idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Fraunhofer-Institut für Sichere Informationstechnologie (SIT)
Oliver Küch

05.10.2015
http://idw-online.de/de/news638838

Forschungs- / Wissenstransfer, Forschungsergebnisse
Informationstechnik, Maschinenbau, Wirtschaft
überregional

Sicherheitswächter für Netze der Zukunft

Fraunhofer zeigt Security-Cockpit für SDN – OrchSec bietet einfaches Monitoring und automatisierte Abwehr von Netzwerkangriffen

Mit Software-Defined Networking (SDN) können Unternehmen ihre Computer-Netzwerke flexibel managen und so Kosten sparen. Zur Absicherung dieser software-basierten Netze hat Fraunhofer SIT OrchSec entwickelt, eine Konzeptstudie, mit der sich Angriffe auf SDN-Netzwerke automatisiert erkennen und abwehren lassen. Das Besondere an der Entwicklung, die das Institut vom 6. bis 8. Oktober auf der it-sa Sicherheitsmesse in Nürnberg am Stand 436 zeigt: Die Abwehrmechanismen sind in einzelne Software-Module gekapselt, die sich besonders leicht anpassen und ergänzen lassen. Mit Hilfe des OrchSec-Konzepts und den Software-Modulen des Fraunhofer SIT können etwa Hersteller von SDN-Controllern die Sicherheit ihrer Produkte enorm verbessern. Weitere Informationen zu OrchSec und dem SDN-Sicherheitslabor des Fraunhofer SIT finden sich im Internet unter www.sit.fraunhofer.de/sdn-security-lab .

Herkömmliche Netzwerke bestehen aus unterschiedlichen Komponenten, die aufwendig abgestimmt werden müssen. Deshalb nutzen immer mehr Unternehmen Software-Defined Networking: Damit lässt sich das gesamte Unternehmensnetzwerk zentral steuern und flexibel auf unterschiedliche Situationen anpassen. Mittels Virtualisierung werden Kontrollschicht (Control Plane) und Datenschicht getrennt. Während die Datenschicht in den Geräten – Router, Switches, Firewalls – nur noch das Empfangen und Senden von Paketen übernimmt, bilden ein oder mehrere Controller eine Kontrollschicht. Diese übernimmt die gesamte Flusskontrolle und regelt die Verarbeitung der Datenströme. Das macht sie jedoch auch zu einem attraktiven Ziel für Hacker. Mit OrchSec erhalten SDN-Netze eine weitere Schicht, die sicherheitsrelevante Informationen sammelt und analysiert. Mit deren Hilfe lassen sich typische Angriffe erkennen und passende Schutzreaktionen auslösen.

OrchSec erkennt zum Beispiel ARP Spoofing, Distributed Denial of Service (DDoS), TCP Slow Read und Distributed Reflected Denial of Service Angriffe (DRDos) wie DNS Amplification. Die jeweiligen Abwehrmaßnahmen sind in Apps organisiert und lassen sich über eine Programmierschnittstelle einfach an die Unternehmensbedürfnisse anpassen und um beliebige neue Funktionen und Schutzmechanismen erweitern. Gleichzeitig visualisiert OrchSec Auslastungs- und Performance-Indikatoren, und bietet dem Netzwerk-Administrator alle sicherheitsrelevanten Informationen auf einen Blick. Auf der Messe sucht das Entwicklerteam nach Partnern für Produktentwicklung und praktische Erprobung.