Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

- Überblick
- Funktionsweise
- Tipps

Virenschutz

Überblick

Als Virenschutz werden Sicherheitsprogramme bezeichnet, die Sie auf Ihrem Computer oder Mobilgerät installieren um es vor der Infektion durch Schadsoftware (engl. malware - eine Kombination aus malicious (schadhaft) und software) zu schützen. “Schadsoftware” ist hier ein weit gefasster Begriff, der sämtliche bösartige Software, wie Viren, Trojaner und sog. Spyware beschreibt. Wenn Ihr Computer mit Schadsoftware infiziert ist, kann ein Cyberkrimineller Ihre Tastenanschläge mitschreiben, Dokumente stehlen oder Ihren Computer nutzen um Andere anzugreifen. Im Gegensatz zum häufig vorherrschenden Glauben kann jedes Betriebssystem, eingeschlossen Mac OS X und Linux, derart infiziert werden.

Gastautor

Jake Williams ist der Gründer von Rendition Infosec (**www.renditioninfosec.com**) und ein zertifizierter SANS Ausbilder und Kursautor. Auf Twitter ist er als **@MalwareJake** zu finden und führt ein Blog unter **malwarejake.blogspot.com**.

Sie können Virenschutz-Programme als eigenständiges Produkt kaufen, oft sind diese jedoch Bestandteil eines ganzen Pakets von Sicherheitssoftware. Die Virenschutz-Technologie steht derzeit vor dem Problem, nicht länger mit den Cyberkriminellen mithalten zu können, die fortwährend neue Arten von Schadsoftware entwickeln und veröffentlichen. Jeden Tag werden so viele neue Versionen von Schadsoftware veröffentlicht, dass kein Virenschutz-Programm sie alle erkennen und davor schützen kann. Daher ist es so wichtig dass Sie verstehen, dass Virenschutz-Programme Ihren Computer zwar bis zu einem gewissen Grad, jedoch nicht vor allen Arten von Schadsoftware schützen können. Um das zu verdeutlichen sehen wir uns im Folgenden an, wie diese Programme arbeiten.

Funktionsweise

Virenschutz-Programme können Schadsoftware auf zwei verschiedene Arten erkennen: mit signatur- oder verhaltensbasierter Erkennung. Signaturbasierte Erkennung funktioniert wie das menschliche Immunsystem. Es durchsucht Ihren Computer nach Charakteristika oder Signaturen von bekannt schadhaften Programmen. Hierbei vergleicht es die auf dem Computer gespeicherten Dateien mit einer Sammlung von Signaturen bekannter Schadsoftware. Wenn etwas auf Ihrem Computer einem Muster in dieser Sammlung gleicht, versucht es die Bedrohung zu neutralisieren. Wie das menschliche Immunsystem benötigt auch dieser Ansatz regelmäßige Aktualisierungen, vergleichbar mit einer Auffrischimpfung, um gegen neue Stämme von Schadsoftware zu schützen. Virenschutz-Programme können nur vor etwas schützen, das sie als schädlich erkennen. Cyberkriminelle erstellen neue Schadsoftware jedoch so schnell, dass die Hersteller von Virenschutz-Programmen damit nicht mehr Schritt halten können. Ganz gleich wie häufig Sie Ihre Virenschutz-Produkte auch aktualisieren, es wird immer irgendeine neue

Virenschutz

Schadsoftware-Abwandlung geben, die möglicherweise an der Erkennung vorbeischlüpft.

Mit verhaltensbasierter Erkennung versucht die Virenschutz-Software nicht, bekannten Schadcode zu erkennen, sondern beobachtet das Verhalten der Software die auf Ihrem Computer installiert ist. Sobald sich ein Programm verdächtig verhält, es also zum Beispiel versucht auf geschützte Dateien zuzugreifen oder ein anderes Programm zu manipulieren, erkennt dies die verhaltensbasierte Erkennung und informiert Sie darüber. Dieser Ansatz bietet einen Schutz vor jeglicher, auch brandaktueller, Schadsoftware, die noch in keiner Sammlung enthalten ist. Das Problematische hieran ist jedoch, dass Falscherkennungen auftreten können. Sie, als Computernutzer, müssen daher oft eine Entscheidung treffen, was Sie zulassen oder unterbinden wollen. Es kann passieren, dass Sie mit der Zeit gegenüber derartigen Warnungen abstumpfen. Sie werden wahrscheinlich versucht sein, einfach bei jeder dieser Meldungen “Annehmen” zu klicken, womit Sie jedoch Ihren Computer Angriffen und Infektionen ungeschützt aussetzen. Hinzu kommt, dass zum Zeitpunkt der Erkennung die Schadsoftware auf Ihrem System bereits ausgeführt wurde und möglicherweise bereits schädliche Aktivitäten durchgeführt hat, bevor sie vom Virenschutz-Programm erkannt wurde.

Virenschutz-Programme sind ein wichtiger Baustein der Computersicherheit, können jedoch nicht alle Angriffe erkennen oder unterbinden. Letztendlich sind Sie der beste Schutz, nicht die Technologie.

Virenschutz ist ein wichtiger Baustein um Ihren Computer und Ihre Mobilgeräte abzusichern, deshalb empfehlen wir die Nutzung wann immer dies möglich ist. Der wichtigste Punkt ist jedoch, dass unabhängig von der Güte Ihres Virenschutz-Produkts nie ein hundertprozentiger Schutz möglich ist. Letztendlich liegt es bei Ihnen selbst, nicht nur bei der Technologie, sich gegen heutige Cyberkriminelle zu wehren.

Virenschutz Tipps

1. Beziehen Sie Virenschutz-Programme nur von bekannten, vertrauenswürdigen Quellen und Anbietern. Es ist eine gängige Masche von Cyberkriminellen, gefälschte Virenschutz-Produkte zu verteilen, bei denen es sich in Wahrheit um Schadsoftware handelt.
2. Stellen Sie sicher, die neueste Version Ihrer Virenschutz-Software installiert zu haben, dass diese noch über ein gültiges Abonnement verfügt und so eingestellt ist, automatisch Aktualisierungen zu beziehen. Wenn Ihr Computer für längere Zeit ausgeschaltet oder vom Internet oder Firmennetz getrennt war, wird Ihre Virenschutz-Software nach dem Start einige Zeit brauchen um sich zu aktualisieren. Verschieben Sie diese Aktualisierungen nicht!
3. Achten Sie darauf, dass Ihre Virenschutz-Software automatisch auch tragbare Medien (z.B. USB Sticks) überprüft und dass die Echtzeitüberwachung aktiviert ist.

Virenschutz

4. Achten Sie auf eingeblendete Warnungen und Alarme, die Ihre Virenschutz-Software generiert. Die meisten Meldungen enthalten die Möglichkeit, weitere Details zur Erkennung oder eine Handlungsempfehlung abzurufen. Wenn Sie eine Warnmeldung auf einem dienstlichen Computer erhalten, kontaktieren Sie umgehend Ihren Vorgesetzten oder den zuständigen Servicedesk.
5. Deaktivieren oder Entfernen Sie Ihre Virenschutz-Software nicht, nur weil Sie den Eindruck haben, sie verlangsamt Ihren Computer, unterbindet den Zugriff auf eine Webseite oder die Installation eines Programms. Das Deaktivieren Ihrer Virenschutz-Software setzt Sie einem unnötigen Risiko aus, das zu einem ernstzunehmenden Sicherheitsvorfall werden kann. Wenn auf Ihrem dienstlichen Computer Probleme bestehen, wenden Sie sich an das zuständige Servicedesk. Wenn Sie mit Ihrem Privatcomputer Probleme haben, versuchen Sie den Hersteller der Virenschutz-Software zu kontaktieren, besuchen Sie dessen Webseite für weiterführende Informationen oder ersetzen Sie das Virenschutz-Produkt durch das eines anderen Herstellers.
6. Betreiben Sie nicht gleichzeitig mehrere Virenschutz-Programme auf Ihrem Computer. Dies wird höchstwahrscheinlich zu Konflikten zwischen den Programmen führen und die Sicherheit Ihres Computers dadurch letztendlich sogar verschlechtern.
7. Machen Sie sich mit den Warnungen Ihres Virenschutz-Programms vertraut. Cyberkriminelle können bösartige Webseiten erstellen, die sehr realistisch gefälschte Virenschutz-Warnungen anzeigen und anbieten, Ihren Computer zu “reparieren”. Das Anklicken derartiger Links oder Schaltflächen kann Ihren Computer jedoch schädigen.

Weiterführende Informationen

Vergleich von Virenschutz-Produkten: http://www.av-test.org/de/
Social Engineering: http://www.securingthehuman.org/ouch/2014#november2014
E-Mail Phishing Angriffe: http://www.securingthehuman.org/ouch/2013#february2013
Ich wurde gehackt, was nun?: http://www.securingthehuman.org/ouch/2014#may2014

Informieren Sie Sich

Abonnieren Sie den monatlichen OUCH! Security Awareness Newsletter, greifen Sie auf die OUCH! Archive zu und lernen Sie mehr über SANS Security Awareness Angebote unter http://www.securingthehuman.org.

Deutsche Ausgabe

OUCH! wurde aus dem Englischen übersetzt von Marek Kreul und René Wiedewilt. Beide arbeiten für das CERT eines deutschen IT-Dienstleisters und haben sich auf IT-Forensik spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

Redaktionsleitung: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis

