Pressemitteilung

McAfee Threat Predictions 2011: Mobile Anwendungen, ortsbezogene Dienste und Apple im Fokus

Steigende Bedrohung durch URL-Verkürzungsdienste, Internet-TV und Hacktivismus

München, 28. Dezember 2010. McAfee präsentiert die aktuelle Ausgabe seines jährlich erscheinenden *Threat Predictions* Reports. Darin nennt der IT-Sicherheitsspezialist die größten Onlinerisiken für das kommende Jahr, die die firmeneigene Forschungsabteilung McAfee Labs ermittelte. Auf der Liste finden sich die meistbeachteten Plattformen und Services – darunter die Betriebssysteme Android, iOS und Mac OS X, der Geolocationdienst Foursquare und die Fernsehplattform Google TV. Sie alle werden als Ziele größerer Cyberangriffe gesehen. Darüber hinaus prognostiziert McAfee Labs, dass das Beispiel Wikileaks Schule machen wird und die Zahl politisch motivierter Attacken zunimmt.

Folgende Trends erwarten die McAfee Labs für das Jahr 2011:

Social Media: Missbrauch von URL-Verkürzungsdiensten
Social-Media-Sites wie Twitter und Facebook haben eine Form der „Echtzeit"-Kommunikation geschaffen, durch die sich im Jahr 2011 die Bedrohungslage grundlegend verändern wird. Nach Ansicht der McAfee Labs spielen dabei besonders die zum Beispiel auf Diensten wie Twitter häufig verwendeten Kurz-URLs eine Rolle. URL-Verkürzungsdienste machen es Cyberkriminellen leicht, das tatsächliche Linkziel zu verschleiern und die Nutzer ohne deren Wissen auf bösartige Websites zu lenken. Eine wachsende Zahl der mehr als 3000 Kurz-URLs, die pro Minute erzeugt werden, wird nach der Prognose von McAfee Labs für Spamming, Betrug und andere unlautere Zwecke verwendet werden.

Social Media: Missbrauch ortsbezogener Dienste
Ortsbezogene Dienste wie Foursquare, Gowalla und Facebook Places können den Aufenthaltsort von Nutzern ermitteln, verfolgen und aufzeichnen. Nach nur wenigen Klicks sehen Cyberkriminelle in Echtzeit, wer twittert, was er twittert, wofür er sich interessiert, mit welchem Betriebssystem er unterwegs ist und welche Applikationen er nutzt. Die Menge an personenbezogenen Daten ermöglicht Cyberkriminellen die Ausführung personalisierter Angriffe. McAfee Labs prognostiziert, dass diese Taktiken 2011 verstärkt auf allen populären Social-Networking-Sites Anwendung finden werden.

Mobile Geräte: Nutzung am Arbeitsplatz nimmt zu und erhöht das Risiko
Bis jetzt waren Angriffe auf Mobilgeräte rar. Die Hauptgefahren im Jahr 2010 bestanden im „Jailbreaking" auf dem iPhone und in der Verbreitung einer Mobilversion des Banking-

Trojaners Zeus. Angesichts der zunehmenden Nutzung mobiler Geräte im Geschäftsleben, der traditionell fragilen Netzinfrastruktur und der schleppenden Implementierung von Verschlüsselungsverfahren erwartet McAfee Labs für das Jahr 2011 eine schnelle Zunahme von Angriffen auf mobile Geräte. Die Gefahr für personenbezogene Daten und Geschäftsinformationen wird als sehr hoch eingestuft.

Apple: Die Schonzeit ist zu Ende

Lange Zeit blieben Nutzer des Mac OS von Angriffen weitgehend verschont. McAfee Labs warnt davor, dass Malware für den Mac im Jahr 2011 zunehmend verfeinert wird. Die Beliebtheit von iPhone und iPad im Geschäftsleben in Verbindung mit der Unwissenheit der Nutzer, was deren Sicherheitsstatus betrifft, wird das Risiko des Daten- und Identitätsdiebstahls erhöhen und Apple-Botnets und -Trojaner alltäglich werden lassen.

Anwendungen: Das Datenleck im Fernseher

Neue Internet-TV-Plattformen gehörten 2010 zu den am heißesten ersehnten Anwendungen. Angesichts der zunehmenden Beliebtheit bei den Verbrauchern und einer überhasteten Vermarktung seitens der Hersteller erwartet McAfee Labs eine wachsende Zahl zweifelhafter und bösartiger Apps für Medienplattformen wie Google TV. Cyberkriminelle könnten mit Hilfe solcher Anwendungen persönliche Daten und Identitätsmerkmale der Benutzer auslesen. Das ermöglicht ihnen, die entsprechenden Geräte zu manipulieren, zu kontrollieren und sie in ihre Botnetze einzubinden. Botnetze werden so noch „effektiver“ und gefährlicher.

Politisch motivierte Hacks: Wikileaks macht Schule

Das kommende Jahr wird eine Zeit um sich greifender politisch motivierter Angriffe und neuer raffinierter Angriffsmethoden sein. Weitere Gruppierungen, die für sich in Anspruch nehmen, von Regierungen oder bestimmten Bewegungen unabhängig zu sein, werden dem Beispiel Wikileaks folgen. Sie werden organisierter und strategischer vorgehen, indem sie soziale Netzwerke in den Prozess einbinden. McAfee Labs glaubt, dass derlei „Hacktivismus“ im kommenden Jahr und darüber hinaus zur neuen Art der Darstellung politischer Positionen avancieren wird.

Advanced Persistent Threats: Eine Klasse für sich

Die „Operation Aurora“ war die Mutter der sogenannten Advanced Persistent Threats (APT). Dabei handelt es sich um einen ganz neuen Typ von Cyberangriffen: zielgerichtete und anhaltende Fälle von Cyberspionage oder -sabotage mit Unterstützung oder im Auftrag von Staaten und mit Zielen, die jenseits der finanziellen Bereicherung oder des politischen Protests liegen. Laut McAfee Labs müssen sich Unternehmen jeder Größe, deren Geschäft nationale Sicherheitsinteressen berührt oder in nennenswertem Ausmaß globalisiert ist, darauf gefasst machen, Opfer solcher Angriffe zu werden. Im Visier der Kriminellen befinden sich Dokumentenbestände jeder Art, von E-Mail-Archiven bis zu Patentdatenbanken.

Der vollständige Bericht *2011 Threat Predictions* von McAfee Labs ist erhältlich unter http://www.mcafee.com.

McAfee
McAfee (NYSE: MFE) ist der weltgrößte dedizierte Spezialist für IT-Sicherheit. Das Unternehmen mit Hauptsitz im kalifornischen Santa Clara hat sich der Beantwortung anspruchsvollster Sicherheitsherausforderungen verschrieben. Seinen Kunden liefert McAfee präventive, praxiserprobte Lösungen und Dienstleistungen, die Computer und ITK-Netze auf der ganzen Welt vor Angriffen schützen und es Anwendern ermöglichen, gefahrlos Verbindung mit dem Internet aufzunehmen und sich im World Wide Web zu bewegen. Unterstützt von der einzigartigen Global Threat Intelligence entwickelt McAfee innovative Produkte, die Privatnutzern, Firmen und Behörden helfen, ihre Daten zu schützen, einschlägige Gesetze einzuhalten, Störungen zu verhindern, Schwachstellen zu ermitteln und die Sicherheit ihrer Systeme laufend zu überwachen und zu verbessern. Weitere Informationen über McAfee finden sich unter www.mcafee.com.

Ansprechpartner

McAfee

Isabell Unseld
PR-Managerin Mittel-, Ost- und Westeuropa
Ohmstraße 1
85716 Unterschleißheim
089 3707-1535
isabell_unseld@mcafee.com

Harvard Public Relations

Felix Laubenthal
Guillermo Luz-y-Graf
Implerstraße 26
81371 München
089 532957-46
089 532957-30
mcafee@harvard.de oder
felix.laubenthal@harvard.de
guillermo.luz-y-graf@harvard.de