

Warum Antispyware von Agnitum

Warum Spyware-Schutz durch eine Firewall sinnvoll ist

Spyware – eine wachsende Bedrohung

Spyware ist ein Problem, mit dem immer mehr Computer-Nutzer zu kämpfen haben. Laut Schätzungen einer Studie der National Cyber Security Alliance sind 9 von 10 PCs mit Internetanschluss von Spyware befallen.

Die Definition von Spyware bleibt zwar unscharf, doch im Allgemeinen steht der Begriff „Spyware“ (deutsch: Spionagesoftware) für Software, die:

- sich ohne Wissen bzw. Einwilligung des Benutzers heimlich selbst installiert,
- Änderungen an der installierten Software oder der internen Konfiguration des Betriebssystems vornimmt,
- unerwünschte Werbe-Banner anzeigt und
- den Diebstahl sensibler Benutzerdaten aus dem Computer ermöglicht.

Spyware-Programme umgehen konventionelle Sicherheitstools wie Antiviren-Software und einfache Firewalls; ihre Entfernung erfordert eine spezielle Technologie, die diese Tools mit einer eher allgemeinen Funktionalität nicht bieten können. Spyware arbeitet verdeckt im Hintergrund und macht sich für die meisten Benutzer erst dann bemerkbar, wenn sie bereits Schaden angerichtet hat.

Spyware-Schutz allein reicht nicht mehr aus

Die meisten Anbieter von Sicherheitstools entwickeln separate Antispyware-Programme, die die Spyware auf einem bereits infizierten Computer aufspüren und vernichten. Diese Lösungen arbeiten nach einem reaktiven Prinzip, das heißt, sie bekämpfen das Problem erst, wenn es schon zum Problem geworden ist. Als ultimativer Schutz gegen Spyware können sie daher wohl kaum angesehen werden. Damit ein Antispyware-Programm wirklich effektiv ist, müssen sowohl proaktive (vorbeugende Abwehr) als auch reaktive (Entfernung nach Erkennung) Mechanismen zum Einsatz kommen.

Und da die meisten eigenständigen Antispyware-Programme auf Definitionen basieren, sind die Benutzer nicht auf die Abwehr so genannter „Zero-Day Threats“ und weniger bekannter Malware-Programme vorbereitet, für die noch keine Signaturen bereitgestellt wurden. Dies ist auch dann der Fall, wenn die Benutzer ihre Software regelmäßig aktualisieren – wovon man nicht immer ausgehen kann.

Outpost Firewall Pro 3.0 kombiniert Antispyware-mit Firewall-Technologie

Outpost Firewall Pro 3.0 von Agnitum ist eine integrierte Sicherheitslösung, die Firewall- und Spyware-Technologie miteinander verbindet und den Computer so vor aktuell und künftig drohenden Spyware-Angriffen schützt. Durch die Kombination dieser beiden Sicherheitstechnologien bietet Outpost DIE ultimative Lösung für das Spyware-Problem.

Doch warum ist eine integrierte Lösung eigentlich zwei separaten Produkten vorzuziehen? Hier die Gründe:

- **Sämtliche Schutzfunktionen werden durch ein- und dasselbe Programm koordiniert.** Mit diesem Konzept können die internen Funktionen der Programmmodule optimiert, Zeitlücken zwischen Angriff und Reaktion geschlossen und Kompatibilitätsprobleme gelöst werden, so dass ein effizienterer Systembetrieb möglich ist.
- **Verwaltung, Überwachung und Aktualisierung erfolgen über eine zentrale Konsole.** Dieser Ansatz verbessert die Effizienz und Einsatzfähigkeit des Programms, spart Zeit und macht Extra-Updates überflüssig.
- **Die Systemressourcen werden weniger belastet.** Das Ergebnis: Speicherbelastung, Festplatten-Performance und Prozessorleistung werden optimiert, da im Hintergrund weniger Prozesse laufen.

Proaktiver Schutz durch Outpost bedeutet: Schon bevor die Spyware versucht, eine Verbindung zu dem Ziel-PC herzustellen, wird sie von der Firewall abgefangen, ohne dass eine spezifische Identifizierung des Angriffs erforderlich ist. Malware, die sich bereits im System befindet, wird aufgespürt und mithilfe der reaktiven, signaturbasierten Technologie vernichtet.

Spyware-Angriffsszenarien: Wie Outpost den Benutzer schützt

Outpost Firewall Pro bietet Multilayer-Schutz gegen Spyware, Trojaner, Würmer und andere gefährliche Programme. Hier nur ein paar Beispiele für mögliche Attacken und die Sicherheitsfunktionen von Outpost:

Phasen eines spyware-angriffs

**Phase 1:
Die Spyware
nähert sich dem
Zielsystem, stellt eine
Verbindung her und
versucht, sich selbst zu
installieren:**

Wie die Spyware auf Ihren Computer gelangt

Über unzureichende Sicherheitseinstellungen im Browser.


Verborgen in einem Email-Anhang.


Über „Drive-by-Downloads“ von Interseiten, die Spyware übertragen.


Mit vertrauenswürdiger Software (z.B. Shareware, P2P-Clients).


Über Sicherheitslücken im System.


Wie Outpost Sie schützt

 Das Active Content-Plugin von Outpost unterstützt die Browser-Sicherheit, indem es Zugangskanäle verschließt, über die Spyware in den Computer eindringen kann.

 Das Attachment Quarantine-Plugin von Outpost ermöglicht die Isolierung anhand des Dateityps. So wird das versehentliche Öffnen von Dateien verhindert, die möglicherweise mit Spyware verseucht sind.

 Der Spyware Scanner von Outpost ermöglicht die Überprüfung jeder heruntergeladener Datei und entfernt Spyware-Software umgehend.

 Der Real-time Monitor von Outpost überwacht permanent alle Aktivitäten auf Ihrem Computer und entfernt Spyware sofort nach der Erkennung.

 Die Firewall Engine von Outpost ermöglicht die Erstellung benutzerdefinierter Regeln. Diese bestimmen, wie Systemfunktionen verarbeitet werden und welche internen Zugriffsberechtigungen die anfälligen Komponenten haben. Auf diese Weise kann das Problem entschärft werden, bis ein entsprechender Patch vom Hersteller verfügbar ist.

**Phase 2:
Die Spyware hat
den Computer infiziert
und sich im System
festgesetzt:**


Was die Spyware auf Ihrem Computer bewirkt


Spyware ist bereits auf Ihrem Computer aktiv.


Ungefährliche Komponenten von installierten Anwendungen werden durch schädlichen Code ersetzt („Application Hijacking“), so dass anstelle des ursprünglich „legalen“ Programms Spyware ausgeführt wird.

Browser- und Windows-Einstellungen werden von eingebetteter Spyware verändert.

Wie Outpost Sie schützt

 Der Real-time Spyware Monitor von Outpost stellt eine aktive Spyware im Hauptspeicher fest und stoppt umgehend den laufenden Prozess. Nach Deaktivierung des Prozesses werden alle Spuren des schädlichen Codes gelöscht.

 Über die Outpost-Funktionen Component Control und Hidden and Open Process Control kann gesteuert werden, ob eine Anwendung Daten mit einer anderen austauschen und für diese Prozesse ausführen darf. So wird eine Lücke geschlossen, die häufig von Spyware-Programmen zur Übertragung von Benutzerdaten verwendet wird.

 Outpost zeichnet Änderungen an Programmen auf und zeigt ein Warnfenster an, über das der Benutzer entscheiden kann, ob er eine bestimmte Änderung zulässt.


**Phase 3:
Die Spyware hat
Steuerfunktionen
übernommen und
versucht, seinen
unerlaubten Auftrag
auszuführen:**


Was die Spyware auf Ihrem Computer bewirkt

Die Spyware versendet sensible Benutzerdaten.

Die Spyware zeigt lästige Werbe-Banner an, öffnet mehrere Pop-up-Fenster und blendet unzulässige bzw. unerwünschte Web-Inhalte ein.

Wie Outpost Sie schützt

 Der Anwendungsfilter in der Firewall verhindert die Übertragung von Daten. Die Spyware wird identifiziert und durch das Antispyware-Modul entfernt. Dieses implementiert zusätzlich einen ID-Block, der die Übertragung bestimmter, zuvor definierter Daten vom Computer unterbindet.

 Das Outpost-Plugin zum Schutz vor unerwünschter Werbung wehrt Werbe-Banner anhand der Größe, des Werbetreibenden, der Animationsart etc. ab. Der Pop-up-Blocker verhindert die Anzeige störender Fenster auf dem Bildschirm. Mit dem Content-Plugin können Web-Inhalte anhand bestimmter Schlüsselbegriffe oder URLs herausgefiltert werden.



Fazit: In allen Phasen einer Spyware-Attacke schützt Outpost Firewall Pro 3.0 mit Antispyware den Computer vor Spyware und bewahrt private Benutzerdaten vor dem Diebstahl ohne Einbußen in der Systemleistung.

Wenn Sie mehr über Outpost Firewall Pro 3.0 erfahren und eine Testversion herunterladen möchten, besuchen Sie uns unter <http://www.agnitum.de/products/outpost>.