Das Fraunhofer-Institut für Naturwissenschaftlich-Technische Trendanalysen berichtet über Neue Technologien

Moving Target Defence

Ein Problem der IT-Sicherheit ist die Tatsache, dass die zu schüzenden Informationssysteme üblicherweise eine eher statische Konfiguration haben und potenziellen Angreifern genügend Zeit bieten, einen Angriff vorzubereiten und durchzuführen. Hier setzt das neue Konzept der Moving Target Defence (MTD) an. Es basiert auf der Implementierung von außen nicht vorhersehbarer ständiger Veränderungen der IT-Konfiurationsparameter und erinnert damit an die zum Schutz von Kommunikationsverbindungen schon länger genutzten Frequenzsprungverfahren. Es gibt unterschiedliche Methoden der MTD, die sich derzeit alle noch mehr oder weniger im Forschungsstadium befinden.

MTD grenzt sich zur konventionellen IT-Sicherheit deutlich ab. Deren grundlegende Herangehensweise ist es, alle potenziellen Sicherheitslücken des Systems zu identifizieren und zu beseitigen. Dies gelingt am besten mit gut ausgetesteten, statischen Konfigurationen, die in der Regel über eine längere Zeit unverändert bleiben. Im Gegensatz dazu geht MTD davon aus, dass es unmöglich ist, alle Sicherheitslücken vollständig zu schließen, bedingt durch den hohen Vernetzungsgrad, die große Komplexität heutiger Komponenten und die begrenzten menschlichen Fähigkeiten. Trotzdem soll dem Angreifer die Durchführung seiner Angriffe so weit wie möglich erschwert werden. MTD fokussiert sich dabei auf die erste Phase eines Angriffs, die Erkundung des Ziels. In der Praxis erfolgt ihre Umsetzung dadurch, dass mehrere Systemkonfigurationen gezielt manipuliert werden. Diese verändern kontrolliert die Angriffsfläche, auf der ein Angreifer mit dem System in Kontakt tritt. Am besten gelingt das mit möglichst flexiblen und veränderbaren Systemen, die dynamische Konfigurationen enthalten. Damit werden für den Angreifer nicht nur die Unsicherheit und die Komplexität bei der Erkundung erhöht, sondern auch die Möglichkeiten zur Identifizierung der anfälligen Systemkomponenten verringert und höhere Aufwendungen für die Durchführung seiner Angriffe erzwungen.

Im Rahmen von Forschungsvorhaben sind MTD-Anwendungen für einzelne Server und kleinere Netzwerke bereits prototypisch implementiert worden. Daneben ist der praktische Einsatz in vielen weiteren Bereichen künftig denkbar. Bei herkömmlichen Netzwerken ändern beispielsweise MTD-Ansätze die homogenen und statischen Konfigurationen. Dies erfolgt in der Regel durch spezifische Werkzeuge, mit denen Administratoren effektive Konfigurationen gemeinsam mit intelligenten Mechanismen zur Anpassung an gegnerische Angriffe erzeugen können. Damit sollte der Schutz vor einer Vielzahl bekannter Angriffsmuster möglich sein. Ein weiterer, ebenfalls denkbarer Anwendungsbereich sind Softwaredefinierte Netzwerke, die durch Entkopplung der Steuerungsebene von der Datenebene einem vernetzten System Flexibilität, Robustheit und Programmierbarkeit verleihen. Solche Eigenschaften eignen sich hervorragend für die Implementierung dynamischer Konfigurationen.

Cloud Computing ist ebenfalls ein mögliches Einsatzgebiet. Es umfasst sowohl internetbasierte Anwendungen, die als Dienste bereitgestellt werden, als auch Hardware und Systemsoftware in den Rechenzentren, die diese Dienste bereitstellen. Der Nachteil der zentralisierten Cloud-Lösungen besteht jedoch darin, dass sie das Risiko nicht verteilen, sondern auf einen einzigen Punkt fokussieren. Dieser kann leicht angegriffen werden. Darüber hinaus verwendet Cloud Computing in der Regel eine Infrastruktur bestehend aus homogenen Komponenten, um eine kosteneffiziente Verwaltung der Ressourcen durchführen zu können. Daher sind erkannte Schwachstellen zumeist auch mehrfach ausnutzbar. MTD-Ansätze werden erforscht, um diese Sicherheitsmängel durch Erhöhung der Vielfalt verwendeter Komponenten und durch kontinuierliche Konfigurationsänderungen abzumildern.

Auch beim Internet der Dinge, also einer Netzwerkumgebung, die durch miteinander interagierende, heterogene Geräte gekennzeichnet ist, kann MTD zur Anwendung kommen. Charakteristisch sind dabei die begrenzten Ressourcen, wie Bandbreite, Rechenleistung und Energie. Herkömmliche Ansätze aus der IT-Sicherheit (z. B. die Verwendung von Antivirensoftware und Firewalls für Endpunkte) wirken hier nur eingeschränkt, da sie größere Ressourcen benötigen als verfügbar sind. Angriffe können daher die permanente Bereitstellung von Diensten wesentlich stören. Aktuell untersucht werden MTD-Ansätze, die solche Umgebungen vor den dort häufig vorkommenden Aufklärungs- und kryptografischen Angriffen schützen.

Mit den aktuellen Entwicklungen im Bereich des autonomen Fahrens hat auch die Bedeutung der Absicherung von Fahrzeugnetzen stark zugenommen. Zum Schutz der Netze – und hier besonders der wichtigen Daten aus den Steuergeräten der Fahrzeuge – wurden mehrere MTD-Ansätze entwickelt. Ein wesentliches Hauptanliegen besteht darin, Angriffen entgegenzuwirken, die Informationen aus den Steuergeräten ausspähen, um diese zu verändern und an andere kritische Komponenten weiterzuleiten.

Insgesamt gesehen begünstigen sich MTD und konventionelle Ansätze der IT-Sicherheit gegenseitig. Auf der einen Seite lassen sich beispielsweise mit Intrusion Detection Systemen gewonnene Informationen für MTD nutzen, um Konfigurationsänderungen auszulösen und damit die Angriffsfläche zu verändern. Auf der anderen Seite kann MTD über Konfigurationsänderungen helfen, dass sich konvenionelle IT-Sicherheitsmechanismen dynamisch anpassen und damit die beispielsweise durch reine Ausspähung der Wirkungsweise einer Firewall entstandenen Sicherheitslücken geschlossen werden können. Zudem lassen sich über die durch MTD verursachte höhere Komplexität einer Angriffsoperation auch Erkenntnisse über Angriffsmuster oder Verhaltensweisen potenzieller Angreifer gewinnen und konventionellen Ansätzen der IT-Sicherheit zur Verfügung stellen. Allerdings besteht je nach konkreter Implementierung auch die Möglichkeit, dass sich MTD und konventionelle IT-Sicherheit gegenseitig behindern, da die Aspekte ihrer Kooperation noch nicht ausreichend untersucht worden sind.

Dr. Dirk Thorleuchter