-Firewall zurückkehren. Diese wehrt seit Jahren zuverlässig unaufgeforderte Verbindungen vom Internet auf Ihren PC ab. Gleichzeitig lässt sie alle ausgehenden Verbindungen zu. Das ist zwar nicht informativ, stört aber eben auch nicht weiter.

Aus der mittlerwile recht überschaubar gewordenen Anzahl an reinen Desktop-Firewalls haben wir zwei Tools ausgewählt. Wer es einfach mag, setzt Sphinx Windows 10 Firewall Control Free ein, wer die volle Kontrolle möchte, nutzt Comodo Firewall Free.

Hinweis: Wenn Sie bereits ein komplettes Sicherheitspaket mit integrierter Firewall einsetzen, sollten Sie keine zusätzliche Desktop-Firewall installieren. Die Tools kommen sich sonst nur in die Quere.

Harte Regeln für die Firewall: Nichts für schwache Nerven

Die Comodo Firewall können Sie sehr strikt einstellen, sodass jede Aktion eines Online-Programms genehmigt werden muss. Dazu zählt dann nicht nur die Erlaubnis, eine Verbindung ins Internet aufzubauen. Sie müssen auch Änderungen an der Registry und andere Konfigurationseinstellungen bestätigen. So löste etwa der Start des Internet Explorers auf unserem Test-PC ganze 14 Nachfragen aus. So wird die Nutzung des

PC’s schnell zu einem Geduldsspiel. Wenn Sie zudem einmal einem erwünschten Programm versehentlich eine Erlaubnis verweigern, blockieren Sie Teile des Programms oder machen es gar vorübergehend ganz funktionsunfähig.

Mit einer Fehlkonfiguration der Firewall können Sie sich auch komplett vom Internet abtrennen. Der Einsatz von Comodo ist also nichts für schwache Nerven. Doch wer es mit der Firewall versucht, erhält zum Lohn tiefe Einblicke in seine Online-Programme. Außerdem lässt sich der Spuk jederzeit beenden, wenn Sie die Comodo Firewall wieder deinstallieren. An ihrer Stelle wird die Windows-Firewall wieder aktiv. Um wirklich keine Gefahr einzugehen, sollten Sie vor der Installation der Comodo Firewall einen Wiederherstellungspunkt in Windows anlegen. So können Sie jederzeit zu diesem Konfigurationszustand des Systems zurückkehren. Das geht über die Systemsteuerung oder über die Tastenkombination Windows-R und die Eingabe von „control sysdm.cpl“. wählen Sie auf der Registerkarte „Computerschutz“ Ihr Systemlaufwerk aus und sichern es über „Erstellen“.

Comodo Firewall: Die Installation Schritt für Schritt erklärt

Der Installationsassistent bietet Ihnen zunächst eine Sprachauswahl an. Im nächsten Schritt sind bereits zwei Optionen aktiviert. Zum einen stimmen Sie zu, dass die Software eine anonymisierte Nutzerstatistik an den Hersteller senden darf. Zum anderen erlauben Sie ihr, dass sie Infos zu unbekannten Programmen einholt. So kann die Firewall einfacher entscheiden, ob ein unbekanntes Tool harmlos ist oder feindselig. welche Daten genau versendet werden, verrät Comodo leider nicht. Das Tool, mit dem Sie Spione auf Ihrem PC finden möchten, will somit selber Daten senden, die Sie kaum einsehen können. Immerhin lässt sich das einfach verhindern, indem Sie den Haken vor dieser Option entfernen. Das hat natürlich deutlich mehr Nachfragen der Firewall bei Ihnen zur Folge.

In den nächsten Schritten können Sie von Ihrem Standard-Browser zum Comodo-Browser wechseln und künftig den DNS-Server von Comodo nutzen sowie die Suchmaschine von Yahoo einsetzen. Bis auf die Option mit Yahoo bringen die genannten Optionen einen gewissen Sicherheitsvorteil, zwingend sind sie aber nicht. Wenn Sie sich nicht sicher sind, wählen Sie alle Optionen ab. Der Comodo-Browser wird trotzdem installiert, sodass Sie ihn auch so testen können.

Nach der Installation macht sich Comodo erst mal etwas auf Ihrem Desktop breit: Neben der Bedienerführung startet ein Infofenster (Widget) in der rechten oberen Ecke und ein weiteres rechts unten. Im unteren Fenster geben Sie an, in welcher Netzwerkumgebung Sie sich gerade befinden (Zuhause, Arbeit oder öffentliches Netz). Das obere Fenster lassen Sie über einen Rechtsklick darauf und „Widget -> Anzeigen“ verschwinden. Außerdem ist noch ein Neustart fällig, was ebenfalls per Infofenster angezeigt wird. Nach dem Neustart wird einiges an Infofenstern geboten, doch wir installieren ja die Firewall, um Infos zu erhalten.

Comodo Firewall für den ersten Einsatz vorbereiten

Nach dem ersten Neustart des PC’s erscheint ein Werbefenster von Comodo, das die Vorteile der Firewall preist. Über „Dieses Fenster nicht mehr anzeigen“ verschwindet es dauerhaft. Bei unserem Test-PC taucht auch gleich die erste Frage auf. Ein Update-Tool für Treiber versucht eine Verbindung ins Internet aufzubauen, und Comodo bietet an, das zu erlauben, zu verbieten oder eine benutzerdefinierte Regel anzuwenden. Wenn jetzt ohnehin in Experimentierlaune sind und bei Ihnen ebenfalls schon eine solche Meldung kommt, können Sie ihr den Online-Zugriff auch verwehren. Sie werden gleich erfahren, wo Sie diese Regeln nachträglich ändern können.

Zuvor sollten Sie aber noch ein paar Grundeinstellungen setzen. Die Einstellungen, die wir hier vorschlagen, sind maximal unbequem und erzeugen deshalb das Maximum an Meldungen. Für die tägliche Arbeit ist das kaum geeignet, für Testzwecke aber sehr informativ.

Starten Sie die Bedienerführung der Firewall, etwa über die Verknüpfung auf Ihrem Desktop. Es präsentiert sich die „Einfache Ansicht“. Ein Klick auf das Einstellungssymbol links oben wechselt zur „Erweiterten Ansicht“. Dort wählen Sie „Firewall“, um die „Erweiterten Einstellungen“ zu öffnen. Die folgenden Änderungen beziehen sich auf diesen Bereich:

Gehen Sie auf „Firewall-Einstellungen“ und ändern Sie hinter „Filtern des Datenverkehrs aktivieren“ die Auswahl auf „Eigene Richtlinie“. Kontrollieren Sie, dass keine Haken unter „Dateibewertung -> Einstellungen zur Dateibewertung -> Online Suche aktivieren“ gesetzt sind. Stößt Comodo auf ein unbekanntes Online-Programm, wird es Sie fragen, ob das Programm ins Internet gehen darf oder nicht. Um noch mehr Meldungen zu bekommen, entfernen Sie zudem die Haken bei den beiden vorletzten Punkten: „Vertraue Anwendungen, die signiert sind“ und „Vertrau Dateien, die von vertrauenswürdigen Installationsprogrammen stammen“. Kontrollieren Sie schließlich noch unter „Allgemeine Einstellungen -> Konfiguration -> Comodo – Firewall Security“, ob hier das Wort „Aktiv“ steht. Falls nicht, ändern Sie das mit einem Doppelklick.

Außerdem: Einige Internetprovider verbinden Sie bereits per IPv6-Protokoll mit dem Internet. Damit die Firewall auch diese Verbindungen kontrolliert, setzen Sie einen Haken bei „Erweiterte Einstellungssymbol -> Firewall -> Firewall Einstellungen - > IPv6-Verkehr filtern“.

So nutzen Sie die Comodo Firewall für den PC

Die eben getroffenen Einstellungen sollten die Comodo Firewall und auch Sie jetzt richtig ins Schwitzen bringen. Vor allem, da die Firewall nun auch keinen signierten Programmen mehr vertraut, meldet sie eine Menge Systemkomponenten von Windows. Wenn Ihnen die Meldungen zu viel werden, sollten Sie diese Einstellung als Erstes rückgängig machen.

Die Meldungen von Comodo erscheinen unten rechts. Sie benennen ein Programm und wollen wissen, ob es eine genannte Aktion durchführen darf oder nicht. Wenn Sie auf den Programmnamen klicken, erhalten Sie weitere Infos zu diesem Tool. Interessantere Infos gibt’s meist über den Pfeil rechts vom Programmnamen. Comodo verrät so, was das Tool gerade anstellen möchte.

Sind Sie sich nicht sicher, was es mit dem Tool auf sich hat, müssen Sie danach etwa bei Google suchen und dann entscheiden, ob es harmlos ist oder nicht. Im Zweifelsfall können Sie immer erst mal „Blockieren“ wählen. Nur bei Ihrem Internet-Browser sollten Sie natürlich „Erlauben“ anklicken, damit Sie ihn nutzen können. Noch besser, Sie wählen die Regel „Behandeln als -> Web-Browser“. Ein Haken unten bei „Antwort merken“ speichert die entsprechende Regel in den Einstellungen. Wird ein legitimes Programm immer wieder gemeldet, etwa weil es laufend Änderungen an der Registry vornehmen möchte, können Sie auch „Behandeln als -> Zugelassene Anwendung“ sowie „Installations- und Updateroutine“ wählen, um weitere Meldungen zu vermeiden.

Entscheidungshilfe: Suchen Sie nach dem Namen eines Online-Programms bei Google, sollten Sie eigentlich Hinweise darauf bekommen, ob das Tool harmlos ist oder nicht. Zusätzliche Hilfe bietet die Shareware Secutity Task Manager, die Bewertungen zu allen aktiven Prozessen gibt.

Online-Verbindungen, die Sie nicht verbieten sollten: Außer dem Browser sollten Sie auch die Anfragen zu Update-Tools mit „Zulassen“ beantworten. Denn wenn etwa Ihr Antiviren-Programm keine Updates mehr-

laden darf, wird es Ihren PC nicht mehr schützen. Und wenn die anfälligen Adobe-Tools Flash und Adobe Reader sich nicht aktualisieren dürfen, hat Ihr System bald Sicherheitslücken.

Firewall-Regeln nachträglich ändern: Möchten Sie eine gespeicherte Regel nachträglich ändern, geht das unter „Erweiterte Einstellungen -> Dateibewertung -> Dateiliste“. Dort werden Sie bereits etliche Programme mit der Einstellung „Vertrauenswürdig“ vorfinden. Diese hat Comodo automatisch so eingestuft, als Sie die Einstellungen noch nicht auf „Eigene Richtlinie“ geändert hatten. Die Regeln lassen sich einzeln pro Programm ändern oder auch komplett löschen.

Protokolle einsehen: Ein Klick auf „Aufgaben“ in der Hauptbedienerführung von Comodo bringt Sie zum Menüpunkt „Protokolle einsehen“. Dort kontrollieren Sie, welche Tools seit der Installation der Firewall ins Internet gegangen sind.

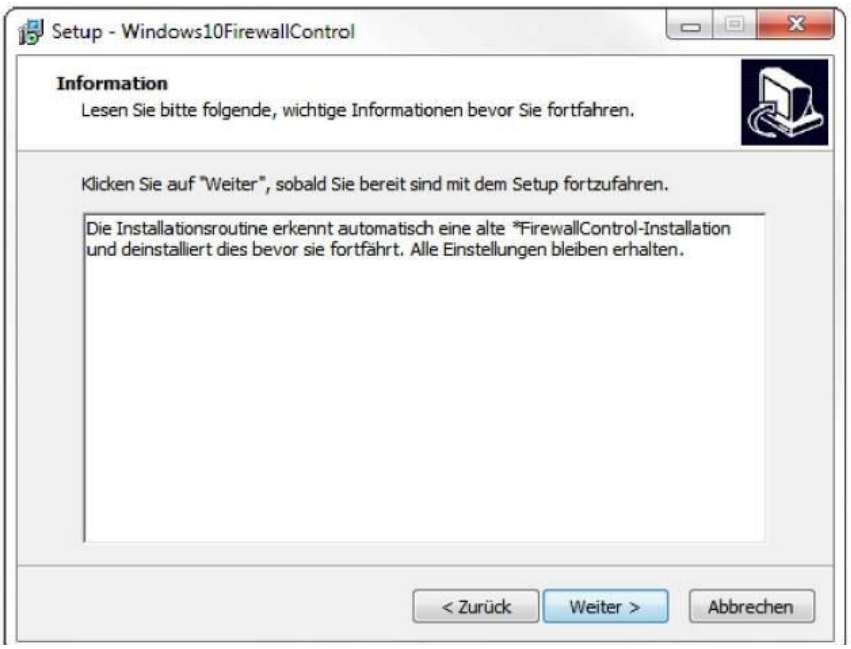
Comodo weniger streng einstellen: Die Firewall von Comodo bietet sehr viele Funktionen und Einstellmöglichkeiten. Wenn Sie lieber weniger Meldungen, dafür mehr automatische Entscheidungen von Comodo bekommen möchten, mache Sie die oben genannten Änderungen rückgängig. Zudem wechseln Sie unter „Einstellungen zur Sicherheit -> Firewall -> Firewall-Einstellungen -> Filtern des Datenverkehrs aktivieren“ die Auswahl von „Eigene Richtline“ hin zu „Sicherer Modus“. Diese Änderung lässt sich auch direkt in der Hauptbedienerführung von Comodo vornehmen. Mit diesen Änderungen sollten nur selten Nachfragen kommen.

Sphinx: Die einfache Alternative zur Firewall von Comodo

Wer das Aufspüren seiner Online-Programme nicht ganz so kompliziert gestalten möchte wie mit der Comodo Firewall, für den gibt es eine praktische Alternative. Das Tool setzt auf der Windows-Firewall auf und erweitert deren Funktionalität. Die Analysemöglichkeiten sind zwar nicht so groß wie bei Comodo, aber für den Hausgebrauch sind sie durchaus ausreichend.

Sphinx Windows 10 Firewall Control Free
Wer das Aufspüren seiner Online-Programme nicht ganz so kompliziert gestalten möchte, wie mit der Comodo Firewall, für den gibt es mit Sphinx Firewall Control Free eine praktische Alternative.
Sphinx Firewall Control

Sphinx Windows 10 Firewall Control Free
Hier sehen Sie die Installation der Firewall.
© PC-Welt

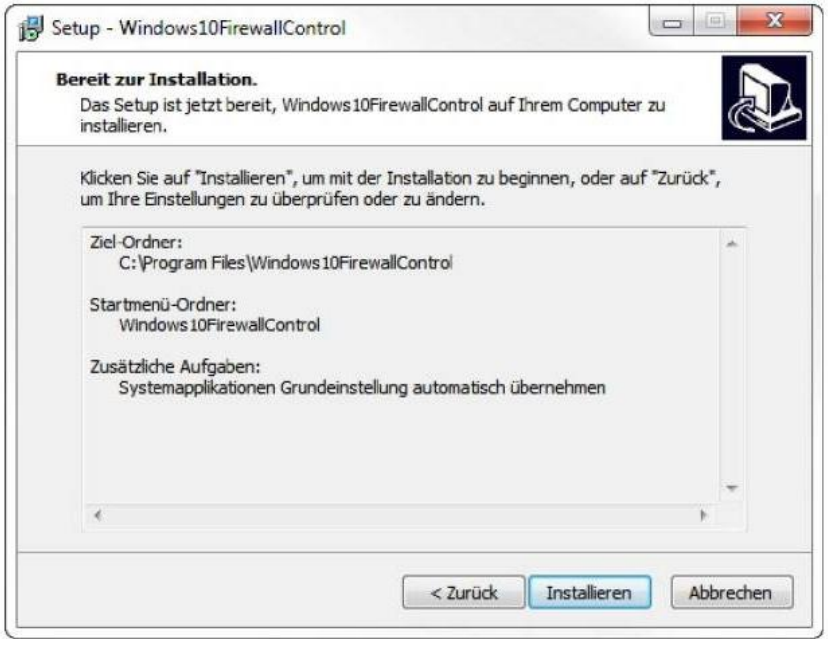


Sphinx Windows 10 Firewall Control Free
Der Setup-Assistent funktioniert wie gewohnt.
© PC-Welt

Sphinx Windows 10 Firewall Control Free

Nach ein paar Klicks…

© PC-Welt



Sphinx Windows 10 Firewall Control Free

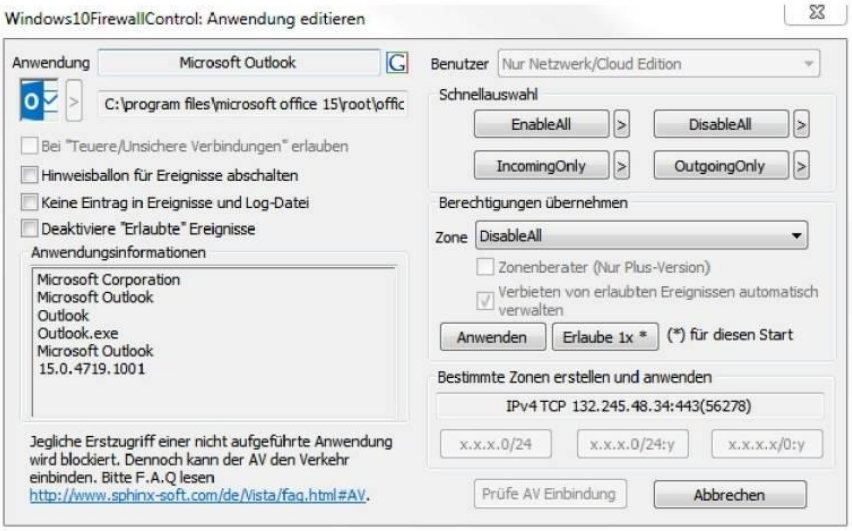
… ist die Installation auch bald…

© PC-Welt

Sphinx Windows 10 Firewall Control Free

… abgeschlossen.

© PC-Welt



Sphinx Windows 10 Firewall Control Free

Sobald ein Online-Programm eine Internet-Verbindung aufbaut, meldet das die Firewall. Per "Allow All" können Sie den Zugriff erlauben.

© PC-Welt