Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR
SICHERE INFORMATIONSTECHNOLOGIE

Fraunhofer-Institut für Sichere Informationstechnologie SIT

Kontakt:
Dr. Kpatcha Bayarou
Rheinstraße 75
64295 Darmstadt

Telefon 06151 869-274
Fax 06151 869-224
kpatcha.bayarou@sit.fraunhofer.de

www.sit.fraunhofer.de

AUTOSEC

AUTOMATISIERTE NETZWERKSICHERHEIT FÜR SDN UND CONNECTED CLIENTS

Software-Defined Networking (SDN) bietet Möglichkeiten, Netzwerke mithilfe eines zentralen Netzwerk-Controllers effizienter und leichter zu managen. Viele Unternehmen haben sich aufgrund der größeren Flexibilität und möglichen Kostenreduzierung bereits für SDN entschieden. Mit der Entwicklung von AutoSec macht sich das Fraunhofer SIT die Vorteile von SDN zunutze, indem neue Schutzmechanismen in SDN-basierte Netzwerke integriert und Endgeräte mit eingebunden werden.

Software-Defined Networking (SDN) und Network Functions Virtualization (NFV)

Das SDN-Konzept basiert auf der Trennung der Kontrollschicht (Control Plane) von der Datenschicht (Data Plane): Während ein SDN-Controller (Control Plane) Entscheidungen aufgrund von Weiterleitungsregeln trifft, führen Router, Switche etc. (Data Plane) diese Entscheidungen aus. Diese zwei Schichten kommunizieren mittels Protokollen wie z.B. OpenFlow. Zusätzlich können Hersteller von SDN-Netzwerkkomponenten mit NFV ihren Kunden ein einheitliches Konfigurationsmanagement sowie eine programmierbare zentralisierte Kontrolle über das gesamte Netzwerk anbieten.

Integration angeschlossener Endgeräte

AutoSec integriert Endgeräte wie Workstations oder Laptops in SDN und NFV, indem es ihre Konfiguration programmierbar macht. Im Fall eines Sicherheitsrisikos, das durch ein Netzwerküberwachungssystem erkannt wurde, ist AutoSec in der Lage, Sicherheitsregeln dynamisch anzuwenden, um Maßnahmen zur Behandlung des Vorfalls auszuführen. Wenn sich zum Beispiel ein Computerwurm innerhalb eines Unternehmensnetzwerks ausbreitet, weist AutoSec die Netzwerkkomponenten an, die Vervielfältigung des Wurms zu verhindern und die betroffenen Clients zu isolieren. Anschließend konfiguriert AutoSec die nicht infizierten Clients neu, um diese gegen den Wurm zu immunisieren.

Dynamische Sicherheit

Um miteinander verbundene Geräte in die Netzwerkschutz-Strategie zu integrieren, setzt AutoSec Managementwerkzeuge zur Systemkonfiguration ein. Abhängig von der jeweiligen Bedrohungssituation in einem Netzwerk, ist AutoSec in der Lage, die folgenden Sicherheitsmechanismen zu aktivieren:

- Verschlüsselung und Integritätsschutz von Netzwerkverbindungen
- Aktivierung oder Änderung von Firewall-Regeln
- Einsatz von Werkzeugen zur Malware-Erkennung und -Beseitigung
- Einsatz zusätzlicher Werkzeuge zur Netzwerküberwachung, um detaillierte Angriffsinformationen zu erhalten
- Individuelle Fernkonfiguration von Geräten und Services

Weitere Funktionen können durch die Geräte- und Netzwerkbetreiber definiert werden.

AutoSec befindet sich momentan in der Proof of Concept-Phase. Das Fraunhofer SIT bietet SDN und Data Center-Betreibern, Internet Service Providern, Anbietern von Konfigurationsmanagement-Werkzeugen und Telekommunikationsanbietern an, AutoSec in ihre Produkte, Netzwerke und Services zu integrieren.