Foto: opolja – stock.adobe.com

Gegen böswillige Angriffe auf IT-Strukturen hilft ein System zur Anomaly Detection (deutsch: Anomalieerkennung).

Digitales Immunsystem

Wer seine Geschäftsprozesse erfolgreich digitalisieren möchte, braucht eine Sicherheitslösung, die ungewöhnliche Verhaltensmuster erkennt.

JAKOB SCHMIDT & GIUSEPPE D'AMICIS

Da die Netzwerke von Kritischen Infrastrukturen (KRITIS) im Laufe der Zeit durch hinzukommende IT-Komponenten immer komplexer werden, haben Hacker mehr denn je leichtes Spiel. So ist Schadsoftware, die beispielsweise ganze Energieanlagen lahmlegen kann, längst keine Ausnahme mehr und der Bedarf an strategischer Cybersecurity steigt. Im Idealfall behindern die eingesetzten Lösungen laufende Prozesse nicht und melden jede Störung zuverlässig und umgehend.

Immer wieder kommt es zu gezielten Attacken auf sensible IT-Systeme, auf das Stromnetz und andere Infrastrukturen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) registriert eine kontinuierliche Zunahme solcher Attacken. Das zeigt mehr als deutlich, dass dringender Handlungsbedarf für einen verlässlichen Schutz von computergestützten Arbeitsplätzen und Unternehmensabläufen besteht.

KRITIS-Betreiber setzen Industrial Control Systems (ICS) ein, um ihre technischen Prozesse zu steuern. Ein solches System ist etwa Scada (Supervisory Control and Data Acquisition), mit dem übergeordnete Steuerungsdaten gesammelt werden können. Angreifer besitzen detailliertes Know-how über solche Systeme und ihre Schwachstellen und nutzen dieses Wissen für ihre Zwecke aus.

Durchdachtes Sicherheitskonzept

Gegen solche Angriffe hilft ein System zur Anomaly Detection (deutsch: Anomalieerkennung). Ob ein Netzwerkgerät plötzlich ein anderes Kommunikationsprotokoll nutzt, oder Netzwerkverkehr ungeplant eine neue Route nimmt – ein derartiges System erkennt solche Vorgänge frühzeitig und alarmiert die entsprechenden Stellen. Um eine Anomalie, also eine Normabweichung beziehungsweise ein unerwartetes Verhalten überhaupt als solche zu identifizieren, muss zuerst einmal der Normalzustand erfasst werden. Dazu analysiert das System die IT-Architektur und lernt im Hintergrund.

Nach Abschluss dieser „Lernphase" sind Lösungen zur Anomalieerkennung in der Lage, das Verhalten einer Schadsoftware als ungewöhnlich einzustufen. Allein der Versuch, einen Treiber zu installieren beziehungsweise zu manipulieren oder einen unberechtigten Zugang zum Internet herzustellen, etwa um weitere Komponenten einer Schadsoftware nachzuladen, wird als Anomalie erkannt. Neben der Angriffserkennung bieten solche Systeme einen weiteren entscheidenden Vorteil: Durch sie lassen sich alle Teilnehmer der Netzwerkkommunikation identifizieren und per Monitoring abbilden. Ein großer Zusatznutzen für gewachsene Systemlandschaften, in denen viele Assets nicht als solche registriert sind.

Zusätzlich bereitet die Lösung Logfiles automatisch auf, alarmiert bei Auffälligkeiten und entlastet so Administratoren

in IT-Abteilungen, die ihre Kapazitäten für andere Aufgaben einsetzen können. Als Ergänzung zu klassischen Sicherheitsmaßnahmen bietet ein solches System einen deutlichen Mehrwert für die IT-Sicherheitslandschaft und trägt dazu bei, das Security-Level maßgeblich zu verbessern.

Die lernfähige Allzweckwaffe

Die Securitylösung Silentdefense von Forescout (ehemals Securitymatters) ist eine solche intelligente Überwachungslösung, die sowohl passiv als auch aktiv eingesetzt werden kann. Sie beobachtet das Verhalten von Netzwerknutzern und angeschlossenen Systemen, um Prozessanomalien, Maschinenstatus, unsicheren Zugriff und potenziell schädliche Aktivitäten zu erkennen. Grundlage ist eine detaillierte Bestandsaufnahme aller Komponenten von Infrastrukturen. Silentdefense basiert auf patentierten maschinellen Lernfunktionen zur Überwachung von ICS-Netzwerken, -Protokollen und -Semantik. Der Systemintegrator Telent GmbH – ein Unternehmen der Euromicron Gruppe, und dessen auf Cybersicherheit spezialisierte Tochter Koramis setzen diese Lösung ein, um den gestiegenen Anforderungen an Security Rechnung zu tragen. Als Spezialist für Planung, Aufbau und Betrieb von ITK-Systemen im Bereich KRITIS verfügt telent über umfassende Praxiserfahrung. Koramis bringt darüber hinaus spezialisierte Expertise für ganzheitliche Lösungen rund um Cybersecurity, Automatisierungs-, Prozess- und Netzleittechnik mit.

2.100

ICS-SPEZIFISCHE Prüfungen umfasst die umfangreiche Bibliothek für industrielle Bedrohungen in der Anomalieerkennungssoftware.

Grundvoraussetzung für die erfolgreiche Überwachung ist die Erfassung des Netzwerkzustands und aller Geräte im Netzwerk sowie die Analyse der Kommunikationsflüsse. Sensoren an Schnittstellen speichern Informationen, Parameter und Werte und lernen so Verhaltensmuster, die per Networkmap festgehalten werden. Dabei spürt die Lösung Netzwerk-, Betriebs- und Sicherheitsprobleme sowie Bedrohungen „out of the box“ auf, wie unerlaubte Zugriffe und Datenflüsse, Manipulations- und Zugangsversuche von außen oder Fehlkonfigurationen von Firewall- und Netzkomponenten. Darüber hinaus informiert es über unsichere Protokolle, falsche Messergebnisse, Verbindungsprobleme zwischen Geräten, Softwarebugs, instabile Prozesse, nicht eingehaltene Protokoll-Spezifikation, Anomalien oder Stillstand der Schaltanlagen sowie unkontrollierte Regelschalterbedienung.

Einfach zu integrieren und skalieren

Ein weiterer Vorteil der Lösung ist die Kompatibilität mit mehr als 120 Protokollen. Sie umfasst zudem eine umfangreiche Bibliothek für industrielle Bedrohungen (Threats) mit über 2.100 ICS-spezifischen Prüfungen und stellt zeitnah Updates zu neuen Bedrohungen bereit. Sie lässt sich nahtlos in das gesamte Ökosystem eines Unternehmens integrieren, einschließlich der Lösungen für Security Information and Event Management (SIEM). Die Lösung ist skalierbar und kann ohne Neuinstallation um weitere benutzerdefinierte Monitoring- oder Analysefunktionen erweitert werden. Die Auswertung erfolgt schließlich über eine Web-Oberfläche. Mittels eines konfigurierbaren Dashboards werden Nutzern Echtzeit- und forensische Netzwerkanalysen bedienungsfreundlich angezeigt. ■

JAKOB SCHMIDT, COORDINATOR AWARENESS, KORAMIS GMBH & GIUSEPPE D'AMICIS, HEAD OF MARKETING UND MITGLIED DES SECURITY INCIDENT RESPONSE TEAMS DER TELENTGMBH.

telent GmbH:
www.telent.de