PRESSEMITTEILUNG

Panda Securitys IT-Sicherheitsprognose für 2016: Cyberattacken greifen immer stärker um sich

Duisburg, den 30. Dezember 2015 – Die IT-Experten von Panda Security, einem der weltweit führenden Anbieter von cloud-basierten IT-Sicherheitslösungen, haben die Entwicklungen der vergangenen 12 Monate im Bereich der Cybersicherheit analysiert. Auf Basis dieser Daten haben sie eine Prognose darüber getroffen, mit welchen Risiken und Herausforderungen die IT-Welt in 2016 voraussichtlich konfrontiert wird. Die wichtigsten Erkenntnisse sind im Folgenden zusammengefasst:

Abermals starke Zunahme an neuen Schädlingen

Die Entwicklung und Verbreitung von neuen Malware-Exemplaren, die darauf abzielen, Nutzer aller Arten von digitalen Geräten zu infizieren, wird auch in 2016 weiterhin exponentiell zunehmen. Ähnliches haben wir bereits 2015 erlebt, als durchschnittlich 230.000 neue Samples pro Tag registriert wurden. Im Jahr 2014 waren es im Schnitt 200.000 neue Schadprogramme täglich.

Vermehrt Infektionen via JavaScript und Powershell

2016 gibt es voraussichtlich einen Anstieg von Infektionen via JavaScript sowie eine zunehmende Anzahl von Cyberkriminellen, die Powershell nutzen. Powershell ist ein Tool, das in Windows 10 enthalten ist und es ermöglicht, Skripte mit allen Arten von Funktionalitäten auszuführen. Diese könnten, so die IT-Experten von Panda Security, vermehrt genutzt werden, um User zu attackieren.

Großangelegte Angriffe mit Hilfe von Exploit Kits

Vorrangiges Ziel von Cyberkriminellen ist es, eine große Anzahl von Personen und Unternehmen anzugreifen, um dabei größtmögliche Profite zu erzielen. Aus diesem Grund werden sie weiterhin Tools wie Exploit Kits verwenden. Da viele aktuelle IT-Security-Lösungen nicht in der Lage sind, derartige Angriffe effektiv zu bekämpfen, ist die Infektionsrate sehr hoch.

Neue Techniken für gezielte Angriffe auf Mobilgeräte

Aus demselben Grund werden auch Mobilgeräte zunehmend mit Malware infiziert. Hier werden insbesondere Geräte mit Android-Betriebssystem betroffen sein, da es das beliebteste und am weitesten verbreitete Betriebssystem auf dem Markt ist.

Zudem wird es eine Zunahme von direkten Angriffen durch Rootkit-Techniken geben, die es den Hackern erlauben, sich vor dem Betriebssystem und den Sicherheitslösungen zu verstecken.

„Angriffe auf Android sind bereits in den vergangenen Jahren immer häufiger vorgekommen. 2016 wird es jedoch neue Methoden für die Infektion von Mobilgeräten geben. Wir werden mehr Bedrohungen erleben, die das Gerät rooten, was ihre frühzeitige Erkennung und Beseitigung zu einer nahezu unlösbaren Aufgabe für Antiviren-Software machen wird. Eine Ausnahme sind hier IT-Security-Lösungen, die bereits vorab vom Werk installiert wurden“, sagt Luis Corrons, Technischer Leiter der PandaLabs.

Internet der Dinge rückt in den Fokus von Cyberkriminellen

Das Internet der Dinge wird 2016 eine Blütezeit erleben: Mehr Geräte als je zuvor werden an das Internet angeschlossen sein. Aus diesem Grund werden Cyberkriminelle vermehrt Angriffe auf diese Geräte starten. Einen ersten Vorgeschmack auf diese Art von Angriffen haben wir bereits 2015 im Bereich der „Connected Cars“ bekommen, also bei Autos, deren Software mit dem Internet verbunden war. Hacker konnten hier die Fernsteuerung der Fahrzeuge übernehmen.

Mobiles Bezahlen wird beliebter und damit zum Ziel von Hackern

Bezahlplattformen auf Mobilgeräten werden im kommenden Jahr verstärkt auf dem Prüfstand stehen. Denn auch hier gilt: Je beliebter diese Zahlungsmethode wird, desto attraktiver wird sie für Hacker. Sie könnte Kriminellen eine einfache und lukrative Möglichkeit bieten, direkt an Geld zu kommen.

„Sollte eine der mobilen Bezahlplattformen beliebter werden als andere, wird diese die erste sein, die die Angreifer auf Schwachstellen in ihrem System prüfen werden“, prognostiziert Luis Corrons.

Anforderungen an die IT-Sicherheitslösungen nehmen zu

Angesichts der stark steigenden Anzahl von Bedrohungen und der technisch immer ausgereifteren Angriffe werden sowohl Unternehmen als auch Privatanwender im kommenden Jahr zusätzliche Sicherheitsmaßnahmen ergreifen müssen, um sich vor den vielfältigen IT-Gefahren zu schützen.

Für Unternehmen wird es noch mehr Bedrohungen geben, die sowohl ihrem Ruf als auch ihren Finanzen ernsthaft schaden können. Cyberkriminelle werden weiterhin darauf abzielen, vertrauliche Firmendaten (Finanzdaten, strategische Pläne usw.) und Kundeninformationen zu stehlen. Sind diese erst einmal in ihrem Besitz, werden sie von der Firma für die Rückgabe der Daten ein Lösegeld fordern. Diese als Cryptolocker bekannt gewordene Methode hat sich bereits in 2015 stark verbreitet.

Um der Komplexität dieser Angriffe, die uns im neuen Jahr bevorstehen, adäquat zu begegnen, wird es für Unternehmen und Privatanwender notwendig sein, neue Sicherheitstools und -lösungen zu installieren, die das Verhalten aller ausführbaren Dateien analysieren und klassifizieren können. Zudem sollten diese IT-Security-Lösungen fortschrittliche Schutzmechanismen beinhalten, die Sicherheitsbedrohungen sowohl verhindern als auch bekämpfen können.

Über PandaLabs

PandaLabs ist das Anti-Malware-Labor des weltweit agierenden IT-Spezialisten Panda Security und fungiert als dessen zentrale Stelle für Malware-Treatment. PandaLabs entwickelt kontinuierlich und in Echtzeit die notwendigen Gegenmaßnahmen, um Panda-Security-Kunden vor allen Arten von schädlicher Software auf globalem Level zu schützen. PandaLabs ist somit verantwortlich für die Durchführung detaillierter Scans aller Malware-Arten. Ziel ist es, sowohl den Schutz für die Panda Security Kunden zu verbessern, als auch die Öffentlichkeit aktuell und zeitnah zu informieren.

Pressekontakt:

Kristin Petersen
Presse & PR

PAV Germany GmbH
Dr.-Alfred-Herrhausen-Allee 26
47228 Duisburg

Tel: +49 2065 961 352
Fax: +49 2065 961 195
Kristin.Petersen@de.pandasecurity.com
www.pandanews.de
www.pandasecurity.com/germany/