Kurzvorstellung

Schutz vor Adobe Flash-Exploits

Die Multimedia- und Software-Plattform Adobe Flash ist sehr beliebt, wenn es um die Präsentation umfangreicher webbasierter Inhalt wie Spiele, Webseiten, Anwendungen und mehr geht. Ihre Popularität macht sie jedoch auch zu einem attraktiven Ziel für Internetkriminelle, die neue, ungepatchte Schwachstellen skrupellos ausnutzen, um arglose Benutzer zu kompromittieren.

Verbreitung der Ausnutzung von Adobe Flash-Schwachstellen

Flash-Exploits werden ausführlich im ***McAfee Labs Threat-Report vom Mai 2015*** vorgestellt. Anfang des 4. Quartals 2014 nahm die Ausnutzung von Flash erheblich zu. Inzwischen gehören Flash-Schwachstellen zu den Hauptzielen von Exploit-Autoren. McAfee Labs zufolge hat dies folgende Ursachen: Es werden immer neue Flash-Schwachstellen entdeckt, Software-Patches zur Behebung der Schwachstellen werden von den Benutzern zu spät installiert, die Schwachstellen werden mit immer neuen, kreativeren Methoden ausgenutzt, es gibt immer mehr Mobilgeräte, die SWF-Dateien wiedergeben können, und schließlich sind Flash-Exploits schwer zu erkennen.

Von allen Exploit-Kits, die Flash-Exploits verbreiten, ist Angler am beliebtesten. Bei diesem leistungsstarken Kit, das ausführlich im ***McAfee Labs Threat-Report vom Februar 2015*** beschrieben wurde, handelt es sich um ein benutzerfreundliches Standard-Toolkit, mit dem über Schwachstellen verschiedenste Schaddaten verbreitet werden können.

Schutz vor Flash-Exploits

Beachten Sie die folgenden Richtlinien und Verfahrensweisen, um sich vor Flash-Exploits zu schützen:

- Aktivieren Sie die automatische Update-Funktion ihres Betriebssystems, oder laden Sie die Betriebssystem-Updates regelmäßig herunter, um Ihr Betriebssystem mit Patches für bekannte Sicherheitslücken zu aktualisieren.
- Konfigurieren Sie Ihre Virenschutz-Software so, dass Anhänge mit SWF-Erweiterung blockiert werden.
- Die Sicherheitseinstellungen des Browsers sollten mindestens auf die mittlere Stufe festgelegt werden.
- Installieren Sie ein Browser-Plug-In, das die Ausführung von Skripten und iFrames verhindert.
- Installieren Sie keine Browser-Plug-Ins, denen Sie nicht vertrauen.

intel Security

- Seien Sie äußerst vorsichtig, wenn Sie Anhänge öffnen, besonders wenn sie die Endung SWF haben.
- Öffnen Sie niemals eine E-Mail, die Ihnen unverlangt zugesendet wurde oder einen unerwarteten Anhang enthält – auch dann nicht, wenn die E-Mail von einem bekannten Absender stammt.
- Fallen Sie nicht auf Phishing-Versuche in Spam-Mails herein. Klicken Sie nicht auf Links in E-Mails oder Textnachrichten.
- Fügen Sie die URLs manuell durch Tippen oder Kopieren in die Adresszeile des Browsers ein, und prüfen Sie die Adresse, statt einfach auf eine Web-Anzeige zu klicken.
- Klicken Sie nicht auf Flash-Filme, die sich auf nicht vertrauenswürdigen Webseiten befinden.

So kann Intel Security vor Flash-Exploits schützen

McAfee Web Gateway

Malvertising, Drive-by-Downloads und böswillige URLs, die in vertrauenswürdige Webseiten eingebettet sind, sind nur einige der Angriffsmethoden, die Flash-Exploits nutzen. Der zuverlässige **McAfee Web Gateway** dehnt den Schutz Ihres Unternehmens auf diese Art der Bedrohung aus.

- **McAfee Gateway Anti-Malware Engine:** Die signaturlose Absichtsanalyse filtert in Echtzeit gefährliche Inhalte aus dem Web-Datenverkehr heraus. Emulation und Verhaltensanalyse bieten präventiven Schutz vor Zero-Day-Bedrohungen und gezielten Angriffen. McAfee Gateway Anti-Malware Engine untersucht Dateien und blockiert das Herunterladen durch den Benutzer, falls sich die Dateien als böswillig erweisen.
- **Integration von McAfee Global Threat Intelligence (McAfee GTI):** Der Echtzeit-Datendienst McAfee GTI bietet Datei- und Web-Reputation sowie Web-Kategorisierungsinformationen und schützt so vor den neuesten Bedrohungen, da McAfee Web Gateway alle Verbindungsversuche zu bekannt böswilligen Webseiten sowie zu Webseiten blockiert, die böswillige Werbe-netzwerke nutzen.

McAfee Application Control

Mit **McAfee Application Control** kann Ihr Unternehmen kontrollieren, welche Anwendungen in Ihrer Umgebung ausgeführt werden. Dabei kommen dynamische Whitelists und Durchsetzungsrichtlinien für vernetzte und eigenständige Endgeräte zum Einsatz. Der Schutz Ihres Unternehmens vor anfälligen Anwendungen wie veralteten Flash-Installationen spielt eine entscheidende Rolle bei der Bekämpfung der immer häufiger auftretenden Flash-Exploits.

- **Dynamische Whitelists:** Damit kann Ihr Unternehmen Anwendungen, die auf einer Whitelist geführt werden, effektiv verwalten, indem die Whitelist automatisch erweitert wird, sobald die Systeme gepatcht und aktualisiert werden. McAfee Application Control verringert die Anfälligkeit für Flash-Exploits, weil es die Ausführung ungepatchter Flash-Versionen in Ihrer Umgebung unterbindet.
- **Datei-Reputation:** Durch die Integration von McAfee GTI kann McAfee Application Control Echtzeitinformationen zu gefährlichen, ungefährlichen und unbekannten Dateitypen abrufen, sodass Ihr Unternehmen stets über neue Schwachstellen oder Angriffe von Anwendungen informiert ist, die möglicherweise geändert wurden.
- **Schutz mit und ohne Vernetzung:** Setzen Sie Kontrollen auf verbundenen oder getrennten Servern, virtuellen Maschinen, Endgeräten und Geräten mit fester Funktion wie Kassen-terminals durch.

McAfee Vulnerability Manager
McAfee Vulnerability Manager zeigt, wie anfällig Ihr Unternehmen durch alte Flash-Versionen in Ihrer Umgebung ist und welche effektiven Gegenmaßnahmen erforderlich sind.

- **Umfassende Schwachstellen-Scans:** McAfee Vulnerability Manager ist ein stark skalierbares eigenständiges Produkt für Host-Erkennung, Ressourcen-Management, Schwachstellenanalyse sowie Berichterstellung zu allen Geräten, die mit dem Netzwerk verbunden sind. McAfee Vulnerability Manager kann die Anfälligkeit Ihrer Umgebung für Flash-Exploits analysieren, indem es nach Systemen sucht, die anfällige Flash-Versionen ausführen.
- **Flexible Berichterstellung und Problembehebung:** McAfee Vulnerability Manager und **McAfee Asset Manager** arbeiten zusammen, um die automatisierte Überwachung und Verwaltung für Scans, Problembehebung, Durchsetzung und Berichterstellung bereitzustellen. Dadurch können Sie zeitaufwändige Alarmübungen, Ad-hoc-Prozesse sowie Fehler vermeiden und mehr Systeme effektiv schützen.
- **Überblick über Ihre Gefährdung:** McAfee Asset Manager zeigt Ihrem Unternehmen, welche Systeme für Flash-Exploits anfällig sind, indem Schwachstellen-Scans mit Scans zur Host-Erkennung korreliert werden. Durch die Echtzeiterkennung von Systemen, die anfällige Flash-Versionen ausführen, haben Sie erheblich schneller Sicherheit darüber, ob Sie gefährdet sind, und können schneller mit der Problembehebung beginnen.

McAfee Threat Intelligence Exchange
Sie benötigen eine Informationsplattform, die sich an Ihre Umgebung anpassen lässt. Dank der Erkennung unmittelbarer Bedrohungen wie unbekannter Dateien oder Anwendungen, die Flash-Schwachstellen in der Umgebung Ihres Unternehmens ausnutzen, kann **McAfee Threat Intelligence Exchange** die Anfälligkeit für diese Art von Angriffen erheblich verringern.

- **Umfassende Bedrohungsanalyse:** Die umfassenden Bedrohungsdaten von weltweiten Datenquellen können unkompliziert angepasst werden. Dabei kann es sich um Feeds von McAfee GTI oder Drittanbietern handeln, die mit lokalen Bedrohungsdaten aus Echtzeit- sowie Verlaufsereignissen kombiniert und über Endgeräte, Gateways sowie andere Sicherheitskomponenten weitergegeben werden.
- **Ausführungsschutz und Behebung:** McAfee Threat Intelligence Exchange kann unbekannte Anwendungen daran hindern, in der Umgebung ausgeführt zu werden. Wenn eine Anwendung, die sich später als böswillig herausstellt, zuvor ausgeführt wurde, kann McAfee Threat Intelligence Exchange die laufenden Prozesse dieser Anwendung in der gesamten Umgebung deaktivieren. Dabei greift die McAfee-Lösung auf ihre leistungsfähigen Funktionen zur zentralen Verwaltung und Richtliniendurchsetzung zurück.
- **Sichtbarkeit:** McAfee Threat Intelligence Exchange kann alle gepackten ausführbaren Dateien und deren Start in der Umgebung sowie alle anschließend stattfindenden Veränderungen verfolgen. Dieser Einblick in die Aktionen von Anwendungen oder Prozessen ab der Installation bis zum aktuellen Zeitpunkt ermöglicht schnellere Reaktionen und Behebungsmaßnahmen.
- **Kompromittierungsindikatoren:** Die Hash-Werte bekannt gefährlicher Dateien werden in McAfee Threat Intelligence Exchange importiert, um Ihre Umgebung mithilfe von Richtliniendurchsetzungen gegen diese Bedrohungen zu immunisieren. Wenn diese Kompromittierungsindikatoren in der Umgebung entdeckt werden, kann McAfee Threat Intelligence Exchange alle Prozesse und Anwendungen blockieren, die mit dem Indikator in Zusammenhang stehen.

McAfee VirusScan Enterprise

Mit **McAfee VirusScan® Enterprise** ist das Erkennen und Entfernen von Malware, die über Flash-Schwachstellen in Ihre Umgebung eindringt, äußerst einfach. McAfee VirusScan Enterprise nutzt das preisgekrönte McAfee-Scan-Modul zum Schutz Ihrer Dateien vor Viren, Würmern, Rootkits, Trojanern und anderen hochentwickelten Bedrohungen.

- **Präventiver Schutz vor Angriffen:** Durch die Verzahnung von Malware-Schutztechnologien und Eindringungsschutz können Exploits abgewehrt werden, die mithilfe von Buffer Overflows Schwachstellen in Anwendungen angreifen.
- **Unschlagbare Malware-Erkennung und -Bereinigung:** Die erweiterte Verhaltensanalyse schützt vor Bedrohungen wie Rootkits und Trojanern. Mithilfe von Techniken wie der Blockierung von Ports und Dateinamen, der Sperrung von Ordnern bzw. Verzeichnissen und Freigaben sowie der Verfolgung und Blockierung von Infektionen wird Malware schon im Ansatz aufgehalten.
- **Echtzeitsicherheit mit McAfee GTI:** Die Plattform für die branchenweit umfassendsten Bedrohungsdaten bietet Schutz vor bekannten und neuen Bedrohungen aus allen Sektoren – Dateien, Web, E-Mails und Netzwerk.

McAfee Global Threat Intelligence

McAfee Global Threat Intelligence (McAfee GTI) ist ein umfassender, in Echtzeit funktionierender und Cloud-basierter Bedrohungsanalysedienst, durch den McAfee-Produkte alle Bedrohungsvektoren blockieren können – Dateien, das Web, Nachrichten und das Netzwerk. McAfee GTI schützt proaktiv mithilfe der folgenden Funktionen vor Flash- und anderen Exploits:

- **Bedrohungsinformationen durch Vektorkorrelierung:** Erfasst und korreliert Daten von allen und für alle wichtigen Bedrohungsvektoren – Datei, Web, E-Mail und Netzwerk – zur Erkennung verschleierter Bedrohungen.
- **Plattform für umfassende Bedrohungsanalysen:** Erfasst Bedrohungsdaten von Millionen Sensoren auf McAfee-Produkten, die bei Kunden auf Endgeräten, Web-, E-Mail- und Netzwerk-eindringungsschutz-Systemen sowie Firewall-Geräten im Einsatz sind.
- **Security Connected:** Die Integration in andere McAfee-Sicherheitsprodukte ermöglicht die branchenweit umfassendsten Daten zu Bedrohungen, die zuverlässigste Korrelation dieser Daten und die vollständigste Produktintegration, damit der Schutz vor Flash-Exploits gewährleistet bleibt.

McAfee VirusScan Mobile

McAfee VirusScan Mobile ist ein System zum Schutz vor Malware. Es scannt und bereinigt mobile Daten und verhindert so eine Beschädigung der Daten durch Viren, Trojaner und anderen böswilligen Code. McAfee VirusScan Mobile schützt Ihre mobilen Geräte an den kritischsten Stellen: ein- und ausgehende E-Mails, Textnachrichten, E-Mail-Anhänge und Internet-Downloads.

- Bedrohungserkennung in Echtzeit: Blockieren Sie Malware in E-Mails, Textnachrichten und Anhängen ohne merkbare Verzögerung. McAfee VirusScan Mobile scannt Geräte innerhalb von weniger als 200 Millisekunden auf zahlreiche Bedrohungen und bietet automatischen und umfassenden Schutz für Smartphones.

Ein Ende der zunehmenden Ausnutzung von Flash-Schwachstellen durch Malware-Autoren ist nicht absehbar. Mit der Technologie von Intel Security kann sich Ihr Unternehmen präventiv vor Angriffen schützen, die diese Schwachstellen nutzen wollen.

McAfee. Part of Intel Security.
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com