

Proaktiver Schutz als Verteidigung gegen Bedrohungen aus dem Internet

Überblick

In dieser technischen Erläuterung wird dargelegt, warum ein proaktiver Schutz ein unverzichtbarer Bestandteil heutiger Sicherheitsprodukte ist. Es wird beschrieben, wie die intelligente Verwendung von Programmverhaltenskontrollen die Auswirkungen von Online-Sicherheitsgefahren auf ein Minimum reduzieren, wenn nicht sogar völlig beseitigen kann.

Die Bedrohungslandschaft

Beinahe täglich entstehen neue Sicherheitsbedrohungen. Neue Viren, Trojaner und andere schädliche Programme werden dazu entwickelt, sich in unsere sichere und produktive Internetnutzung hineinzudrängen. Ungepatchte Sicherheitslücken¹ machen Computer anfällig für eine Infektion durch Zero-Day-Angriffe (Angriffe direkt nach dem Auftauchen einer neuen Bedrohung, bevor die Sicherheitsprodukte entsprechend aktualisiert werden können), die innerhalb weniger Stunden nach ihrem ersten Auftreten im Internet ernsthaften Schaden anrichten können.

Sicherheitsfachleute haben in Studien festgestellt, dass das Ausmaß an Bedrohungen innerhalb der letzten 5 Jahre erheblich angestiegen ist und bestätigen, dass es immer schwieriger wird, durch eine Signatur-Erkennung mit den Malware-Programmierern Schritt zu halten. Mit leicht verfügbaren Toolkits für die Erstellung individuell angepasster Malware aus Code-Mustern können selbst Hobby-Programmierer ihre eigene Malware herstellen. Darüber hinaus ist die Personalbesetzung in den Forschungsabteilungen der Sicherheitsfirmen geradezu winzig, wenn man sie mit der Anzahl von Programmierern auf der „dunklen Seite“ vergleicht, die mittlerweile in bevölkerungsreichen Ländern wie China und Indien aktiv sind und die Reihen der Hacker und Cyberkriminellen verstärken.

Eine erfolgreiche Abwehr der Bedrohungen wird zusätzlich dadurch erschwert, dass Virenautoren dieselben Techniken zur Qualitätskontrolle verwenden wie die Entwickler von Anti-Malware-Produkten. Sie testen ihre neuesten Entwicklungen mit den neuesten Versionen von Anti-Malware-Produkten, um sicherzugehen, dass sie immer einen Schritt voraus sind.

Es ist offensichtlich fast unmöglich, sich nur mit einer signatur-basierten Lösung gegen neue, modifizierte oder unklare Malware zu schützen. Die Autoren von bösartigen Programmen werden gegenüber dieser reaktiven Art der Verteidigung² immer einen Vorsprung wahrnehmen können.

Die Notwendigkeit zusätzlicher Maßnahmen

Während der reaktive Schutz zur genauen Identifizierung und Desinfizierung bekannter Schadprogramme nach wie vor ein wichtiger Bestandteil des Malware-Schutzes ist, besteht eindeutig die Notwendigkeit eines proaktiven Schutzes, der unautorisierte Programmaktivitäten von vornherein verhindern kann.

Durch einen zusätzlichen proaktiven Schutz, der überwacht, was Programme tun, mit welchen Programmen und Komponenten ein bestimmtes Programm kommunizieren darf und welche Änderungen am Betriebssystem versucht werden, sind Computer besser gegen unzulässige Aktivitäten geschützt und besser dafür ausgerüstet, einen Malware-Befall bereits im Frühstadium zu verhindern.

¹ Ein Beispiel dafür ist die Sicherheitslücke durch den Animierten Windows-Cursor (<http://secunia.com/advisories/24659>). Dieser Fehler ermöglicht es einem Angreifer, auf dem Anwender-Rechner auf Daten zuzugreifen und unzulässigen Code auszuführen. Microsoft hat vor einiger Zeit einen Patch dafür herausgegeben; es werden jedoch nach wie vor Rechner von Anwendern infiziert, die die neuesten Patches nicht installiert haben.

² „Antiviren-Programme sind tot: Lang lebe Anti-Malware-Schutz“ – diese Studie der Yankee Group wird umfassend in einem (englischsprachigen) [PC-World-Artikel](#) besprochen.

Programm-Interaktivität – eine Haupt-Schwachstelle

Windows bietet den Programmen auf einem PC zahlreiche Interaktionsmöglichkeiten³ und die meisten dieser Interaktionen sind zulässig. Die Programme können ohne Einschränkungen Komponenten gemeinsam nutzen, gegenseitig ihre ausführbaren Dateien aufrufen und starten und eine Reihe verschiedener Hooks („Haken“) verwenden, um die Programm-Interaktion zu vereinfachen und das Computer-Erlebnis des Anwenders stromlinienförmiger und benutzerfreundlicher zu machen. Wenn man zum Beispiel eine an eine E-Mail angehängte PDF-Datei lesen möchte, muss man dazu lediglich auf das Datei-Symbol klicken, und die PDF-Datei wird automatisch im Standard-Programm geöffnet. Es wäre wesentlich zeitaufwendiger, wenn man die Datei auf der Festplatte abspeichern, den Acrobat Reader öffnen und die Datei in die Anwendung laden müsste.

Windows lässt jedoch auch weniger harmlose Interaktionen zu, und das stellt ein erhebliches Sicherheitsrisiko dar. Auch die Programme selbst dürfen vielleicht schädliche Aktivitäten durchführen, von der Prozessspeicher-Übernahme über die Verwendung der Berechtigungen eines anderen Programms für bösartige Zwecke bis hin zu unzulässigen Veränderungen der Windows-Konfiguration.

Diese Anwendungsarten sind natürlich völlig inakzeptabel und müssen kontrolliert werden. Das erfolgt am besten über spezielle Werkzeuge, die eigens dafür entwickelt wurden, diese Arten von Aktivität zu überwachen und illegale Operationen schon zu blockieren, bevor versucht werden kann, sie auszuführen.

Anwendungsfall

Ein durchschnittlicher Windows-Anwender wird täglich zahlreichen Risikofenstern ausgesetzt. Die Haupt-Angriffsvektoren sind:

1) *Drive-By-Downloads von Malware beim Besuch von Websites, die nur mit bösartigen Zwecken erstellt oder durch Sicherheitslücken übernommen wurden und die eingebettete Programme zur Ausnutzung von Sicherheitslücken hosten oder bösartige Skripte ausführen.*

Das kann zum Beispiel der Fall sein, wenn jemand auf der Suche nach beliebten Inhalten wie etwa Bildschirmschonern, Musik-Downloads oder Java-Spielen im Internet surft und versehentlich auf einer verseuchten Webseite landet, die heimlich schädlichen Code in den Browser injiziert. Die Sicherheit des Browsers wird so eingeschränkt und kann eine Infektion des PCs ermöglichen. Auch durch Spam oder Phishing kann ein ahnungsloses Opfer auf kriminelle Webseiten gelockt werden.

2) *Ausgeführte Programme von Peer-to-Peer-Netzwerken.*

Man sollte auf jeden Fall daran denken, dass Dateien aus nicht vertrauenswürdigen Quellen nicht immer das sind, was sie zu sein scheinen. Die Datei „Britney.mpg“ ist zum Beispiel nicht unbedingt ein Video-Clip von Britney Spears, sondern kann genauso gut ein Trojaner sein. Wenn die entsprechende Malware noch relativ neu ist, können herkömmliche Anti-Malware-Programme sie vielleicht nicht entdecken, bevor sie ausgeführt werden kann.

3) *Das Öffnen infizierter E-Mail-Anhänge oder der Download von Links über eine Instant-Messenger-Kommunikation.*

Die Virenverbreitung per E-Mail ist nach wie vor einer der häufigsten Angriffsvektoren, und die Anwender sollten beim Öffnen von E-Mail-Anhängen vorsichtig sein. Dateien mit der Endung .exe usw., bei denen es sich nicht um reine Datenformate handelt, sollte man immer mit Argwohn begegnen, es sei denn, Sie erwarten eine Datei von einem Ihnen bekannten Absender und können die Zulässigkeit des Anhangs telefonisch oder über andere Computer-unabhängige Wege überprüfen.

4) *Ausführung oder Installation eines allem Anschein nach harmlosen Programms, das eine bösartige Ladung befördert.*

³Dabei wird vorausgesetzt, dass ein Anwender in Windows XP als Administrator angemeldet ist. In Windows Vista wurde der Benutzerkontenschutz (UAC – User Account Control) eingeführt, um einen eingeschränkten Zugriff auf zulässige Aktionen zu ermöglichen, ohne die Programmberechtigungen auszuweiten.

Jede Komponente einer heruntergeladenen Anwendung kann Viren enthalten. Vor allem Freeware-Programme sind für eingebettete Spyware-Komponenten berüchtigt. Laden Sie vor allem ***niemals*** etwas von einer Warez-Website herunter.

Der proaktive Unterschied

Wie hilft der proaktive Schutz also, einen Malware-Befall zu verhindern?

Der größte Teil der Vorgänge zwischen verschiedenen Programmen findet unter der Aufsicht von Tools statt, die die Programmaktivitäten kontrollieren. Dadurch kann der Anwender entscheiden, welche Art von Aktivität zugelassen und welche blockiert werden soll. Die Anwender können unzulässige Aktivitäten so im Voraus verhindern, indem sie proaktiv danach Ausschau halten und verhindern, dass Malware aktiv wird, kommuniziert oder sich über den geschützten Computer hinaus verbreitet. Reaktive, signaturbasierte Anti-Malware-Produkte werden dieser Aufgabe nicht gerecht; sie können lediglich desinfizieren oder bereits infizierte Objekte entfernen.

Die Outpost-Lösung

Die Outpost Security Suite Pro verfügt über ein Host-Schutz-Modul, mit dem die Anwender die Programmaktivitäten überwachen und den Aktionsspielraum jedes Programms einschränken können. Mit dem Host-Schutz können Anwender den installierten Programmen benutzerdefinierte Einstellungen zuweisen, die u.a. festlegen, welche Programme mit anderer Software interagieren und Systemeinstellungen ändern dürfen. Das trägt dazu bei, unzulässige Aktivitäten jedes Programms auf einem PC zu verhindern – so wird der Malware-Scan eher zu einem sekundären als zum hauptsächlichen Verteidigungsmechanismus.

Die Anwender können selbst entscheiden, welche Aktivitäten das Modul überwachen und kontrollieren soll und sie können ihre eigene Liste von vertrauenswürdigen Anwendungen zusammenstellen.

Um dieses Modul in Aktion zu sehen und einen echten Eindruck davon zu bekommen, wie es Sicherheitsbedrohungen entgegentritt, indem es verdächtiges Verhalten einfach überwacht und meldet, sehen Sie sich dieses englischsprachige [Video](#) mit dem Titel Proaktiver Schutz an.

Schlussfolgerungen

Der proaktive Schutz ist ein Schlüsselement jeder PC-Verteidigungsstrategie. Durch die Überwachung unzulässigen Verhaltens kann er die Anfälligkeit des Computers für Bedrohungen beträchtlich verringern, ohne sich dabei komplett auf die Aktualität und Genauigkeit von Signatur-Datenbanken zu verlassen.