crn.de

BSI Lagebericht 2019: Mehr Angriffe, neue Ziele

Lars Bube

3 Minuten

In seinem aktuellen »Lagebericht zur IT-Sicherheit 2019« konstatiert das BSI eine »hoch angespannte Gefährdungslage«. Neben Unternehmen und Privatnutzern geraten immer häufiger auch öffentliche Einrichtungen sowie IoT-Geräte und Cloud-Server ins Visier der Angreifer.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat seinen »Lagebericht zur IT-Sicherheit 2019« vorgestellt. Darin Analysiert das BSI eingehend die in den letzten zwölf Monaten verzeichneten Cyber-Angriffe und ihre Hintergründe einschließlich einer Beschreibung der dabei verwendeten Methoden und Mittel der Angreifer. Daraus leiten die Experten einen detaillierten Überblick der aktuellen Bedrohungslage sowie Vorschläge für Verbesserungsmaßnahmen ab.

Der klare Tenor des aktuellen Berichts lautet: Auch wenn sich im Bereich Sicherheit viel tut, reicht das noch lange nicht aus. Die Sicherheitslage in Deutschland bleibt insgesamt hoch angespannt. Die Angreifer setzen auf immer raffiniertere Methoden und widmen sich zugleich neuen, für sie lukrativen Zielen. Dabei helfen ihnen Schwachstellen in Hard- und Software genauso, wie unzureichende Schutzmechanismen und Sicherheitsstrategien sowie menschliches Versagen. Letztendlich

steigt damit sowohl die Qualität als auch die Quantität der Angriffe.Rund 11,5 Millionen Infektionen wurden an die Netzbetreiber übermittelt.

Ein eindrückliches Beispiel für diese Entwicklungen liefert Emotet. Schon seit 2010 bekannt und erst im Vorjahr vom BSI als »gefährlichste Schadsoftware der Welt « gebrandmarkt, sorgt sie in immer neuen Varianten weiterhin für erhebliche Schäden. Nachdem zuerst vor allem Banken und Unternehmen betroffen waren, wurden in letzter Zeit immer häufiger auch öffentliche Einrichtungen wie etwa das Berliner Kammergericht und mehrere Krankenhäuser damit attackiert und weitgehend lahmgelegt.

Am Beginn der Infektion stehen meist Mitarbeiter, die maliziöse Anhänge oder Links aus gut gefälschten Spam-Mails öffnen, die dann Schwachstellen in den Systemen und der Sicherheitsarchitektur ausnutzen, um sich festzusetzen und weitere Schadsoftware nachzuladen. Allein aus deutschen Regierungsnetzen filterte das BSI über 750.000 verseuchte E-Mails heraus.

Seite 1 von 2 ›

---

crn.de

BSI Lagebericht 2019: Mehr Angriffe, neue Ziele

Lars Bube

3-4 Minuten

Fortsetzung des Artikels von Teil 1 .

Angriffe auf das IoT und die Cloud

Mehr als 50 Prozent der registrierten Cyberangriffe waren auf solche Malware zurückzuführen, bei der Mehrzahl davon handelte es sich um erpresserische Ransomware. Aber auch der direkte Diebstahl von Informationen, Daten, Betriebsgeheimnissen und Identitäten spielt weiterhin eine große Rolle, manchmal auch in Kombination. Insgesamt wurden 2018 rund 114 Millionen neue Schadprogramm-Varianten registriert, im Durchschnitt also über 300.000 pro Tag, in der Spitze waren es sogar mehr als 450.000. Nur noch etwas mehr als 50 Prozent davon richten sich direkt gegen Windows-Rechner, knapp 3 Prozent gegen Android und weniger als 1 Prozent haben es auf MacOS abgesehen.

Enorm gewachsen ist der Anteil an betriebssystemunabhängiger Schadsoftware (34 Prozent), die sich etwa gegen Skripte richtet. Damit greifen die Hintermänner vermehrt auch das Internet der Dinge (IoT) an. Durch die fatale Kombination aus einer rasant wachsenden Geräteanzahl mit einem oft erschreckend niedrigen

Sicherheitsniveau sind die Erfolgsaussichten hier besonders groß und die Angreifer konnten an einzelnen Tagen alleine in Deutschland bis zu 110.000 Geräte infizieren und als Bots kapern. Aber auch vermeintlich professionell geschützte Cloud-Server gehen den Angreifern dabei immer wieder ins Netz.

Anschließend verwenden die Cyberkriminellen ihre Armeen aus Zombie-Rechnern dann beispielsweise für weitere Spam-Kampagnen, Informationsdiebstahl, Banking-Betrug, das Berechnen von Krypto-Währungen oder auch DDoS-Angriffe. Letztere werden laut BSI zwar etwas seltener, bekommen dafür aber mit Angriffsbandbreiten von bis zu 300 Gbit/s deutlich mehr Schlagkraft. Darüber hinaus bereitet dem BSI auch die wachsende Anzahl von Hardware-Schwachstellen, namentlich etwa die als »Meltdown« und »Spectre« bekannt gewordenen Lücken in weit verbreiteten Prozessoren, Sorgen.

Diese Entwicklungen zeigen, dass die Dimension der Sicherheit bei der Digitalisierung eine deutlich größere Rolle spielen muss. Neben der Entwicklung und Umsetzung tragfähiger Sicherheitsstrategien muss das Thema dazu auch bei der Entwicklung neuer Software und Geräte, insbesondere für IoT-Anwendungen, von Anfang an höchste Priorität genießen, etwa durch Security-by-Design.

〈 **Seite 2 von 2**

1. Mehr Angriffe, neue Ziele
2. **Angriffe auf das IoT und die Cloud**