Anomalieerkennung für kritische Infrastrukturen und die Industrie

Mit der Einführung des IT-SiG 2.0 gewinnt das Thema Anomalieerkennung in der Leit-, Automatisierungs- und Fernwirktechnik in allen Bereichen absolute Aufmerksamkeit. Gründe dafür sind die Frequenz und Komplexität von Cyberangriffen. Die Maßnahmen der Angriffserkennung und -reaktion („Detect and Respond") sind entsprechend wichtig.

Von Dieter Barelmann, VIDEC Data Engineering GmbH

Bis zum 1. Mai 2023 (BSIG § 8a Abs. 1a, EnWG § 11 Abs 1f) verlangen das BSI-Gesetz (§ 2 Abs. 9b, § 8a Abs 1) und Energiewirtschaftsgesetz (§ 11 Abs. 1e) von Betreibern kritischer Infrastrukturen und Energieverteilungsnetzen ein System zur Angriffserkennung (SzA). In weiteren Schritten werden auch andere Bereiche zu diesen Maßnahmen verpflichtet.

Industrielle Cybersicherheitslösungen müssen eine umfassende Übersicht sowie einen tiefen Einblick der zu überwachenden Anlagen zur Verfügung stellen. Aktuellen Angriffen lässt sich entsprechend der Vielfalt von Geräten und Protokollen – auch sehr alten – nur noch bedingt durch eine Absicherung an den Netzgrenzen begegnen. In den meisten Fällen wird bei der Incident-Response (direkte Aktivitäten nach dem Vorfall) und fast immer bei der folgenden Analyse klar, dass es immer Anzeichen im Produktionsnetzwerk gab. Anomalien, also Abweichungen vom Normalbetrieb, sind erste Anzeichen. Eine Angriffserkennung ist somit Stand der Technik und ein absolutes Muss für alle automatisierten Anlagen.

Angriffserkennung

Die Einrichtung einer Angriffserkennung ist in den Ethernet-basierten Netzen schnell umgesetzt. Die vollständige Erfassung und Analyse aller Kommunikationspartner, Assets, Zeitpunkt und Dauer der Kommunikation sowie der gesprochenen Protokolle aller Sitzungen passiert ohne weitere Anpassungen.

Alarmierungen erfolgen dabei ohne Konfiguration auf Basis von Anomalien. Anomalien sind einerseits abweichendes Verhalten vom Normalbetrieb (Fingerprint der Anlage), anderseits sind es auch Protokollfehler und -manipulationen bis hin zur automatisierten Erkennung von Aktivitäten unterschiedlicher Angriffsmodelle.

Die Detektion bietet indirekten Schutz gegen Angriffe auf das Netzwerk und deckt diese frühzeitig auf. Aktuell beträgt die Zeit zwischen Infizierung, also dem Beginn des Angriffs und dem Schadenseintritt circa sieben Monate. Diese „Inkubationszeit" kann mit einer Anomalieerkennung effizient genutzt werden. Für die Reaktion, den „Respond", stehen die aufgezeichneten Daten direkt innerhalb der Alarmierung zur Verfügung und werden für die forensischen Untersuchung gespeichert. Schnell wird klar, ob alle Assets bekannt sind, welche Bedrohungen vorhanden sind und wie bereits vorhandene Maßnahmen helfen. Mit einer Anomalieerkennung wirken die Maßnahmen weit vor dem Eintritt eines Notfalls.

Der ehemals hohe Aufwand für einen Schutz hat sich durch den Einsatz einer Anomalieerkennung stark reduziert. IRMA wurde als Anomalieerkennung, Risikobewertung und Netzplan für Kritis- und Industrieunternehmen entwickelt. Eine Zielsetzung war es, die Security in den Automatisierungsbereichen möglichst einfach mit dem vorhandenen Personal zu bewerkstelligen.

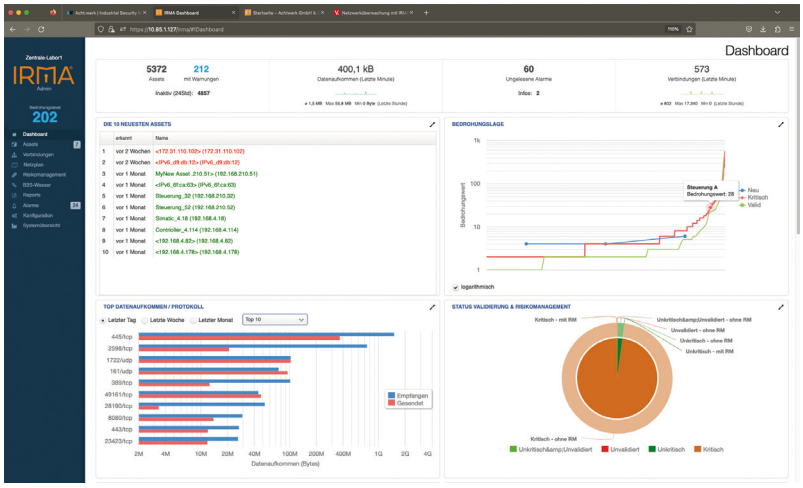
IRMA

Security muss übersichtlich, bedienbar und einfach sein. Dieser Anspruch und das Prinzip „Security by Design" bilden die Grundpfeiler für die Entwicklung von IRMA. Das Resultat ist die Erfüllung der Empfehlungen des BSI CS 134 zum „Monitoring und Anomalieerkennung in Produktionsnetzwerken", des IT-Sicherheitsgesetzes 2.0 und die Verwendung in allen Branchen.

IRMA enthält in der Grundkonfiguration bereits die wichtigsten Kernfunktionen, um die Kritis-Anforderungen der Anomalieerkennung zu erfüllen.

Automatische Erkennung der Assets

Insgesamt geht es um die Erfassung relevanter Protokolldaten der betreffenden Systeme und Netzwerke, die Aufschluss über einen Cyber-



Das Dashboard von IRMA

angriff geben können. Idealerweise mit einer Deep-Packet-Inspection für relevante Protokolle (z. B. 104er Fernwirkprotokoll oder Siemens S7).

IRMA identifiziert vollständig autonom, erfasst und analysiert alle Systeme und Verbindungen ohne jegliche Aktivität im Netzwerk der Produktionsanlage. Diese grundsätzliche Funktion ist im Wesentlichen passiv, bedeutet, dass zunächst kein Teilnehmer aktiv angefragt wird. Ein wichtiger Aspekt, da viele alte Geräte auf solche Abfragen sehr sensibel reagieren und neue Teilnehmer dadurch automatisch erkannt werden. Auch bei segmentierten Netzwerken wird dabei die ganzheitliche Überwachung durch den Einsatz IRMA-Client-TAPs (verteilte Sensoren) gewährleistet.

Eine Anzeige des Bedrohungslevels in Form eines Wertes gibt dem Anwender einen kontinuierlichen Überblick über den Zustand seiner Anlage. Über die Zeit gesehen, lässt sich die Kennzahl auch für eine Langzeitbetrachtung nutzen. Ein nützliches Werkzeug für jeden Anlagenfahrer, der mit einem Blick seine Anlage einschätzen und eventuell notwendige Maßnahmen einleiten kann.

Risikomanagement

Das Risikomanagement unterstützt die Mitarbeiter (IT- und Automatisierungsfacharbeiter) bei der Bewertung eines jeden Assets und ermöglicht die standardkonforme Dokumentation für das Security-Management. Mit der Bewertung der Risiken lassen sich Maßnahmen optimaler planen und bei Anomalien besser einschätzen.

Netzwerkplan

IRMA bietet eine grafische Darstellung des gesamten Netzwerkes mit allen Querverbindungen in der Kommunikation sowie die Auswertungen zu jedem einzelnen Teilnehmer. Jeder Netzwerkplan kann einzeln gespeichert werden, und bei erneuter Öffnung wird der Anwender sofort auf die Änderungen hingewiesen.

Alarmierung

Die Alarmierung bei Anomalien wird in der Bedienoberfläche angezeigt und automatisiert über gesicherte Verbindungen kommuniziert. Es steht mit der Schaltung von potenzialfreien Kontakten eine elektrische Alarmierung direkt in das Leitsystem zur Verfügung. Durch die Vielzahl der elektronischen Datenschnittstellen als restAPI, SMTP oder SFTP ist die Weitergabe und Integration in ein Alarmierungssystem (z. B. AIP) oder in unternehmensweite Security-Information-Event-Management-(SIEM)-Systeme sowie in Information-Security-Management-Systeme (ISMS) aufwandsarm möglich.

Die aktive Suchfunktion

Die Informationen aus dem Datenpool gehen in IRMA grundsätzlich zwei Wege. Zum einen werden die Daten in IRMA analysiert und in der Weboberfläche übersichtlich und verständlich dargestellt. Bei Anomalien erfolgt automatisch eine Alarmierung. Zum anderen werden alle passiv erfassten Netzwerkpakete in einem Speicherbereich gesichert und stehen im Nachgang für eine forensische Analyse über PCAP-Dateien zur Verfügung.

Somit steht mit IRMA der Angriffserkennung im Unternehmensumfeld ein intuitiv bedienbares Paket zur Verfügung. Dabei kann der Betreiber seine Sicherheitsaufgaben auch an ein kompetentes Unternehmen auslagern und IRMA als Sensor für die Datenbeschaffung und Alarmierung verwenden.

Eine SIEM-Integration mittels der integrierten Rest API ist ohne Probleme möglich. In solch einer Konstellation liefert IRMA die notwendigen Daten für ein übergeordnetes System.

Die Produktentwicklung in Bremen folgt den Prinzipien des Security-by-Design-Ansatzes (vgl. IEC 62443-4-x). Die Entwicklungsmannschaft besteht aus einem Team kompetenter IT-/OT-Sicherheitsexperten, die auf mehrere Jahrzehnte Berufserfahrung in den Marktsegmenten IT-Security und Automatisierung zurückblicken können. IRMA ist durch die Selbstverpflichtungserklärung bereits seit vielen Jahren Trägerin des TeleTrusT-Vertrauenszeichen „IT Security made in Germany“.