Zusammenfassung

Das Internet hat sich in den letzten Jahren zu einem globalen System etabliert, welches von Hunderten von Millionen Menschen tagtäglich verwendet wird. Dies umfasst verschiedenste Aktivitäten wie Online-Shopping, die Nutzung von sozialen Netzwerken oder die Beschaffung von Informationen. Die Schattenseite des Internets offenbart jedoch auch vermehrt verdächtige und bösartige Aktivitäten, die mit Netzwerk-basierten Angriffen oder Schadsoftware in Verbindung stehen. Zum einen sind viele der häufig eingesetzten Netzwerkprotokolle und Internetgeräte für verschiedenste Angriffsszenarien verwundbar. Zum anderen arbeiten Angreifer unentwegt daran, neuartige Angriffstechniken auf Computersysteme zu entwickeln. Als solches sind die Internetnutzer einer Vielzahl von alltäglichen Gefahren ausgesetzt.

Im Fokus dieser Dissertation wird diese Gefährdung aus zwei unterschiedlichen Blickwinkeln betrachtet. Der erste Teil dieser Arbeit befasst sich mit der Bedrohung durch Netzwerk-basierte Angriffe. Zu diesem Zweck sind zwei umfangreiche empirische Langzeitstudien initiiert worden, in denen über Monate hinweg wöchentliche Internetweite Netzwerkscans durchgeführt worden sind. Die erste Studie richtet dabei ihren Schwerpunkt auf Bedrohungen auf der TCP- und UDP-Protokollebene, im Speziellen auf Endgeräte, die für den Missbrauch für *Amplification Distributed Denial-of-Service* Angriffe anfällig sind. Diese Art von Angriffen wird zunehmend eingesetzt, um Netzwerke gezielt mit Verkehr von mehreren Hundert Gbit/s zu überlasten. Die zweite Studie führt diese Art von Analysen fort und betrachtet Bedrohungen auf der Anwendungsebene, speziell die Integrität der Antworten im *Domain Name System* (DNS). Hierzu werden die Antworten von öffentlich verfügbaren DNS-Resolvern untersucht, um Systeme zu identifizieren, welche die DNS-Auflösung manipulieren und somit Anwender auf nicht-legitime Zielsysteme umleiten, die mit verdächtigen oder bösartigen Aktivitäten in Verbindung stehen.

Der zweite Teil dieser Dissertation befasst sich mit potentiellen Gegenmaßnahmen, um einige der Bedrohungen abzuschwächen oder vollständig zu beseitigen. Dazu werden in einem ersten Schritt Malware Blacklisten untersucht, die gegen maliziöse Aktivitäten schützen sollen. Unsere Auswertungen der Blacklistdaten deuten jedoch darauf hin, dass diese Blacklisten nur unvollständig gegen einen Großteil der vorherrschenden Malwarebedrohungen schützen. Weiterhin besteht ein generelles Problem dieser Listen darin, dass sie meist nicht gegen die eigentliche Infektion mit bösartiger Software schützen, da die gelisteten Einträge wie bösartige Domains oft erst von einem System kontaktiert werden, wenn das System bereits kompromittiert ist. Im letzten Abschnitt dieser Arbeit wird daher ein Ansatz vorgestellt, in welchem bösartige Aktivitäten auf Endgeräten möglichst früh identifiziert werden sollen. Dabei werden die Aktivitäten auf den Endgeräten direkt auf dem API- und Systemaufruf-Level überwacht, wohingegen die eigentliche Analyse auf bösartiges Verhalten in einer kontinuierlich gewarteten Cloud-Umgebung durchgeführt wird.