Mehr Sicherheit für Netzwerke

Anomalieerkennung zum Schutz vor Cyberangriffen

Bernhard Reimann

Anomalieerkennung gewinnt im Kampf gegen immer raffiniertere Cyberangriffe stark an Bedeutung. Während klassische Signaturverfahren bekannte Muster zuverlässig identifizieren, versagen sie häufig bei neuartigen Angriffstaktiken, die sich dynamisch anpassen und gezielt unauffällig agieren. Moderne Anomaliesysteme setzen deshalb auf statistische Modelle und maschinelles Lernen, um subtile Abweichungen in Datenströmen frühzeitig sichtbar zu machen. Für sicherheitskritische Infrastrukturen eröffnet dieser Ansatz die Chance, Bedrohungen nicht nur zu erkennen, sondern auch proaktiv einzugrenzen. Gleichzeitig stellt die Vielfalt legitimer Verhaltensmuster Netzwerkbetreiber vor komplexe Herausforderungen, die eine präzise Bewertung von Risiken und Fehlalarmen erfordern.

Eine weitreichende Protokollierung des Daten-Verkehrs in einem Netzwerk ermöglicht Plausibilitätsprüfungen etwa von Fernwirkprotokollen sowie eine schnelle Alarmierung bei verdächtigem Netzverkehr (Foto: Pete Linforth, Pixabay)

Anomalieerkennung sowie das Schwachstellenmanagement sind heute wichtiger denn je. Die Bedrohungen durch Cyberangriffe auf digitale Infrastrukturen steigen kontinuierlich. Laut Bitkom entsteht der deutschen Wirtschaft durch Cyberattacken jährlich ein Schaden von gut 179 Milliarden Euro; 65 Prozent der Unternehmen sehen ihre Existenz durch einen erfolgreichen Cyberangriff bedroht. Vor allem der Schutz der Datennetze hat oberste Priorität, gleichzeitig stehen Netzbetreiber vor enormen technischen und organisatorischen Herausforderungen. Syserso Networks unterstützt mit jahrzehntelanger Expertise Unternehmen bei der Absicherung und Stabilisierung digitaler Infrastrukturen. Das Unternehmen bietet umfassende Lösungen, um Netzwerke, insbesondere in kritischen Infrastrukturen und Weiterverkehrsnetzen (WANs), zuverlässig zu schützen und die Betriebssicherheit langfristig zu gewährleisten.

Ein zentrales Element dieser Sicherheitsstrategie ist die Anomalieerkennung. Sie ermöglicht die Identifikation ungewöhnlicher oder verdächtiger Aktivitäten in Netzwerken in Echtzeit. Diese Netze sind entscheidend für Kommunikation und Betrieb von Industrieanlagen, Energieversorgungssystemen oder Behörden – entsprechend hat ihre Sicherheit höchste Priorität. Durch die kontinuierliche Analyse des Datenverkehrs werden Muster erkannt, die von der Norm abweichen. Zum Einsatz kommen häufig Machine-Learning-Verfahren als auch regelbasierte Analysen. Ziel ist es, potenzielle Cyberangriffe, Fehlkonfigurationen oder defekte Geräte frühzeitig zu erkennen, um Schäden zu verhindern, bevor sie entstehen.

Sicherer Netzwerkbetrieb

Eine umfassende, sichere Überwachung des relevanten Verkehrs in Transportnetzen sowie eine schnelle Klassifizierung auffälli-

Bernhard Reimann ist Chefredakteur der NET

ger Ereignisse sind für die Cyberabwehr entscheidend. Darüber hinaus müssen die dafür eingesetzte Hard- und Software aktuell gehalten werden – ganz zu schweigen vom notwendigen Know-how der Mitarbeitenden. Beides verursacht nicht zu unterschätzende Kosten. Die Syserso Networks GmbH ist auf den Schutz und den zuverlässigen Betrieb von Netzwerken unter anderem auch aus dem Bereich kritischer Infrastrukturen spezialisiert.

Dank moderner Technologien und ausgereifter Monitoring-Tools analysieren die Systemspezialisten von Syserso Networks Netzwerkdaten in Echtzeit und identifizieren Anomalien, die auf drohende Störungen oder Sicherheitsprobleme hindeuten.

Angriffsfläche Datentransport

Eine der Herausforderungen in Netzwerken und damit für Netzbetreiber ist der Transport großer Datenmengen über lange Strecken. Dabei entstehen zahlreiche potenzielle Angriffspunkte, die von Cyberkriminellen genutzt werden können. Klassische, primär signaturbasierte Sicherheitslösungen wie Firewalls oder einfache Intrusion-Detection-Systeme stoßen hier an Grenzen, weil sie oft nur auf bekannte Bedrohungen reagieren. Anomalieerkennung hilft, auch unbekannte oder neuartige Angriffsmuster aufzudecken, indem sie auf ungewöhnliche Abweichungen im Netzwerkverhalten achtet.

„In Netzwerken der kritischen Infrastruktur ist der Schutz besonders komplex, da es sich oft um heterogene Systeme mit verschiedenen Protokollen und Geräten handelt. Ein herkömmlicher Angriff kann hier schwerwiegende Konsequenzen haben, beispielsweise einen Ausfall der Stromversorgung oder der Verkehrssteuerung“, führt Verena Klein, Marketingleiterin bei Syserso Networks, aus. Die Anomalieerkennung unterstützt Systemoperatoren dabei, solche Bedrohungen frühzeitig festzustellen, indem sie ungewöhnliche Kommunikationsmuster zwischen Steuerungssystemen, Sensoren und übergeordneten Kontrollsystemen überwacht. „Sie erleichtert die Erkennung von Sicherheitslücken und unzulässiger Geräte im Netz“, ergänzt Klein. „Eine weitreichende Protokollierung des Verkehrs ermöglicht Plausibilitätsprüfungen etwa von Fernwirkprotokollen sowie eine schnelle Alarmierung bei verdächtigem Netzverkehr.“

Ein weiteres Problem ist die Unterscheidung zwischen echten Bedrohungen und harmlosen Abweichungen. Ingenieure müssen daher das Verhalten ihres Netzwerks gut kennen, um Fehlalarme zu minimieren. Moderne Systeme nutzen daher bereits KI-gestützte Algorithmen, die sich an das normale Netzwerkverhalten anpassen und zwischen kritischen und unkritischen Ereignissen unterscheiden.

Secure Gateways schützen

Für die sichere Standortvernetzung, wie zum Beispiel bei der Fernwirktechnik/SCADA, bietet Syserso Networks Secure Gateways an. Diese ermöglichen IPsec-verschlüsselte Datenübertragung in die Zentrale, stellen Firewall-Funktionalität bereit und unterstützen verschiedene Übertragungsmedien. So lassen sich entfernte Standorte mit einem kompakten Gerät effektiv gegen unterschiedliche Cyberbedrohungen absichern.

Mit Anomalieerkennung lassen sich Netzwerke proaktiv schützen, indem auch unerwartete Abweichungen erkannt werden, die klassische Lösungen übersehen. Das ist insbesondere in Transportnetzen, WANs und kritischen Infrastrukturen essenziell – dort, wo ein Angriff besonders schwerwiegende Folgen haben kann.

www.syserso.com