

Sicherheitstrends 2014: Bedrohungen für Android werden Rekordzahlen erreichen

17.12.2013, 16:14 | IT, New Media & Software

Pressemitteilung von: *Panda Security PAV Germany GmbH*

Kurz vor Jahresende hat Panda Security, die Cloud Security Company, einen Blick in die Zukunft gewagt und eine Prognose bezüglich der größten Sicherheitsrisiken 2014 in der IT-Welt abgegeben. Cyber-Spionage bedroht zunehmend die politische und wirtschaftliche Sicherheit, die permanente Verfügbarkeit von Daten und die wachsende Anzahl von mobilen Geräten öffnen Hackern neue Möglichkeiten für kriminelle Machenschaften und die Masse an neuen digitalen Bedrohungen nimmt kontinuierlich zu. Ein bedeutender Anstieg bei der Entwicklung von Malware sowie Angriffe auf Java und soziale Medien werden in den kommenden Monaten die Quelle erhöhter Sicherheitsgefahren darstellen.

Was die Unternehmenssicherheit angeht, werden neue Lösungen erscheinen, welche die Datensicherheit und –Integrität effektiver gewährleisten. „Da Angriffe auf Unternehmen zunehmend aggressiver werden, sind traditionelle Perimeterlösungen – obwohl notwendig – für bestimmte Szenarien nicht länger ausreichend. Es wird neue Lösungen geben, die diesen Bedürfnissen entsprechen und die Sicherheit sensibler Daten viel effektiver gewährleisten“, so Luis Corrons, Technischer Direktor von PandaLabs.

Im Bereich der mobilen Sicherheit wird Android weiterhin das Hauptziel für Cyber-Kriminelle bleiben. Außerdem wird erwartet, dass Ransomware sowie Banking-Trojaner und Bots die am weitesten verbreiteten Gefahren sein werden. Schließlich wird es auch einen erheblichen Anstieg von Cyber-Angriffen auf alle Arten von Geräten geben.

Die PandaLabs Security Trends 2014 im Überblick:

- **Malware:** Die Anzahl der neuen Schadprogramme wird 2014 ein neues Rekordhoch erreichen. „Ein Großteil der neuen Schädlinge werden Varianten bekannter Malware sein, die einfach modifiziert werden, um Sicherheitslösungen zu umgehen“, erklärt Corrons.
- **Schwachstellen:** Sicherheitslücken bei Java sind für die meisten Infektionen, die im gesamten Jahr 2013 entdeckt wurden, verantwortlich. Das wird sich wahrscheinlich auch 2014 nicht ändern. Die Tatsache, dass Java auf Milliarden von Computern installiert ist und offensichtlich zahlreiche Sicherheitslücken aufweist, macht es zu einem beliebten Ziel für Cyber-Kriminelle. Derzeit gibt es kein Exploit-Kit auf dem Schwarzmarkt, das nicht eine Reihe von Javas Schwachstellen ausnutzt.
- **Social Engineering:** Social Engineering gibt Cyber-Kriminellen Raum, um ihre Kreativität zu demonstrieren. Nach den Schwachstellen ist die zweithäufigste Ursache für Computerinfektionen der Anwender selbst, wenn er unwissentlich in die Fallen der Internet-Kriminellen tritt. Dieser Trend wird weiterhin zunehmen und obwohl sich viele der Betrügereien per E-Mail verbreiten, werden die meisten davon auf Webseiten sozialer Netzwerke auftauchen.
- **Mobile Malware:** Android wird das mobile Ziel Nummer 1 für Cyber-Kriminelle bleiben und im kommenden Jahr wird es ein neues Rekordhoch bei den Gefahren für diese Plattform geben.
- **Ransomware:** Zusätzlich zu Banking-Trojanern und Bots wird Ransomware im Jahr 2014 eine der am weitesten verbreiteten Gefahren sein. Es wird neue Wellen von Malware geben, die ihre Opfer auffordert, ein Lösegeld zu zahlen, um ihre Computer wieder zu entsperren, auf ihre Dateien zugreifen zu können (CryptoLocker) oder vermeintliche Gefahren zu beseitigen (gefälschte Antivirensoftware). Einige Arten von Ransomware fordern sogar zur Zahlung einer „Strafe“ für vermeintlich illegale Aktivitäten (Police Virus) auf. Ransomware ermöglicht es Kriminellen, Geld direkt von den Anwendern zu ergaunern und so ist zu erwarten, dass die Verbreitung dieser Art von Schadprogrammen zunimmt und sich auf andere Gerätearten wie beispielsweise Smartphones ausbreitet.

- **Unternehmenssicherheit:** Da Malware-Angriffe zunehmend aggressiver werden (wie der CryptoLocker gezeigt hat) und die Anzahl der gezielten Angriffe auf Firmen weiterhin steigt, wird es einen Bedarf an besonders effektiven Sicherheitsmaßnahmen, die über den Schutz „herkömmlicher“ Antivirenlösungen hinausgehen, geben.
- **Internet der Dinge:** Die Anzahl der Geräte, die an das Internet angeschlossen werden, steigt ständig und das wird sich fortsetzen. IP-Kameras, Fernseher, Multimediaplayer, etc. sind jetzt ein wesentlicher Bestandteil des Internets und haben oft Eigenschaften, die sie von anderen Geräten wie Laptops, Smartphones oder Tablets unterscheiden: Die Anwender aktualisieren sie selten. Infolgedessen sind sie hinsichtlich der Ausnutzung ihrer Schwachstellen äußerst gefährdet. Also ist es sehr wahrscheinlich, dass wir in Zukunft Angriffe, die auf diese Geräte gerichtet sind, erleben werden.

Portrait

1990 in Bilbao, Spanien, gegründet, hat sich Panda Security zum Ziel gesetzt, seinen Kunden intelligenten Schutz gegen Malware bei geringstmöglicher Systembelastung zu bieten. Als erster Anbieter überhaupt hat Panda dazu im Jahr 2006 eine Scan-Technik vorgestellt, die die Vorteile des Cloud-Computing mit dem Wissen aller Panda-Nutzer kombiniert. Wird irgendwo auf der Welt ein neues Schadprogramm entdeckt, kann Panda alle seine Nutzer durch diesen „Collective Intelligence“-Ansatz in kürzester Zeit schützen. Panda Security entwickelt und vertreibt leistungsfähige Consumer- wie auch Enterprise-Lösungen. In Deutschland und Österreich leitet die PAV Germany GmbH das Panda-Geschäft und bietet Unternehmenskunden kostenfreien 24/7/365-Support auf Deutsch durch die eigenen Techniker. Den Vertrieb organisiert Panda Security durch Channel-Partner. Mit 61 Niederlassungen weltweit und einem Kundenstamm aus fast 200 Ländern hat sich Panda Security eine globale Präsenz geschaffen.

News-ID: 767684 • Views: 191 (Stand: 06.10.2026)

Link zur Pressemitteilung:

<https://www.openpr.de/news/767684/Sicherheitstrends-2014-Bedrohungen-fuer-Android-werden-Rekordzahlen-erreichen.html>