3 allgemeine Irrtümer über Firewalls

3 allgemeine Irrtümer über Firewalls

Dieser Beitrag wird mit freundlicher Genehmigung von EMSISOFT, dem einzigartigen Antiviren-Software-Hersteller

zu Beziehen bei Nicos-EDVDienst Emsisoft-Handelspartner

Autoren: In Sicherheitswissen by Doreen on May 2, 2016 | Français, English, Deutsch



Jeder weiß, was eine Firewall ist, oder? Leider nicht …

Weiß beispielsweise Ihre Mutter, was es mit einer Firewall auf sich hat? Interessiert es sie überhaupt? Benötigt Ihre Tochter eine Firewall, um sich vor Online-Kriminellen zu schützen? Damit auch unsere weniger erfahrenen Anwender verstehen, welche Rolle Firewalls im modernen Produktangebot zum Online-Schutz spielen, möchten wir heute drei Missverständnisse aufklären.

Für erfahrenere Emsisoft-Nutzer hatten wir bereits einen Artikel über die technischen Eigenschaften und Anwendungsbereiche von Firewalls veröffentlicht. Immerhin sind sie die häufigste Maßnahme, die PC-Anwender zum Schutz vor bösartiger Software und Spionage ergreifen.

Aber die Zeiten ändern sich. Heutzutage ist das Verhalten von Online-Bedrohungen oftmals so ausgelegt, dass Firewalls die Mehrheit typischer Internetnutzer nicht mehr schützen können.

3 Irrtümer über Firewalls

Irrtum 1: „Firewall“ war ein guter Film.

Ihre Mutter würde wahrscheinlich nur wegen des gut aussehenden Harrison Fords über die doch recht vorhersehbare Handlung hinwegsehen. Auch wenn der Film Firewall aus dem Jahr 2006 einige Bedrohungen der Online-Welt aufgreift, war er dennoch kein Oscar-würdiges Meisterwerk. Mehr dürfte dazu nicht zu sagen sein.

Irrtum 2: Firewalls schützen Ihren Computer, indem sie Malware erkennen.

In der heutigen Online-Welt geben Firewalls oftmals ein falsches Gefühl der Sicherheit. Weshalb? Der wesentliche Zweck einer Software-Firewall ist es, mögliche Punkte zu blockieren, über die Hacker auf Ihren Computer zugreifen könnten. Doch was passiert, wenn Ihr Computer bereits beim Installieren der Firewall mit Malware befallen ist? Sie fühlen sich sicher, obwohl Ihr System infiziert ist. Daran ändert dann auch die Firewall nichts.

Sie ist schlicht und einfach nicht dazu ausgelegt, Malware zu erkennen, die bereits auf Ihrem Computer aktiv ist.

> *Das Schadprogramm kann ungehindert mit dem Hacker auf der anderen Seite der Welt kommunizieren – selbst mit Firewall.*

Typische Vorgänge zur Malware-Infizierung benötigen keine sogenannten Brute-Force-Verfahren, um auf Ihren Computer zu gelangen. Sie setzen auf Verfahren, die die Firewall gar nicht erst blockiert. Hierzu wird beispielsweise der Benutzer überzeugt, eine Anwendung zu installieren, die er für etwas anderes hält.

Aber warum erkennen Firewalls Malware nicht?



Sicher können moderne Software-Firewalls einige ausgehende Verbindungen von Schadprogrammen blockieren. Indem die Malware jedoch bereits auf Ihren Computer gelangt ist, konnte sie höchstwahrscheinlich auch Ihre gesamte Firewall deaktivieren, um eine Kommunikation zu ermöglichen. Das nachträgliche Installieren einer Firewall hat also wenig Sinn. Stattdessen ist eine Anti-Malware-Software ratsam, die aktiv nach der Malware in Ihrem System sucht.

Das bedeutet keinesfalls, dass Firewalls unnütz sind! Sie sind einfach nicht darauf ausgelegt, Malware zu blockieren.

> *Für diese Aufgabe ist Anti-Malware-Software zuständig wie Emsisoft Anti-Malware. Eine Firewall soll Sie lediglich nach außen hin „unsichtbar" machen, indem sie die Kommunikation mit anderen Programmen über bestimmte Kanäle oder Ports unterbindet.*

Irrtum 3: Firewalls sind immer HIPS (Host-basierte Systeme zur Angriffsabwehr).

Vor gar nicht allzu langer Zeit machten Software-Firewalls genau das, was die Benutzer von ihnen erwarteten: Netzwerkdaten filtern. Das ist auch heute noch die gängige Definition für den Begriff „Firewall". Doch indem es kaum noch Raum für Innovation gab und alle Anbieter mehr oder weniger dieselbe Qualität boten, war die Technologie schon bald am Ende ihrer Möglichkeiten angelangt. Folglich wurden die Produkte mit neuen und unnötigen Funktionen überladen, etwa die Überwachung von Änderungen im Betriebssystem oder das Erkennen zahlloser anderer „verdächtiger" Vorgänge.

Das Hauptproblem an diesen Technologien ist, dass ihre Überwachungs- und Erkennungsfunktionen relativ ungenau sind. Oftmals werden für alle möglicherweise mit einem Angriff in Zusammenhang stehenden Aktionen Warnungen ausgegeben. In 99,9 % der Fälle handelt es sich dabei jedoch um

vollkommen ungefährliche Prozesse.

Eine derartige Fülle an Warnmeldungen ist nicht nur extrem störend, sondern kann auch gefährlich werden. Der Anwender gewöhnt sich zu leicht an, ohne weiteres Überprüfen immer auf „Zulassen“ zu klicken.

> *Und genau das kann früher oder später dazu führen, dass ein Angreifer doch den Schutz durchbricht.*

HIPS sind daher nur für Experten ratsam, die mit einer derartig großen Menge von Warnmeldungen umgehen und von diesem zusätzlichen Schutz profitieren können.

HIPS sind die Vorgänger moderner Anti-Malware-Software



Den HIPS ist viel zu verdanken: Aufgrund der Firewall-Technologie verlieren HIPS für normale Anwender keinesfalls an Bedeutung. Tatsächlich ist die ihnen zugrunde liegende Funktionsweise der Ausgangspunkt für die spätere Entwicklung der Verhaltensanalyse, einem wichtigen Bestandteil moderner Anti-Malware-Software. Programme, die diese Technologie nutzen, erzeugen nur höchst selten Fehlalarme. Dabei sind HIPS jedoch weder mit Verhaltensanalyse noch dem Begriff „Firewall“ gleichzusetzen.

> *Für weniger erfahrene Anwender lässt sich das Ganze recht einfach ausdrücken: Den meisten Computerbenutzern reicht als Schutzmaßnahme eine hochwertige Software zur Internetsicherheit. Sie schützt nicht nur den Computer, sondern erkennt auch aktive Malware.*

Wie sollten normale Anwender also vorgehen?

Falls Sie ein Anwender sind, der häufig auf Reisen ist und seinen Laptop mit

verschiedenen Netzwerken verbindet, etwa über öffentliches WLAN in Cafés oder auf Flughäfen, empfehlen wir Ihnen Emsisoft Internet Security (verfügt über eine integrierte Firewall). Sollte Ihr Computer immer mit demselben Netzwerk verbunden sein (beispielsweise zu Hause), reicht zum Schutz Emsisoft Anti-Malware (Windows 7 und neuere Versionen verfügen über eine integrierte Firewall).

Sie sind mit beiden Emsisoft-Produkten optimal geschützt und können darauf vertrauen, dass jede aktive Malware auf Ihrem Computer erkannt wird – mit oder ohne Firewall.

Eine kleine Erinnerung an unsere Bestandskunden: Wenn Sie von Emsisoft Anti-Malware zu Emsisoft Internet Security wechseln möchten, können Sie das jederzeit über die Lizenzverlängerung tun. Sollten Sie den vollen Funktionsumfang von Emsisoft Internet Security nicht mehr benötigen und ein „Downgrade“ zu Emsisoft Anti-Malware vornehmen wollen, hilft Ihnen gerne unser Kundendienst weiter.

Bis dahin wünschen wir Ihnen eine gut geschützte Zeit.

Sollten Sie Ihren Computer besser schützen wollen, fragen Sie uns nach Emsisoft. Wir machen die Installation und Wartung.
Zum Virenschutz von Nicos-EDV-Dienst