Chaos mit Malware

Ralf Sydekum, 2013-04-10

Vor einiger Zeit hat McAfee Labs den McAfee Threats Report: Second Quarter 2013 vorgestellt. McAfee stellt darin fest, dass die Zahl Android-basierter Malware um 35 Prozent zugenommen hat. Zuletzt wurde ein derartiges Wachstum zu Beginn des Jahres 2012 verzeichnet. McAfee hat zudem doppelt so viel Ransomware in Quartal Zwei als in Quartal Eins festgestellt. Die Zahl von Ransomware (Pop-Ups oder andere Nachrichten, die den Nutzer bedrohen, bis er ein „Lösegeld“ überweist) in 2013 liegt damit jetzt schon höher als in allen vorherigen Perioden zusammengenommen. Alle Arten von Malware wurden gefunden – Malware, die mTans vom Online Banking stiehlt, seriöse, aber infizierte Apps, bösartige Apps im Schafspelz sowie getürkte Dating- und Entertainment-Apps. Wir verbringen mit Apps einen großen Teil unserer mobilen Internet-Zeit – und viele sind mit gefährlicher Malware durchsetzt.

Zusätzlich zu den Bedrohungen, die auf mobile Endgeräte abzielen, stellte McAfee im zweiten Quartal 2013 einen 16-prozentigen Anstieg von verdächtigen URLs und 50 Prozent mehr Malware fest, die über ein digitales Zertifikat verfügen. Eine „tolle“ Masche: Man wiegt sich aufgrund des Zertifikats in Sicherheit und dann wird man von der Malware kalt erwischt. Die Angreifer passen sich also fortwährend der veränderten Umgebung an und finden immer neue Möglichkeiten, um Anwender auszunehmen.

Gerne würde ich an dieser Stelle den einfachen Rat geben, der bis vor kurzem auch Bestand hatte: Passen Sie auf, was Sie eintippen, klicken Sie nicht auf verdächtige Links, meiden Sie zwielichtige Angebote im Internet! Aber mittlerweile kann sich Schadsoftware auch über eine Werbung in Ihr System einschleichen, die auf einer populären Nachrichtenseite geladen wird. Kaum einer ist immun vor einer Infektion. Man muss sich nur mal vorstellen, dass Spam-Nachrichten noch immer fast 70 Prozent des gesamten E-Mailverkehrs ausmachen. Wir verfassen und erhalten täglich unzählige echte E-Mails und trotzdem machen sie nur 30 Prozent des Gesamtvolumens aus?

Das Ponemon Institute veröffentlichte kürzlich den Current State of Application Security Report, für den 642 IT-Fachkräfte (sowohl Entscheider als auch Techniker) zur Verwendung von Tools, dem Kenntnisstand der Entwicklungsteams und Best Practices befragt wurden. Die Studie besagt, dass bei Angriffen auf die Unternehmensinfrastruktur die Applikationsebene für mehr als 90 Prozent der Schwachstellen verantwortlich ist. Trotzdem geben Unternehmen weiterhin mehr als 80 Prozent ihres IT-Security-Budgets für den Schutz des Netzwerks und der Endpoint-Ebene aus. Laut Ponemon liegen die meisten Unternehmen bei der Applikationssicherheit deutlich zurück. Interessanterweise beurteilen die Entscheider die Sicherheitsvorkehrungen anders als Techniker, die tagtäglich die Maßnahmen durchführen, also ganz nah dran sind an der tatsächlichen Wirkungsweise. Während also 71 Prozent der Entscheider davon ausgehen, dass die Sicherheit auf Applikationsebene auf dem neuesten Stand ist, sind nur 20 Prozent der Techniker derselben Überzeugung. Rund zwei Drittel der Entscheider bewerten ihr Sicherheitsprogramm als gut ausgebaut. Bei den Technikern ist es nur ein Drittel. Bei der IT-Architektur gehen die unterschiedlichen Bewertungen sogar noch weiter auseinander: Drei Viertel der Entscheider gehen davon aus, dass die Architektur sicher ist, bei den Technikern sind es nur 23 Prozent. Entweder liegen diese unterschiedlichen Bewertungen an der internen Kommunikation oder es ist noch nicht in die Führungsebenen vorgedrungen, dass die Applikationssicherheit proaktiv angegangen werden muss. Ebenso müssen die neuen Sicherheitsrisiken verstanden und die Mitarbeiter dazu geschult werden.

Besonders beunruhigend ist die Tatsache, dass die meisten Unternehmen trotz der aufsehenerregenden Medienberichterstattung und der Statistiken ihre Applikationen nicht mit Blick auf die Sicherheit entwickeln oder testen. Der Ponemon-Studie zufolge testen nur 43 Prozent der Befragten Applikationen vor dem Release überhaupt auf Sicherheitsrisiken. Nur 41 Prozent nutzen automatisierte Scan-Tools, um Applikationen während der Entwicklung zu testen. Und nur 42 Prozent lassen ihre Applikationen manuell von internen oder externen Teams testen.

Wahrscheinlich ist es mit der IT-Sicherheit wie in anderen Bereichen des Lebens: Wir fühlen uns so lange sicher, bis etwas passiert. Und erst dann reagieren wir mit Vorsichtsmaßnahmen. Für Unternehmen kommt diese Einsicht dann zu spät, der Schaden ist dann schon entstanden.

Wir bei F5 helfen Ihnen gerne dabei, es gar nicht so weit kommen zu lassen. Ihre Sicherheit ist unser Anliegen und wir haben gerade für die oft vernachlässigte Applikationsebene die richtige Lösung: der Mobile App Manager von F5 sorgt für eine sichere Auslieferung von Applikationen und ist darüber hinaus hoch skalierbar. Rufen Sie uns an, wir informieren Sie gerne!

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com