Bild: NanoStockk/iStock.com

Offene Datenplattform für durchgängige Sicherheit

Die Analyse von Log-Daten aus unterschiedlichen Quellen, kombiniert mit künstlicher Intelligenz, ist eine hervorragende Basis für umfassende Sicherheitsanwendungen.

Geht es um die Erkennung und Abwehr von Cyber-Gefahren, werden Log- und Telemetrie-Daten von Firewalls, Cloud-Anwendungen und Endpunkten meist nur teilweise genutzt. Dies obwohl die Logs zahlreiche Informationen enthalten, die sich auch für weitergehende Analysen eignen – namentlich dann, wenn Informationen aus verschiedenen Quellen kombiniert betrachtet werden. So wird aus separaten Datensilos ein kompletter «Data Lake», der mehr Erkenntnisse birgt als die Summe der einzelnen Logfiles. Palo Alto Networks stellt mit Cortex Data Lake, Cortex XDR und Cortex Hub eine universelle Plattform zur Auswertung der Log-Informationen seiner Produkte bereit. Dazu gehören die Next-Generation-Firewalls, die Endpoint-Protection-Lösung Traps sowie Cloud-Services.

KI-gestützte, kombinierte Analyse

Cortex Data Lake sammelt und integriert die Sicherheitsdaten von Netzwerk-, Endpunkt- und Cloud-Services. Cortex XDR normalisiert und korreliert die Daten und analysiert das Nutzerverhalten. Das schafft Transparenz über die Sicherheitslage und bildet die Basis für fortgeschrittene Analysen (dies mit Unterstützung durch künstliche Intelligenz und maschinelles Lernen). Nebst den Log-Daten werden dabei Daten aus dem Malware-Prevention-Service WildFire von Palo Alto Networks genutzt, der laufend Bedrohungsinformationen von zehntausenden Unternehmen sammelt. Der Threat-Intelligence-Service AutoFocus klassifiziert diese Informationen, setzt sie in Kontext und erlaubt detaillierte Analysen. Auch das von Palo Alto Networks initiierte, in Cortex integrierte Open-Source-Tool MineMeld fasst Daten zu Cyber-Bedrohungen aus verschiedenen Quellen zusammen und ermöglicht, Firewall-Regeln dynamisch der Situation anzupassen.

Marktplatz für Sicherheitsanwendungen

Der Cortex Hub stellt Sicherheitsanwendungen auf Basis der Cortex-Plattform zur Verfügung – und zwar Apps von Palo Alto Networks und Apps von Drittanbietern (aktuell rund 40 Anwendungen).

Cortex wird damit zur offenen, integrierten Plattform für Sicherheitsanwendungen verschiedener Anbieter, die herstellerübergreifend analysieren und kommunizieren. Cortex XDR ist eine der von Palo Alto Networks selbst bereitgestellten Apps im Cortex Hub. Sie führt eine Verhaltensanalyse aufgrund von Netzwerk-, Cloud- und Gerätedaten durch, erkennt so das normale Verhalten und gibt bei Abweichungen Alarm. Zum Beispiel, wenn von einer Workstation in der Buchhaltung aus plötzlich auf einen Industrieroboter zugegriffen wird. Cortex XDR kombiniert dabei alle Datenquellen und überwacht den gesamten Weg der Daten auf dem Endpunkt, im Netzwerk und in der Cloud.

Sicherheit für medizintechnische Geräte

Medigate ist eine weitere App aus dem Cortex Hub, die vom gleichnamigen Hersteller spezifisch für das Gesundheitswesen entwickelt wurde. Die Anwendung erkennt anhand der Logdaten medizinisches Equipment wie Röntgengeräte, Bildserver, Defibrillatoren, Dosierpumpen etc.

Mit den aus den Geräteinformationen gewonnenen Erkenntnissen kann Medigate erstens ein Inventar aller medizintechnischen Geräte einer Klinik erstellen – in manchen Institutionen keine Selbstverständlichkeit. Zweitens kann die App die Gerätedaten mit Tags anreichern, die dann von der Firewall bei der Anwendung von Regeln genutzt werden. Auf diese Weise ermöglicht Medigate, automatisiert eine stringente Sicherheitsstrategie nicht nur für die IT, sondern auch für den oft schlecht geschützten und nur selten mit Updates versorgten medizintechnischen Gerätepark zu implementieren und das Risiko, das solche IoT/IoMT-Geräte bergen, deutlich zu senken.

Palo Alto Networks Cortex: die Highlights

- Offene, integrierte Plattform für durchgängige Sicherheit
- Unterstützt durch künstliche Intelligenz und maschinelles Lernen
- Kombinierte Analyse von Sicherheitsdaten aus Endpunkten, Firewalls und Cloud-Diensten
- Skalierbar bis zu grössten Umgebungen
- Hub für Sicherheitsanwendungen von Palo Alto Networks, Drittanbietern und Anwendern

Medigate: die Highlights

- Erkennung medizintechnischer Geräte anhand von Logdaten
- Komplettes Inventar des medizinischen Geräteparks, Anreicherung durch kontextuelle Informationen
- Identifikation der Gerätetypen mit Tags
- Auf das Gesundheitswesen adaptierte Analysen und Kontrollen
- Automatische Anwendung von Firewall-Regeln für Geräte und Gerätetypen

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58
5430 Wettingen
Tel. 056 437 60 60

info@boll.ch
www.boll.ch