Schwachstellen in OT-Systemen im Griff

Konventionelle Cybersicherheitstools für das Vulnerability- und Konfigurationsmanagement kennen sich nicht mit der Bedrohungslage bei industriellen Kontroll- und Steuerungssystemen aus. Ein OT-spezifischer, standardisierter Datenfeed kann helfen. Bernhard Aregger von BOLL Engineering erklärt im Interview, wie es funktioniert.

OT-Systeme und Cybersecurity – wie ist hier der Status?

Bernhard Aregger: Analog zu IT-Systemen sind auch Systeme der Operational Technology (OT), darunter SCADA-Server (Supervisory Control and Data Acquisition) und industrielle Kontroll- und Automatisierungssysteme (IACS), nicht vor Cyberangriffen sicher, wie die Praxis auch in der DACH-Region immer wieder zeigt. Cyberangriffe nutzen Schwachstellen in diesen Systemen, um einzudringen und Schaden anzurichten. Und solche Schwachstellen sind keineswegs selten: Die National Vulnerability Database (NVD) der US-Standardbehörde NIST verzeichnet Tausende Sicherheitslücken in industrieller Automatisierungssoftware.

Worin liegt dabei das Problem im Vergleich zu IT-Systemen?

Die gängigen Vulnerability- und Configuration-Management-Tools nutzen die Forschung der Hersteller und die gesammelten Vorfallsdaten, genannt auch Threat Intelligence, um Schwachstellen zu identifizieren und zu neutralisieren oder Vorschläge zu deren Behebung zu liefern. Die Tools kennen sich bestens mit Schwachstellen in IT-Systemen aus. Dagegen mangelt es generell an Threat Intelligence zu OT-Systemen mit ihren teils proprietären und sehr spezifischen Protokollen. Es braucht also Lösungen, die auch die OT-Welt kennen und über entsprechende Daten verfügen.

Wie gehen Security-Lösungen mit Daten zu Schwachstellen um?

Schwachstelleninformationen erreichen Sicherheitstools unter anderem in Form von maschinenlesbaren Datenfeeds. Diese können von der Threat Intelligence des Tool-Herstellers, aber auch aus anderen Quellen stammen. Es gibt für die Übertragung von Schwachstelleninformationen zwischen verschiedenen Sicherheitstools und -diensten einen Open-Source-Standard namens OVAL (Open Vulnerability and Assessment Language).

Bernhard Aregger ist Sales Specialist bei BOLL und in dieser Rolle unter anderem für die Produkte von Kaspersky zuständig.

Wie nutzt man solche Feeds konkret?

OVAL-Feeds lassen sich mithilfe von Open-Source-OVAL-Interpretern in kompatible Schwachstellenmanagementlösungen integrieren und liefern, üblicherweise in einem XML-Format, detaillierte Informationen zu erkannten Schwachstellen. Die Angaben enthalten etwa Beschreibung, Name und Version der betroffenen Software sowie Schweregrad und CVSS-Score. Darüber hinaus können solche Feeds Anleitungen zur Schadensbegrenzung enthalten.

Das klingt theoretisch – existieren OT-bezogene OVAL-Feeds tatsächlich?

Ja, ein Beispiel ist der Kaspersky Industrial OVAL Feed for Windows. Er basiert auf Daten aus verschiedenen offiziellen Quellen wie NVD, MITRE und US-CERT, aber auch von Security- und OT-Anbietern sowie Anwender-Communitys. Eigene Recherchen des ICS-Cert-Teams von Kaspersky ergänzen diese Informationen aus Drittquellen. Das Team analysiert alle Daten und hält Ausschau nach möglichen Fehlinformationen, die der korrekten Identifizierung und Bewertung der Schwachstellen entgegenstehen.

Welche OT-Systeme deckt der Feed ab?

Der Feed berücksichtigt die OT-Produkte global führender Hersteller wie Siemens, Schneider Electric, Yokogawa und Emerson. Weitere Systeme können nach Bedarf der Kunden ergänzt werden. Die im Feed empfohlenen Schadensbegrenzungsmassnahmen basieren auf der Erfahrung des ICS-Cert-Teams und folgen den Empfehlungen des jeweiligen OT- beziehungsweise SCADA-Anbieters.

Und welche Lösungen verstehen sich auf OVAL?

Naturgemäss kommt hier die Lösung KICS von Kaspersky ins Spiel (Kaspersky Industrial CyberSecurity). Der Industrial OVAL Feed for Windows ist integraler Bestandteil dieser auf OT spezialisierten, umfassenden Sicherheitsplattform, die praktisch alle Aspekte der industriellen Überwachungs-, Steuerungs- und Automatisierungsprodukte abdeckt – von SCADA-Systemen bis zu Steuerelementen wie PLCs. OVAL wird zudem von verschiedenen weiteren Anbietern unterstützt. Beispiele sind Red Hat mit direktem Support für OVAL-Definitionen in Enterprise Linux und Cisco.

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58 | 5430 Wettingen
Tel. 056 437 60 60 | info@boll.ch
www.boll.ch