Inhalt

1. Mobilgeräte-Malware forciert im Jahr 2014 die Entwicklung technischer Innovationen bei Malware sowie die Zunahme von Angriffen.

Im Jahr 2013 überstieg die Zunahme neuer Mobilgeräte-Malware-Varianten, die sich fast ausschließlich auf die Android-Plattform konzentrierten, die Zunahme von Malware für PCs bei Weitem. In den letzten zwei Quartalen blieb das Wachstum von Malware für PCs nahezu konstant, während die Anzahl der Android-Malware-Varianten um 33 Prozent zunahm.

Während McAfee Labs davon ausgeht, dass sich diese Entwicklung im Jahr 2014 fortsetzt, werden wohl nicht nur die Zuwächse bei Mobilgeräte-Angriffen Schlagzeilen machen. Wir rechnen auch mit völlig neuen Arten von Angriffen auf Android. Sehr wahrscheinlich werden die ersten echten Ransomware-Angriffe auf Mobilgeräte erfolgen, bei denen wichtige Daten auf dem Gerät verschlüsselt und unter Lösegeldforderungen gesperrt werden. Die Informationen werden nur freigegeben, wenn das Opfer das geforderte Lösegeld entweder in konventioneller oder einer virtuellen Währung wie Bitcoin zahlt. Wir erwarten zudem neue Angriffsmethoden wie Attacken auf Schwachstellen in den Nahfeldkommunikationsfunktionen, die jetzt in vielen Geräten enthalten sind. Eine weitere Variante sind Attacken auf legitime Apps, um unbemerkt Daten abrufen zu können.

Angriffe auf Mobilgeräte zielen auch auf Unternehmensinfrastrukturen ab. Dabei nutzen sie die Tatsache aus, dass einerseits BYOD (Bring-Your-Own-Device) weit verbreitet ist und andererseits die Mobilgeräte-Sicherheitstechnologie noch nicht ausgereift ist. Dadurch gelangt von Benutzern unabsichtlich heruntergeladene Malware in das Unternehmensnetzwerk, wo sie vertrauliche Daten exfiltriert. Da Unternehmen nicht auf BYOD verzichten möchten, benötigen sie umfassende Richtlinien und Lösungen zur Geräteverwaltung.

2. Virtuelle Währungen fördern weltweit die Verbreitung von böswilliger Ransomware.

Ransomware-Angriffe, bei denen die Daten auf den Geräten der Opfer verschlüsselt werden, sind nichts Neues. Diese Angriffe wurden in der Vergangenheit jedoch durch Strafverfolgungsbehörden erschwert, die gegen die Zahlungsanbieter der Kriminellen vorgegangen sind.

CryptoLocker-Dialogfeld

Die zunehmende Nutzung virtueller Währungen hat positive Auswirkungen auf die Wirtschaft, bietet jedoch gleichzeitig die perfekte ungeregelte und anonyme Zahlungsinfrastruktur, über die Internetkriminelle das Geld ihrer Opfer eintreiben können. Wir erwarten, dass sich Angriffe wie CryptoLocker so lange weiter verbreiten, wie sie (sehr) hohe Profite versprechen. Ebenso rechnen wir mit Ransomware-Angriffen, die direkt auf Unternehmen abzielen und deren wichtigsten Datenressourcen verschlüsseln.

Die gute Nachricht für Einzelpersonen und Unternehmen besteht darin, dass die Wirkfunktion der Ransomware zwar einmalig ist, die Verbreitungsmechanismen (also Spam, Drive-by-Downloads und infizierte Apps) aber nicht. Wenn Verbraucher und Firmen darauf achten, dass ihre Malware-Schutzsysteme für Endgeräte und Netzwerke aktuell bleiben, sind sie vor dieser Bedrohung relativ gut geschützt. Mit einem zuverlässigen privaten oder unternehmensbasierten Backup-System können Opfer zudem die schwerwiegendsten Folgen von Ransomware vermeiden.

3. In der Halbwelt der Internetkriminalität und Internetkriegsführung setzen kriminelle Banden und staatliche Akteure auf neue Stealth-Angriffe, die noch schwerer erkannt und blockiert werden können.

Nicht nur die Informationssicherheitslösungen sind immer raffinierter geworden, auch die Internetkriminellen werden immer geschickter dabei, diese Schutzmaßnahmen zu umgehen. Angriffe mit hochentwickelten Umgehungstechniken gehören zu den neuesten Taktiken in den Schlachten des Datensicherheitskriegs gegen Unternehmen. Zu den beliebten Umgehungstechniken der Internetkriminellen werden im Jahr 2014 Angriffe mit Sandbox-Erkennung sein, die nur dann bis zu Ende durchgeführt werden, wenn die Malware glaubt, dass sie direkt auf einem völlig ungeschützten Gerät ausgeführt wird.

Im Jahr 2014 rechnen wir mit weiteren Angriffstechnologien, die ausgebaut und eingesetzt werden. Dazu gehören ROP-Angriffe (Return-Oriented Programming), bei denen legitime Anwendungen so verändert werden, dass sie böswillige Aktionen durchführen. Andere Varianten sind sich selbst löschende Malware, die nach der Kompromittierung des Opfers ihre eigenen Spuren verwischt, sowie hochentwickelte Angriffe auf dedizierte Industrieleitsysteme, die öffentliche und private Infrastrukturen gefährden können.

Politisch motivierte Angriffe werden zunehmen. Das gilt insbesondere während der Winterolympiade im Februar 2014 in Sotschi und der Fußballweltmeisterschaft im Juni und Juli in Brasilien. Zudem werden Hacktivisten diese Großereignisse nutzen, um ihre Botschaften zu verbreiten.

Die IT-Abteilungen der Unternehmen müssen auf diese neuen Entwicklungen reagieren, um sicherstellen zu können, dass die eingesetzte Verteidigung sich nicht ausschließlich auf Sicherheitsmaßnahmen verlässt, die von weltweit tätigen internetkriminellen Organisationen auf einfache Weise umgangen werden können.

4. Zum Ende des Jahres 2014 werden „soziale Angriffe" allgegenwärtig sein.

Angriffe auf soziale Netzwerke nutzen die große Benutzeranzahl von sozialen Plattformen wie Facebook, Twitter, LinkedIn und Instagram aus. Diese Angriffe verwenden dabei häufig die gleichen Taktiken wie ältere Malware-Varianten wie Koobface und missbrauchen die sozialen Plattformen als Verbreitungsmechanismus. Wir rechnen für das Jahr 2014 jedoch mit Angriffen, die die speziellen Funktionen dieser Plattformen dazu nutzen, Daten zu Benutzerkontakten, Standorten oder Geschäftsaktivitäten zu erlangen, die anschließend für gezielte Werbung oder Verbrechen in der virtuellen oder realen Welt missbraucht werden.

Eine der typischsten Angriffsmethoden auf die Plattformen besteht schlicht darin, die Benutzeranmeldedaten zu erfassen, mit denen persönliche Daten ahnungsloser Kontakte und Kollegen extrahiert werden können. Das Pony-Botnet[1], mit dem mehr als zwei Millionen Nutzerkennwörter von Facebook, Google, Yahoo! und anderen Anbietern kompromittiert wurden, ist wahrscheinlich nur die Spitze des Eisbergs. Facebook gibt selbst an, dass 50 bis 100 Millionen sogenannter MAU-Konten (Monthly Active User) in Wirklichkeit Duplikate sind und bis zu 14 Millionen der registrierten MAU-Benutzer als „unerwünscht" gelten. In einer kürzlich durchgeführten Stratecast-Umfage gaben 22 Prozent der Befragten an, bereits einen sicherheitsrelevanten Zwischenfall erlebt zu haben.[2]

Öffentliche ebenso wie private Unternehmen werden soziale Plattformen außerdem für „Spähangriffe" auf Wettbewerber und Rivalen nutzen. Diese Angriffe erfolgen entweder direkt oder über Dritte. Bereits im Jahr 2013 wurden große Organisationen im privaten und öffentlichen Bereich Ziel solcher Angriffe. Wir erwarten, dass die Häufigkeit und der Umfang solcher Attacken im kommenden Jahr zunehmen werden.

Wir rechnen für das Jahr 2014 jedoch mit einer weiteren häufigen Form sozialer Angriffe: Bei diesen Attacken „unter falscher Flagge" werden Benutzer dazu verleitet, persönliche Informationen oder die Anmeldedaten preiszugeben. Zu den häufigsten Varianten zählen dabei „dringende" Aufforderungen zur Kennwortzurücksetzung, bei denen der Benutzername sowie das Kennwort gestohlen und anschließend dazu missbraucht werden, mithilfe des Kontos des ahnungslosen Opfers persönliche Informationen über das Opfer und seine Kontakte zu sammeln.

Zur Erkennung solcher Attacken sowie von Angriffen auf soziale Plattformen ist bei Einzelpersonen ebenso wie Unternehmen noch mehr Wachsamkeit erforderlich. Zudem müssen Unternehmen Richtlinien und Lösungen einsetzen, mit denen gewährleistet werden kann, dass die Nutzung sozialer Plattformen durch Mitarbeiter nicht zu schwerwiegenden Datenkompromittierungen führt.

5. Neue Angriffsvarianten auf PCs und Servern greifen Schwachstellen an, die sich ober- oder unterhalb des Betriebssystems befinden.

Während sich viele Internetkriminelle Mobilgeräten zuwenden, werden andere weiterhin PC- und Server-Plattformen angreifen. Die neuen Angriffe werden 2014 jedoch nicht nur einfach Schwachstellen im Betriebssystem ins Visier nehmen, sondern auch solche Sicherheitslücken zum Ziel haben, die sich ober- oder unterhalb des Betriebssystems befinden.

Dazu zählen Schwachstellen in HTML5, das Programmierern die Erstellung von interaktiven, personalisierten und funktionsreichen Webseiten erlaubt, aber auch zahlreiche neue Angriffsflächen bietet. So haben Forscher bereits gezeigt, wie sie mithilfe von HTML5 den Browser-Verlauf eines Benutzers überwachen und dadurch gezieltere Werbung schalten können. Da viele HTML5-basierte Anwendungen auf Mobilgeräte zugeschnitten sind, erwarten wir Angriffe, die die Grenzen der Browser-Sandbox überwinden und Angreifern direkten Zugriff auf das Gerät und seine Dienste ermöglichen. Gleichzeitig werden viele Unternehmen Geschäftsanwendungen entwickeln, die auf HTML5 basieren. Um die Exfiltrierung der von diesen Anwendungen genutzten Daten verhindern zu können, müssen von Anfang an Sicherheitsfunktionen in diese neuen Systeme integriert werden.

Internetkriminelle werden zunehmend Schwachstellen anvisieren, die sich unterhalb des Betriebssystems – etwa im Speicher-Stack oder im BIOS – befinden. Damit solche Angriffe in Unternehmensumgebungen blockiert werden können, sind Hardware-unterstützte Sicherheitsmaßnahmen erforderlich, die auch unterhalb der Betriebssystemebene Schutz bieten.

6. Die wandlungsfähigen Bedrohungen machen die Nutzung von Big-Data-Sicherheitsanalysen erforderlich, um die Anforderungen an Erkennung und Leistung erfüllen zu können.

Bislang verließen sich die meisten Informationssicherheitslösungen auf die Erkennung böswilliger Inhalte (Blacklists) oder die Überwachung als zulässig bekannter Anwendungen (Whitelists). In jüngster Zeit stehen Sicherheitsexperten jedoch vor der Aufgabe, „graue Inhalte" zu identifizieren und entsprechend zu behandeln. Dazu werden zahlreiche Sicherheitstechnologien mit zuverlässigen Bedrohungsreputationsdiensten kombiniert.

Diese Bedrohungsreputationsdienste haben sich bereits bei der Erkennung von Malware, böswilligen Webseiten, Spam sowie Netzwerkangriffen bewährt. Im Jahr 2014 werden Sicherheitsanbieter neue Bedrohungsreputationsdienste und Analyse-Tools einführen, mit denen sie und ihre Benutzer noch schneller und zuverlässiger als bisher verschleierte und hochentwickelte Bedrohungen identifizieren können. Big-Data-Analysen ermöglichen Sicherheitsexperten die Erkennung raffinierter Umgehungstechniken sowie hochentwickelter hartnäckiger Bedrohungen, die geschäftskritische Unternehmensprozesse unterbrechen können.

7. Die Bereitstellung Cloud-basierter Unternehmensanwendungen schafft neue Angriffsflächen, die von Internetkriminellen ausgenutzt werden.

Willie Sutton, der Anfang des 20. Jahrhunderts 100 Banken ausgeraubt haben soll, soll als Motivation angegeben haben: „Weil hier das Geld liegt."[3] Internetkriminelle Banden des 21. Jahrhunderts werden zunehmend Cloud-basierte Anwendungen und Daten-Repositories ins Visier nehmen, da hier die Daten liegen – oder schon bald liegen werden. Als Einfallstor kann schon eine einzige Geschäftsanwendung dienen, die nicht auf Compliance mit den IT-Sicherheitsrichtlinien des Unternehmens geprüft wurde. Laut einem aktuellen Bericht nutzen mehr als 80 Prozent der Geschäftsanwender Cloud-Anwendungen, die von der IT-Abteilung nicht genehmigt oder nicht unterstützt werden.[4]

Obwohl Cloud-basierte Anwendungen zweifellos große wirtschaftliche und funktionelle Vorteile mit sich bringen, bieten sie gleichzeitig völlig neue Angriffsflächen. Dazu gehören die in allen Rechenzentren vorhandenen Hypervisoren, die von mehreren Kunden gemeinsam genutzten Cloud-Kommunikationsinfrastrukturen sowie die Verwaltungsinfrastruktur zur Bereitstellung und Überwachung großer Cloud-Dienste. Für die Sicherheitsexperten in Unternehmen besteht das Problem darin, dass das Unternehmen beim Wechsel der Geschäftsanwendungen in die Cloud den Überblick und die Kontrolle über fast sämtliche Sicherheitsaspekte verliert.

Dieser Verlust unmittelbarer Kontrolle der Sicherheitsperipherie des Unternehmens verstärkt den Druck auf die Sicherheitsverantwortlichen und Administratoren, da sichergestellt werden muss, dass der Vertrag mit dem Cloud-Anbieter sowie dessen Betriebsabläufe die erforderlichen Sicherheitsmaßnahmen umfasst. Des Weiteren muss gewährleistet sein, dass diese Maßnahmen permanent an die neuesten Bedrohungen angepasst werden. Große Unternehmen können häufig ausreichend Druck auf die Cloud-Anbieter ausüben, sodass dessen Sicherheitsmaßnahmen tatsächlich den Anforderungen des Unternehmens entsprechen. Kleinere Kunden Cloud-basierter Dienste müssen sich jedoch genau mit den häufig vage formulierten Nutzungsverträgen auseinandersetzen, da dort die Verantwortung für Sicherheit und Daten geregelt ist. Gerade neue Cloud-Dienste eröffnen neue Einfallstore, da sie häufig noch nicht die Tools und Gegenmaßnahmen umfassen, mit denen die Sicherheit der Daten gewährleistet wird.

Informationen zu den Autoren

Dieser Bericht wurde von Christoph Alme, Cedric Cochin, Geoffrey Cooper, Benjamin Cruz, Toralv Dirro, Paula Greve, Aditya Kapoor, Klaus Majewski, Doug McLean, Igor Muttik, Yukihiro Okutomi, François Paget, Craig Schmugar, Jimmy Shah, Ryan Sherstobitoff, Rick Simon, Dan Sommer, Bing Sun, Ramnath Venugopalan, Adam Wosotowsky und Chong Xu vorbereitet und geschrieben.

Informationen zu McAfee Labs

McAfee Labs gilt als weltweiter Vordenker bei Bedrohungsforschung und -erkennung sowie Internetsicherheit. Die 500 Forscher bei McAfee Labs erfassen Bedrohungsdaten von Millionen Sensoren in den wesentlichen Bedrohungsvektoren: Dateien, Web, Nachrichten und dem Netzwerk. Das McAfee Labs-Team korreliert diese Daten und erhält so Echtzeit-Bedrohungsinformationen, die über den Cloud-basierten Dienst McAfee Global Threat Intelligence an eng integrierte McAfee-Sicherheitsprodukte für Endgeräte und Netzwerke weitergegeben werden. McAfee Labs entwickelt auch grundlegende Bedrohungserkennungstechnologien wie DeepSAFE, Anwendungsprofile und Graylist-Management, die in das branchenweit umfassendste Sicherheitsprodukt-Portfolio einfließen.

Informationen zu McAfee

McAfee ist ein hundertprozentiges Tochterunternehmen der Intel Corporation (NASDAQ: INTC) und der weltweit größte auf IT-Sicherheit spezialisierte Anbieter. Seinen Kunden liefert McAfee präventive, praxiserprobte Lösungen und Dienstleistungen, die Computer, ITK-Netze und Mobilgeräte auf der ganzen Welt vor Angriffen schützen und es Anwendern ermöglicht, Verbindung mit dem Internet aufzunehmen und sich im World Wide Web zu bewegen. Mit der visionären Security Connected-Strategie, dem innovativen Ansatz für Hardware-unterstützte Sicherheit, sowie dem einzigartigen Global Threat Intelligence-Netzwerk engagiert sich McAfee unermüdlich dafür, seine Kunden zu schützen.
www.mcafee.com/de

[1] http://blogs.mcafee.com/consumer/pony-botnet-steals-2-million-passwords

[2] Stratecast: *The Hidden Truth Behind Shadow IT* (Die verborgene Wahrheit hinter Schatten-IT), November 2013. http://www.mcafee.com/de/resources/reports/rp-six-trends-security.pdf

[3] Sutton sagte aus, dass sein bekanntes Zitat gar nicht von ihm stammt. Stattdessen erklärte er, dass er die Banken „aus Spaß" ausraubte.

[4] Stratecast: *The Hidden Truth Behind Shadow IT* (Die verborgene Wahrheit hinter Schatten-IT), November 2013. http://www.mcafee.com/de/resources/reports/rp-six-trends-security.pdf

McAfee GmbH
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.mcafee.com/de

60756rpt_threats-predictions_1213_fnl_ETMG