Kurzvorstellung

Schutz vor steganographischen Bedrohungen

Steganographie – die Kunst und Wissenschaft des verborgenen Schreibens – eignet sich auch in der digitalen Welt dazu, Informationen zu verbergen. So kann eine Nachricht in Bildern, Audiospuren, Videoclips oder Textdateien versteckt werden. Dies kann zwar auch zu legitimen Zwecken erfolgen, wird aber viel öfter von Malware eingesetzt.

Einige Malware-Varianten setzen Steganographie ein, um ihren böswilligen Inhalt innerhalb einer anscheinend harmlosen Datei zu verbergen und so der Entdeckung zu entgehen. Diese Umgehungstechnik funktioniert deshalb, weil die meisten Malware-Schutzprodukte mithilfe von Signaturen in der Malware-Konfigurationsdatei nach böswilligen Inhalten suchen. Bei Steganographie wird die Konfigurationsdatei in der harmlosen Datei eingebettet. Außerdem ist es möglich, die resultierende steganographische Datei in den Arbeitsspeicher zu entschlüsseln, was die Wahrscheinlichkeit einer Entdeckung weiter verringert. Und letztendlich ist es außerordentlich schwierig, überhaupt zu erkennen, dass versteckte Informationen (z. B. eine Konfigurationsdatei, ein Update für eine Binärdatei oder Bot-Befehle) in steganographischen Dateien vorhanden sind. Leider ist Steganographie in Cyber-Angriffen leicht zu implementieren, aber schwer zu entdecken.

Richtlinien und Vorgehensweisen zum Schutz vor steganographischen Angriffen

McAfee empfiehlt die folgenden Maßnahmen zum Schutz vor steganographischen Bedrohungen.

- **Verschärfen Sie die Software-Übertragungs- und -Verteilungsmechanismen, die zum Schutz vor Insider-Bedrohungen dienen.** Es empfiehlt sich auch immer, über ein zentrales Repository mit vertrauenswürdigen Unternehmensanwendungen zu verfügen, aus dem die Benutzer genehmigte Software herunterladen können. Den Benutzern sollte nicht erlaubt werden, riskante Software aus zweifelhaften Quellen herunterzuladen, die möglicherweise steganographischen Code enthalten.

McAfee™
Together is power.

- **Passen Sie bei Bildern besonders auf.** Suchen Sie mithilfe von Bildbearbeitungs-Software nach Hinweisen auf Steganographie, z. B. leichte Farbunterschiede in Bildern oder zahlreiche doppelt vorhandene, identische Farben in der Farbpalette eines Bildes.
- **Kontrollieren Sie die Verwendung steganographischer Software streng.** Sofern nicht für geschäftliche Zwecke erforderlich, sollte die Anwesenheit steganographischer Software auf Firmensystemen generell verboten sein. Stellen Sie diese Software nur in einem abgeschlossenen Netzwerksegment bereit.
- **Lassen Sie nur vertrauenswürdige Signaturen zu.** Installieren Sie nur Anwendungen, die über vertrauenswürdige Signaturen von vertrauenswürdigen Anbietern verfügen.
- **Konfigurieren Sie Ihre Malware-Schutz-Software so, dass sie auch Binder erkennt.** Malware-Schutz-Software sollte so konfiguriert werden, dass sie die Anwesenheit von Bindern erkennt, die steganographische Bilder enthalten könnten.
- **Segmentieren Sie das Netzwerk.** Für den Fall eines erfolgreichen steganographischen Angriffs können vertrauenswürdige Virtualisierungsarchitekturen in Kombination mit einer geeigneten Netzwerksegmentierung helfen, einen Ausbruch einzudämmen, da Anwendungen dank des sicheren sowie nachprüfbaren Startvorgangs virtualisierter Systeme und der kontinuierlichen Überwachung des Netzwerkdatenverkehrs leichter isoliert werden können.
- **Überwachen Sie ausgehenden Datenverkehr.** Durch die Überwachung des ausgehenden Datenverkehrs können Sie erkennen, ob Ihre Systeme erfolgreich mit steganographischen Methoden angegriffen werden.

So schützen McAfee-Produkte vor steganographischem Code in Malware-Angriffen

McAfee Endpoint Security

Bedrohungsschutz

Vergewissern Sie sich, dass McAfee Endpoint Security (ENS) so konfiguriert ist, dass es vor allen bekannten Bedrohungen schützt, die möglicherweise steganographischen Code enthalten:

- Halten Sie McAfee ENS immer auf dem neuesten Stand (inklusive Patches, DAT-Version und Scan-Modul).
- Stellen Sie sicher, dass alle Systeme in Ihrer Umgebung geschützt sind und aktualisiert werden.
- Legen Sie fest, dass bei Zugriff ein Echtzeit-Scan durchgeführt wird, damit alle Dateien bei Lese- und Schreibzugriffen gescannt werden. Deaktivieren Sie niemals Echtzeit-Scans bei Lesezugriffen (mögliche Ausnahme: während der Konfiguration von Prozessen mit einem niedrigen Risikopotential).
- Ausnahmeregeln für Scan-Vorgänge sollten so wenig wie möglich und nur dort eingesetzt werden, wo dies wirklich erforderlich ist. Wenn der Verdacht einer Malware-Infektion besteht, sollten unbedingt sämtliche Scan-Ausnahmen vorübergehend deaktiviert werden. Informationen zum Einrichten von Scan-Ausnahmen finden Sie im Wissensdatenbank-Artikel KB88595.
- Sie können mit den Konfigurationen vom Typ „Hohes Risiko/Standard/Geringes Risiko“ die Angriffsfläche für steganographische Bedrohungen begrenzen. Lesen Sie nach, wie sich diese Einstellungen in stark genutzten Umgebungen oder in Umgebungen mit minimaler Hardware-Sicherheit auf die Leistung auswirken können. Weitere Informationen zur Verbesserung der Leistung mit McAfee Endpoint Security finden Sie im Artikel KB88205.
- Konfigurieren Sie McAfee ENS so, dass die Dateireputationsfunktion von McAfee Global Threat Intelligence (GTI) verwendet wird. Mit dieser Technologie können Sie die Lücke zwischen Zero-Day-Bedrohungen und signaturbasierten Erkennungen schließen. Informationen zu empfohlenen Einstellungen für die Dateireputationsfunktion von McAfee GTI finden Sie im Wissensdatenbank-Artikel KB74983, weitere Details im Artikel KB53735.

- Konfigurieren Sie McAfee ENS-Zugriffsschutzregeln so, dass keine autorun.inf-Dateien erstellt werden können.
- Verwenden Sie Zugriffsschutzregeln, um die Installation unbekannter Bedrohungen zu verhindern.

Web-Kontrolle

McAfee ENS Web-Kontrolle basiert auf den Web-Reputations- und Web-Kategorisierungsdiensten von McAfee GTI. Steganographisch infizierte Software befindet sich häufig auf Webseiten, die der Verteilung von Malware dienen.

McAfee ENS Web-Kontrolle stellt – bevor Sie eine Webseite besuchen – fest, ob diese als Host für Malware dient, von Malware infiziert ist oder unangemessene Inhalte enthält.

McAfee Web-Kontrolle:

- Zeigt mithilfe eines Farbschemas und mit Symbolen an, wie relativ sicher Webseiten sind:
  - Grün = Sicher (sehr geringes oder kein Risiko)
  - Gelb = Vorsicht! (geringes Risiko)
  - Rot = Warnung! (ernstes Risiko)
  - Grau = Unbekannt (noch nicht bewertet, bitte vorsichtig sein)
  - McAfee Secure = Täglich auf Hacker-Schwachstellen getestet
- Kann per McAfee ePolicy Orchestrator unkompliziert bereitgestellt und konfiguriert werden.
- Stellt eine weitere Schutzschicht für Endgeräte bereit und kann mit Internet Explorer, Firefox sowie Chrome verwendet werden.
- Verhindert mithilfe eines effektiven Spam-Schutzes, dass böswillige E-Mails in Netzwerke gelangen.

Mehr dazu: McAfee Endpoint Security-Produkthandbuch – Verwenden der Webkontrolle

Adaptiver Bedrohungsschutz

- Aktivieren Sie McAfee Real Protect, um mithilfe von Machine Learning-Techniken hochentwickelte Bedrohungen sowohl anhand ihres Aussehens sowie am möglichen Verhalten (Analyse vor der Ausführung) als auch am tatsächlichen Verhalten (dynamische Verhaltensanalyse) zu erkennen. Hierfür werden keine Signaturen benötigt. Weitere Informationen: Adaptiver Bedrohungsschutz – Real Protect)
- Implementieren Sie die McAfee-Funktion zur dynamischen Eindämmung von Anwendungsprozessen, und befolgen Sie dabei die empfohlenen Vorgehensweisen. Mehr dazu: KB87843.

McAfee VirusScan® Enterprise

Wenn Sie nicht die neueste Version von McAfee ENS implementiert haben, vergewissern Sie sich, dass McAfee VirusScan Enterprise (VSE) so konfiguriert ist, dass es vor allen bekannten Bedrohungen schützt, die möglicherweise steganographischen Code enthalten:

- Halten Sie McAfee VSE immer auf dem neuesten Stand (inklusive Patches, DAT-Version und Scan-Modul).
- Stellen Sie sicher, dass alle Systeme in Ihrer Umgebung geschützt sind und aktualisiert werden.
- Legen Sie fest, dass bei Zugriff ein Echtzeit-Scan durchgeführt wird, damit alle Dateien bei Lese- und Schreibzugriffen gescannt werden. Deaktivieren Sie niemals Echtzeit-Scans bei Lesezugriffen (mögliche Ausnahme: während der Konfiguration von Prozessen mit einem niedrigen Risikopotential).

- Ausnahmeregeln für Scan-Vorgänge sollten so wenig wie möglich und nur dort eingesetzt werden, wo dies wirklich erforderlich ist. Wenn der Verdacht einer Malware-Infektion besteht, sollten unbedingt sämtliche Scan-Ausnahmen vorübergehend deaktiviert werden. Informationen zum Einrichten von Scan-Ausnahmen finden Sie im Wissensdatenbank-Artikel KB50998.
- Setzen Sie in stark genutzten Umgebungen oder in Umgebungen mit minimaler Hardware-Sicherheit Konfigurationen vom Typ „Hohes Risiko/Standard/Geringes Risiko“ ein, um die Angriffsfläche für steganographische Bedrohungen zu begrenzen. Grundlagen zu dieser Funktion finden Sie im Wissensdatenbank-Artikel KB55139, Informationen zu deren Konfiguration im Artikel KB58692.
- Konfigurieren Sie McAfee VSE so, dass die Dateireputationsfunktion von McAfee Global Threat Intelligence (GTI) verwendet wird. Mit dieser Technologie können Sie die Lücke zwischen Zero-Day-Bedrohungen und signaturbasierten Erkennungen schließen. Informationen zu empfohlenen Einstellungen für die Dateireputationsfunktion von McAfee GTI finden Sie im Wissensdatenbank-Artikel KB74983, weitere Details im Artikel KB53735.
- Konfigurieren Sie McAfee VSE-Zugriffsschutzregeln so, dass keine autorun.inf-Dateien erstellt werden können.
- Verwenden Sie Zugriffsschutzregeln, um die Installation unbekannter Bedrohungen zu verhindern.

McAfee Application Control
McAfee Application Control blockiert effektiv nicht autorisierte Anwendungen sowie Code auf Servern, Desktop-Rechnern von Unternehmen und Geräten mit festen Funktionen. McAfee Application Control verhindert die Kompromittierung von Dateien und stoppt die Ausbreitung von Dateiinfektoren über das Netzwerk.

McAfee Application Control bietet Schutzfunktionen für zwei Bereiche:

- **Dateibasierter Schutz:** Schützt vor dateibasierten Angriffen, die für steganographische Angriffe typisch sind. Im Rahmen solcher Angriffe kann es zu Versuchen kommen, neue Anwendungen auszuführen oder aktuelle Anwendungen zu modifizieren.
- **Speicherschutz:** Schützt vor RAM-basierten Angriffen, die aus dem Internet, über das Netzwerk oder vom lokalen System aus (infolge einer Dateiausführung) stattfinden können.

Dateibasierter Schutz
Anwendungen, die nicht in der Whitelist aufgeführt sind, sind weder autorisiert noch geschützt. Anwendungen dagegen, die auf der Whitelist stehen, sind sowohl autorisiert als auch geschützt. Wenn ein nicht autorisiertes Element auf ein Endgerät gelangt (z. B. per Download, Netzwerkzugriff oder lokal per Flash- oder CD-Laufwerk), kann es zwar auf das Endgerät kopiert, dort geändert oder zwischen Ordnern auf dem Endgerät verschoben, aber niemals ausgeführt werden. Nachfolgend sind einige Beispiele für Ereignisse dieser Art aufgeführt.

Ausführung verweigert	Es wird versucht, eine Anwendung auszuführen, die in der Whitelist nicht aufgeführt ist. Die Ausführung wird von McAfee Application Control jedoch verhindert.
ActiveX-Installation verhindert	McAfee Application Control verhindert Versuche, nicht autorisierte ActiveX-Steuerelemente zu installieren.

Wenn ein nicht autorisierter Prozess (z. B. ein Prozess, der aus einer böswilligen Datei stammt, die auf einem Remote-Endgerät ausgeführt wird) oder ein nicht autorisierter Benutzer versucht, eine per Whitelist geschützte Datei zu modifizieren, umzubenennen, zu verschieben oder zu löschen, wird dieser Vorgang von McAfee Application Control unterbunden. Nachfolgend sind einige Beispiele für Ereignisse dieser Art aufgeführt.

Schreiben in Datei verweigert	McAfee Application Control hält einen nicht autorisierten Prozess davon ab, eine in der Whitelist aufgeführte Anwendung zu modifizieren.
Paketänderung verhindert	McAfee Application Control verhindert, dass eine Anwendung mithilfe eines MSI-basierten Installationspakets auf nicht autorisierte Weise installiert, modifiziert oder entfernt wird.

Mehr dazu: Empfohlene Vorgehensweisen zu McAfee Application Control

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense (ATD) findet mit seinem innovativen, mehrschichtigen Ansatz verborgene, hochentwickelte Packer, verschlüsselte Schaddaten und Zero-Day-Malware. Hierfür kombiniert die Lösung Schutzmaßnahmen mit geringem Ressourcenverbrauch (Malware-Schutzsignaturen, Reputationsdaten und Echtzeitemulation) mit gründlicher statischer Code-Überprüfung sowie dynamischer Analyse (Sandboxing), um das Verhalten von Malware zu analysieren.

Mehr dazu: Häufige Fragen zu McAfee Advanced Threat Defense

Weitere Informationen

McAfee Security Advice Center: Schutz vor Phishing

Dashboard zur Bedrohungslage: Das Sundown-Exploit-Kit wurde Ende 2016 aktualisiert und setzt nun Steganographie ein, um Exploit-Code zu verbergen

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/de