Kurzvorstellung

Vertrauensmissbrauch

Die Ausnutzung der Vertrauensseligen

Das Sprichwort „Vertrauen kann nur verdient, nicht verschenkt werden“ beweist sich immer wieder, und wir alle kennen Beispiele dafür. Andererseits kann etwas, das über Jahre hinweg aufgebaut wurde, innerhalb von Sekunden zerstört werden. Vertrauenswürdigkeit war nie eine Konstante, und das zeigt sich immer deutlicher, seit die Menschen weltweit das Internet in immer stärkerem Maße nutzen.

Was ist Vertrauensmissbrauch?

Der Missbrauch der Vertrauenswürdigkeit wird ausführlich im **McAfee Labs Threat-Report vom November 2014** besprochen. In der Online-Welt gehen wir davon aus, dass das, was wir sehen, vertrauenswürdig ist. Dabei kann es sich um eine heruntergeladene App auf einem Mobilgerät, eine scheinbar legitime Werbung auf einer beliebten Webseite oder die E-Mail eines Unternehmens handeln, mit dem wir zu tun haben. Angreifer nutzen das etablierte Vertrauen auf vielfältige Weise aus, wobei die nichts ahnenden Opfer das Hauptziel sind. In diesem Bericht werden die folgenden Angriffstypen vorgestellt:

- **Malvertising:** Wenn sich scheinbar harmlose Werbung auf einer Unternehmenswebseite als Quelle des Angriffs auf nichts ahnende Kunden herausstellt, fragen sich diese zu Recht, ob ihr Vertrauen nicht fehl am Platz ist. **Böswillige Werbenetzwerke wie „Kyle and Stan“** liefern Malware über „Malvertisements“, also böswillige Werbung, auf Webseiten wie amazon.com, youtube.com und **großen Werbenetzwerken wie Double-Click und Zedo** aus.
- **Signierte Malware:** Immer häufiger erschleichen sich Malware-Autoren Zertifikate von einer Zertifizierungsstelle (Certificate Authority, CA), mit denen sie entweder die Vertrauenswürdigkeit bekannter Unternehmen ausnutzen oder sich als legitimes Unternehmen ausgeben. Die Angreifer nutzen also unser Vertrauen in CAs aus. Kürzlich wurden im Rahmen einer Malvertising-Kampagne signierte CryptoWall-Varianten über das Werbenetzwerk Zedo ausgeliefert. **Betroffen waren die Benutzer von Webseiten, die in der Rangliste von Alexa auf vordersten Plätzen geführt werden**. Die digitale Signatur war auf „Trend“ ausgestellt, was wahrscheinlich ein Versuch war, sich als der Sicherheitsanbieter Trend Micro auszugeben. Dies ist ein perfektes Beispiel für die Ausnutzung des Unschuld-durch-Zugehörigkeit-Prinzips.
- **Gefälschte Anwendungen:** Kommerzielle Unternehmen wenden viel Zeit und Mühe auf, um ihre Kunden vor gefälschten Produkten zu schützen, mit denen das Vertrauensverhältnis zwischen Kunden und Marke ausgenutzt werden soll. Da Anwendungen Funktionen bieten, die nicht nur auf die digitale Welt beschränkt sind, sind Angreifer wenig überraschend dazu übergegangen, gefälschte Varianten legitimer und meist beliebter Programme zu entwickeln.

intel Security

In diesem Quartal beobachtete McAfee, dass Betrüger eine Anwendung zu verbreiten versuchen, die sich als Adobe Flash Player 11 ausgibt. Die Download-Zahlen von Google Play und die Erkennungstelemetrie von McAfee Mobile Security legen nahe, dass die Kriminellen mit einigem Erfolg Benutzer dazu verleiten konnten, die böswillige Fälschung herunterzuladen.

- **DLL Side Loading:** Die Angreifer wissen, dass ihr Schadcode größeren Erfolg hat, wenn er sich an eine vertrauenswürdige Anwendung anhängt. Malware nutzt diese Tatsache schon seit einigen Jahren mithilfe einer Angriffstechnik namens DLL Side Loading aus. Bei dieser Technik wird eine legitime Anwendung ausgeführt, die Code aus einer externen DLL-Datei ausführt. Die Angreifer können ihren Schadcode so anpassen, dass er sich als externe DLL ausgibt, sodass die legitime Anwendung böswilligen Code ausführt.

  Im dritten Quartal beobachtete McAfee Labs Angriffe auf die Google Updater-Anwendung. Die neue Variante der PlugX-Malware-Familie nimmt die Rolle der importierten GOOPDATE.DLL an, doch PlugX geht beim Verbergen der eigenen Aktionen noch einen Schritt weiter. Das GOOPDATE.DLL-Modul ist lediglich ein Mittelsmann, der den Inhalt der verschlüsselten Datendatei GOOPDATE.DLL.MAP liest, sie im Arbeitsspeicher entschlüsselt und die Ausführungskontrolle an diesen böswilligen Code weitergibt.

- **Betriebssysteme und Netzwerk-Software:** Es gibt viele Beispiele für Angriffe, die die Vertrauenswürdigkeit innerhalb und zwischen Betriebssystemen und Netzwerk-Software missbrauchen. Einige nutzen die Tatsache aus, dass die Software sichere Verbindungen über das Internet herstellt. Arglose Anwendungen vertrauen diesen Verbindungen, die ihnen vom Betriebssystem zugewiesen werden, das wiederum der Netzwerk-Software vertraut, die diese scheinbar sicheren Verbindungen hergestellt hat. Andere Angriffe nutzen Schwachstellen in Betriebssystemen oder der Netzwerk-Software aus. Häufig nutzen diese Angriffe Open-Source-Software aus, die im Betriebssystem oder im Netzwerk-Software-Stack verwendet wird.

  BERserk ist eine **vor kurzem bekannt gegebene** Schwachstelle bei der Signaturüberprüfung, die das Vertrauen zwischen Betriebssystem und Netzwerk-Software ausnutzt. Mit BERserk können Angreifer Man-in-the-Middle-Attacken durchführen, indem sie RSA-Signaturen fälschen und die SSL/TLS-Authentifizierung von Webseiten aushebeln.

McAfee-Lösungen

Die Sicherheitstechnologien von McAfee können vor Angriffen schützen, bei denen das Vertrauen Ihres Unternehmens in die alltäglichen Betriebsabläufe missbraucht wird. Im Folgenden werden einige der McAfee-Produkte vorgestellt, mit denen Ihr Unternehmen gewährleisten kann, dass Ihr Vertrauensmodell nicht von potenziellen Angreifern ausgenutzt werden kann.

McAfee Application Control

Der Schutz Ihres Unternehmens und seiner legitimen Anwendungen vor böswilligem Code wie BERserk ist unverzichtbar. 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.

- **Dynamische Whitelist:** 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 Ihre Anfälligkeit für BERserk, indem die Ausführung von Anwendungen verhindert wird, die den anfälligen RSA-Signaturprüfungs-Code aufrufen.
- **Dateireputation:** Durch die Integration von McAfee Global Threat Intelligence kann McAfee Application Control Echtzeitinformationen zu gefährlichen, ungefährlichen und unbekannten Dateitypen abrufen, sodass Ihr Unternehmen stets über neue Schwachstellen wie BERserk informiert ist.

- **Schutz mit und ohne Vernetzung:** Setzen Sie Kontrollen auf verbundenen oder getrennten Servern, virtuellen Maschinen, Endgeräten und Geräten mit fester Funktion wie Kassenterminals durch.

McAfee Email Gateway

Eine wichtige Frage für Unternehmen ist, ob eine E-Mail im Posteingang eines Benutzers legitim ist oder mit böswilliger Absicht verschickt wurde. Angreifer versuchen mithilfe von Spearphishing-Methoden, nichts ahnende Opfer dazu zu verleiten, auf ihrer Seite die Kompromittierung durch eingebettete Malware oder böswillige URLs anzustoßen. **McAfee Email Gateway** bietet verschiedene Funktionen, die Schutz vor diesen Angriffen gewähren:

- **ClickProtect:** Diese Funktion wehrt Bedrohungen durch eingebettete URLs in E-Mails ab, indem die URLs zum Klick-Zeitpunkt gescannt werden. Dabei wird die URL-Reputation überprüft sowie eine proaktive Emulation mithilfe der McAfee Gateway Anti-Malware Engine durchgeführt.
- **Integration von McAfee Advanced Threat Defense:** Durch die statische und dynamische Code-Analyse verdächtiger Dateien, die an E-Mails angehängt sind, kann hochentwickelte und verschleierte Malware entdeckt werden, sodass böswillige Dateien den Posteingang erst gar nicht erreichen.
- **Integration von McAfee Global Threat Intelligence:** Durch die Kombination von Daten aus dem lokalen Netzwerk mit Reputationsinformationen, die über McAfee Global Threat Intelligence bereitgestellt werden, bietet die Lösung den lückenlosesten erhältlichen Schutz vor eingehenden Bedrohungen, Spam und Malware.

McAfee Global Threat Intelligence

McAfee Global Threat Intelligence (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 Vertrauensmissbrauch:

- **Zertifikatreputation:** Die Echtzeitabfrage bekannt guter oder gefährlicher Zertifikate schützt Ihr Unternehmen vor Bedrohungen wie signierte Malware, die durch böswillige Werbenetzwerke verteilt wird.
- **Dateireputation:** Diese Funktion schützt vor gefälschten Anwendungen auf dem Desktop und informiert Sie über Anwendungen, die für Angriffe wie BERserk anfällig sind. Dabei erfolgen die Abfragen zur Suche nach gefährlichen, ungefährlichen und unbekannten Dateien in Echtzeit.
- **Bedrohungsinformationen durch Vektorkorrelierung:** Erfasst und korreliert Daten von allen und für alle wichtigen Bedrohungsvektoren – Datei, Web, E-Mail und Netzwerk – zur Erkennung verschleierter Bedrohungen. Dazu gehören beispielsweise Werbenetzwerke, die signierte Malware verteilen, Spearphishing-E-Mails von scheinbar vertrauenswürdigen Quellen sowie Drive-by-Downloads, die auf böswilligen oder kompromittierten „vertrauenswürdigen“ Webseiten gehostet werden.
- **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 Angriffen auf die Vertrauenswürdigkeit gewährleistet bleibt.

McAfee Vulnerability Manager
Angriffe wie BERserk verdeutlichen den ständigen Wandel der Bedrohung für das Vertrauensmodell. Es kann zeitaufwändig und komplex sein zu erkennen, ob Sie für diese neuen Angriffe anfällig sind. Im Folgenden stellen wir einige Möglichkeiten vor, wie **McAfee Vulnerability Manager** zusammen mit **McAfee Asset Manager** Ihrem Unternehmen dabei helfen kann, Schwachstellen wie BERserk zu verstehen und die notwendigen Maßnahmen zu ihrer Beseitigung zu ergreifen:

- **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 nach BERserk suchen, indem die Lösung auf den Systemen überprüft, ob anfällige Versionen von Firefox, Chrome und anderen Produkten mit dem anfälligen RSA-Signaturprüfungs-Code verwendet werden.
- **Anpassung von Scans an neue Bedrohungen:** Der FSL-Editor (Foundstone Scripting Language) kann vordefinierte Überprüfungen und Aktualisierungen für Zero-Day-Bedrohungen und Schwachstellen wie BERserk verbessern, indem die Erstellung benutzerdefinierter Skripte und Überprüfungen zur Analyse Ihrer Umgebung ermöglicht wird. McAfee Vulnerability Manager kann seit dem 24. September 2014 mithilfe der vordefinierten Überprüfungen Systeme erkennen, die für BERserk anfällig sind.
- **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 BERserk anfällig sind, indem Schwachstellen-Scans mit Scans zur Host-Erkennung korreliert werden. Durch die Echtzeiterkennung von Systemen, die anfällige Anwendungsversionen ausführen, haben Sie erheblich schneller Sicherheit darüber, ob Sie gefährdet sind, und können schneller mit der Problembehebung beginnen.

McAfee Web Gateway
Malvertising, Drive-by-Downloads und böswillige URLs, die in vertrauenswürdige URLs eingebettet sind, sind nur einige der Angriffsmethoden, mit denen das Vertrauen missbraucht werden soll. **McAfee Web Gateway** dehnt den Schutz Ihres Unternehmens auf diese Art Bedrohungen 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. Die McAfee Gateway Anti-Malware Engine untersucht Dateien und blockiert das Herunterladen durch den Benutzer, falls sich die Dateien als böswillig erweisen. McAfee Web Gateway ist branchenweit einmalig, da die Lösung mithilfe ihres einzigartigen Untersuchungsmoduls Malware-Downloads blockieren kann.
- **Integration von McAfee GTI:** Der Echtzeitdienst 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 Werbenetzwerke nutzen.

McAfee SiteAdvisor® Enterprise

Es ist mit einigem Aufwand verbunden, der wandlungsfähigen Bedrohungssituation einen Schritt voraus zu bleiben. Dies gilt insbesondere dann, wenn Online-Benutzer vor Bedrohungen wie Vertrauensmissbrauch geschützt werden sollen, ohne dass ihnen dabei die Arbeit durch strikte Richtlinien erschwert wird.

- **Einfache Erkennung von Bedrohungen wie böswilligen Webseiten, die sich als legitim ausgeben:** Mit dem intuitiven farbcodierten Bewertungssystem bietet **McAfee SiteAdvisor Enterprise** eine zusätzliche Schutzebene für den Desktop. McAfee SiteAdvisor Enterprise blockiert alle Verbindungen zu bekannt böswilligen Webseiten und informiert die Benutzer über die Bedrohung.
- **Erweiterte Sicherheit durch McAfee GTI:** McAfee GTI stellt für McAfee SiteAdvisor Enterprise Echtzeitbedrohungsdaten bereit, sodass diese Lösung Webseiten anhand der aktuellsten Informationen einstufen kann.

McAfee Threat Intelligence Exchange

Vertrauensmissbrauch hat viele Gesichter, sodass eine Informationsplattform dringend notwendig ist, die sich im Laufe der Zeit an Ihre Umgebung anpassen lässt. Dank der Anzeige von Bedrohungen wie böswilligen Zertifikaten, die in Ihrer Umgebung gefunden wurden, verringert **McAfee Threat Intelligence Exchange (TIE)** Ihre Anfälligkeit für Angriffe erheblich.

- **Zertifikatreputation:** Durch die Integration von McAfee GTI kann sich Ihr Unternehmen in Echtzeit vor Bedrohungen schützen, die signierten Malware-Code verwenden. Dazu ruft der Dienst Echtzeitinformationen zu legitimen und gefährlichen Zertifikaten ab. Mithilfe zentral verwalteter Richtlinien, die zum Schutz vernetzter und eigenständiger Endgeräte ausgebracht werden können, kann McAfee TIE Ihre Endgeräte vor böswilligen Zertifikaten schützen.
- **Schutz vor DLL Side Loading, gefälschten Apps und anderen Angriffen:** Die innovative Endgeräteschutz-Technologie entscheidet anhand von Regeln, die sich auf den Endgerätekontext beziehen (Datei, Prozess und Umgebungsattribute), sowie anhand kollektiver Bedrohungsdaten über die Ausführung von Dateien.
- **Kompromittierungsindikatoren:** Die Hash-Werte bekannt gefährlicher Dateien sowie bekannt böswillige Zertifikate werden in McAfee TIE importiert, um Ihre Umgebung mithilfe von Richtliniendurchsetzungen gegen diese Bedrohungen zu immunisieren. Wenn diese Kompromittierungsindikatoren in der Umgebung entdeckt werden, kann McAfee TIE alle Prozesse und Anwendungen blockieren, die mit dem Indikator in Zusammenhang stehen.

McAfee VirusScan® Mobile Security

- **Schutz vor gefälschten Apps:** Dank der Unterstützung durch McAfee GTI schützt **McAfee VirusScan Mobile Security** beinahe in Echtzeit vor gefälschten Malware-verseuchten Anwendungen. Die Lösung entdeckt Malware innerhalb von weniger als 200 Millisekunden, ohne dass dafür der Wireless-Betrieb oder die drahtlose Verbindung unterbrochen werden.

Der Schutz Ihres Unternehmens vor Angreifern, die das dynamische Vertrauensmodell ausnutzen möchten, kann eine schwierige Aufgabe darstellen. Dank McAfee-Sicherheitstechnologien hat Ihr Unternehmen die Möglichkeit, sich präventiv vor Angriffen zu schützen, die das Vertrauen der Benutzer zu missbrauchen versuchen.

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