Maximilian Eibl, Martin Gaedke. (Hrsg.): INFORMATIK 2017,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2017 2243

Workshop „Digitalen Veränderungen auf der Spur: Open vs. Closed Source Forensic Tools“

Roman Povalej[1]

Der Erfolg mobiler Geräte ist unaufhaltsam. Mehr als 44 Mio. Menschen in Deutschland besitzen ein Smartphone, mit dem sie im Internet surfen, Bilder und Filme ansehen, Nachrichten lesen sowie versenden und noch vieles mehr. Die Vernetzung schreitet weiter voran. Ob bei der Arbeit, beim Einkaufen, in der Straßenbahn oder beim Abendessen, der Mensch ist immer mehr online. Wegen des großen Erfolgs mobiler Gerätschaften werden große Geldmengen investiert und transferiert sowie Daten analysiert und gesammelt. Allerdings weckt dies auch illegale Begehrlichkeiten und die Nutzer werden Opfer von Hacks bzw. Malware. Daten werden ausgespäht, Rechner werden missbraucht, Identitäten werden geraubt. Der wirtschaftliche Schaden ist enorm.

Derartige Risiken waren, sind und werden immer eine Herausforderung im Internet, in Netzwerken und auf Rechnersystemen sein. Selbst bei einem komplett autarken und abgeschotteten System, ohne jegliche Kommunikation nach außen, bleibt immer noch der Mensch als potenzielle Gefahrenquelle. Durch die immer größere Vernetzung werden auch weitere Angriffsflächen geschaffen. Trends wie Internet-der-Dinge oder Industrie 4.0 oder Integrierte Ökosysteme erhöhen die Vernetzung, bieten aber gleichzeitig weitere Angriffspunkte.

Jeder Hack bzw. jede Malware hinterlässt digitale Spuren im Netzwerk und auf dem kompromittierten System. Mittels forensischen Werkzeugen sollen diese digitalen Spuren aufgedeckt und analysiert werden sowie die richtigen Schlussfolgerungen über den Verursacher gezogen und Maßnahmen eingeleitet werden. Zum Einsatz kommen sowohl Open Source als auch Closed Source Lösungen. Jede Lösung für sich betrachtet hat Stärken und Vorteile, unter Umständen aber auch Grenzen, die insgesamt näher zu betrachten sind, um zu entscheiden, wann welche Lösung zum Einsatz kommen sollte.

Und zu guter Letzt, aber nicht nur, sollte den folgenden Fragen nachgegangen werden: Gibt es primäre Einsatzgebiete von einzelnen Lösungen? Wo liegen deren Grenzen? In welche Richtungen müssen sich die forensischen Lösungen entwickeln? Inwieweit werden neue Herausforderungen bereits heute schon abgedeckt?

Roman Povalej

[1] Polizeiakademie Niedersachsen., Studiengebiet 1, Gimter Str. 10, 34346 Hann. Münden, roman.povalej@polizei.niedersachsen.de

doi:10.18420/in2017_223