Das richtige OT-Monitoring für die Angriffserkennung in der kritischen Infrastruktur

Erkenntnis kommt von Erkennen

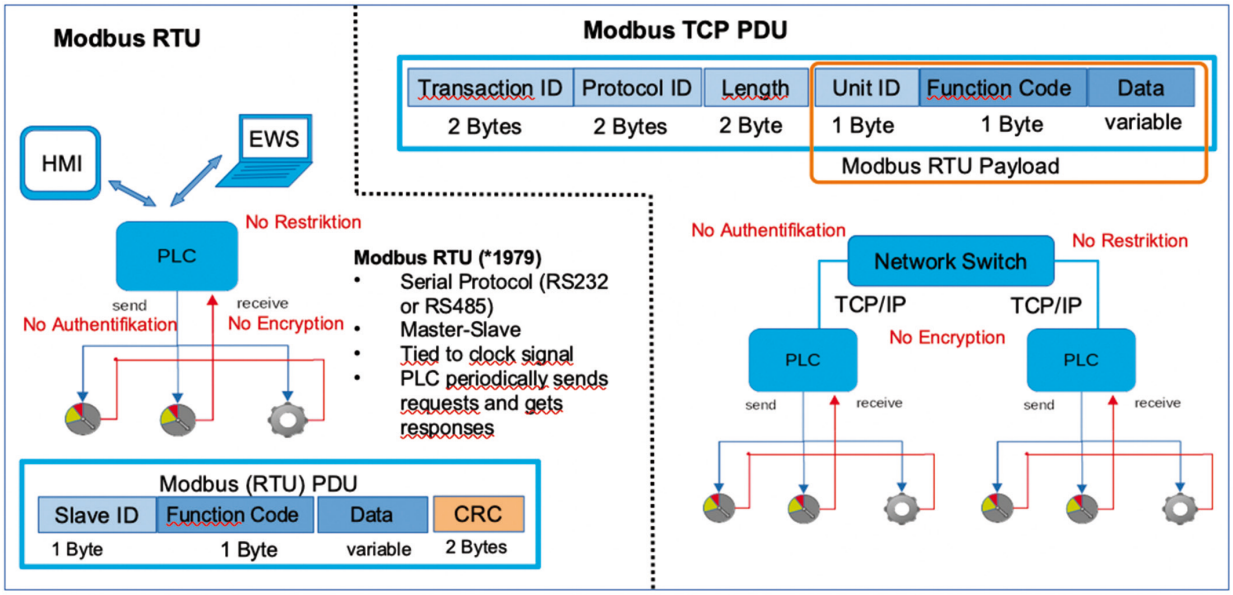
Das aktualisierte IT-Sicherheitsgesetz schreibt KRITIS-Betreibern vor, dass sie ab Mai 2023 Systeme zur Angriffserkennung nutzen müssen. Im Gesetzestext werden solche Systeme beschrieben als „technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme." [1] Aber was bedeutet eine Angriffserkennung für die Operational Technology (OT)?

Von Jens Bußjäger, Achtwerk GmbH & Co. KG und Dieter Barelmann, VIDEC Data Engineering GmbH

Für KRITIS-Betreiber sind die Anforderungen des IT-Sicherheitsgesetzes 2.0 (ITSiG) bald verpflichtend umzusetzen. Allerdings sind nahezu alle Unternehmen von gezielten Angriffen betroffen – und die wenigsten können solchen Attacken standhalten. Auffällig ist jedoch, dass immer mehr erfolgreiche Angriffe auf Betreiber kritischer Infrastrukturen gemeldet werden. Die Erkenntnis aus der steigenden Anzahl der Vorfälle und der nachfolgenden forensischen Aufarbeitung ist eindeutig: Oft gibt es vor dem eigentlichen Angriff erste Indizien von kritischen und verdächtigen Aktivitäten im Netzwerk. Durch eine Früherkennung ist es also möglich, Angriffe rechtzeitig zu erkennen und die Auswirkungen zu verhindern oder zumindest deutlich zu verringern. Das hat auch der Gesetzgeber erkannt und die Angriffserkennung nun gesetzlich festgeschrieben. Es gilt nun, die „Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten" zu lassen.

Erkenntnis – Erkennen – Detektion

Eine Angriffserkennung für die Produktionsanlagen bedarf aufgrund ihrer Strukturen, Geräte und Protokolle spezieller Lösungen. Herkömmliche Erkennungsmethoden sind für die Domaine der vernetzten Automatisierungs- und Produktionsanlagen oft nicht anwendbar und auch nicht ausreichend. Für den Produktionsbereich sind Angriffserkennungen sogar noch wichtiger, da



Modbus RTU-Transformation in Modbus TCP

die Laufzeiten der Geräte wesentlich länger sind und die in Betrieb befindlichen Anlagen in der Regel selten ein Update erhalten – getreu dem Motto „Never change a running system“. Entsprechend sind Geräte und Protokolle überwiegend von Haus aus veraltet und unsicher.

Beispiel Modbus: Insecurity by Design?

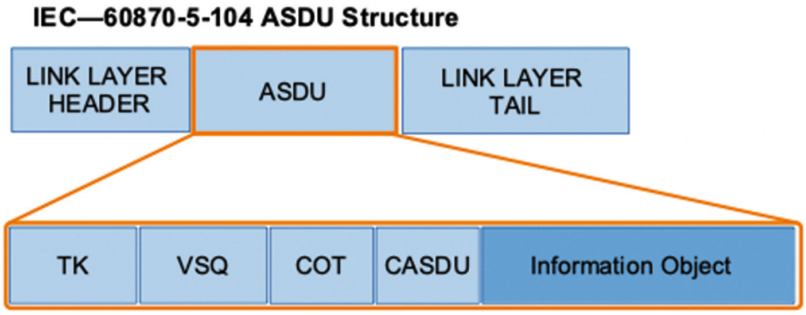
Die noch verbreitete Meinung, dass „die Steuerungsprotokolle innerhalb der Anlagen proprietär sind, es teurer Spezialisten bedarf und somit sicher sind“, ist überholt. Auch das Hacker „nicht das nötige Spezialwissen haben, um in unsere Produktion einzugreifen“ ist leider nicht richtig. Ist der Perimeter überwunden, das VPN der Fernwartung gekapert, ein USB-Stick, eine Firmware, eine Engineering Workstation infiziert, fehlt jeglicher Schutz. Selbst die Segmentierung von Netzwerken hilft nicht weiter, da bei einem solchem Befall die zulässigen Verbindungen und Funktionen der Industrieprotokolle direkt genutzt werden. Beispiele für Sicherheitslücken im weit verbreiteten Modbus TCP sind:

_____ Modbus TCP enthält keine Authentifizierung und Verschlüsselung.
_____ Legitime Funktionen sind nutzbar und leistungsfähig (z. B. Modicon - Code 90), um die Steuerung zu stören.
_____ Zur Steuerung können die Funktionen direkt genutzt werden,

Erkennung und Kontrolle im IEC 60870-5-104

Umspannwerke oder Kraftwerke verwenden zur Fernsteuerung der dezentralen Standorte von der zentralen Leitwarte die Protokolle der Norm IEC 60870-5-104. Hier hat die IEC zuerst das Fernsteuerungsprotokoll IEC 60870-5-101 für die begrenzte Bandbreite der seriellen Kommunikation über Funkverbindungen oder das Telefonnetz, in den meisten Fällen über private Netze, definiert. Die Norm definiert Typen von Nachrichten (ASDU) und eine Reihe von Anwendungsfunktionen zur Steuerung sowie Überwachung von Fernstationen.

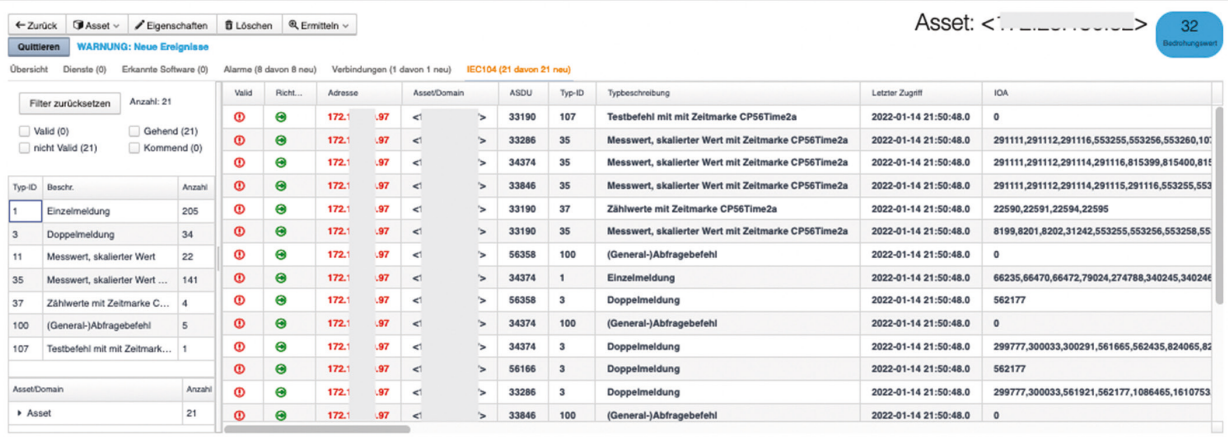
Durch die Verfügbarkeit des Internet per TCP/IP und der somit höheren Bandbreiten konnte die Reaktionszeit der Systeme verbessert werden. Verfügbare Leitungen mit



IEC 60870-5-105 ASDU-Struktur

Glasfaser, digitale Funkverbindungen oder die Funknetze mit 3G/4G ermöglichen des Weiteren mit mehreren Kommunikationskanälen zuzugreifen. Die IEC 60870-5-104 verwendet TCP/IP um die in IEC 60870-5-101 definierten Fernsteuerungsaufgaben zu erfüllen.

Die Authentifizierung und Integrität durch serielle Leitungen wurde nicht durch entsprechende Verfahren (TLS, X509 Zertifikate) abgelöst. Manipulationen sind deshalb einfach möglich. Eine unabhängige Erkennung von Anomalien durch ein OT-Netzwerk-Monitoring ist deshalb unumgänglich. Das Protokoll IEC 60870 5-104 muss im Detail inspiziert und überwacht werden, damit ein sicherer Betrieb gewährleistet ist.



Detaildarstellung der IEC-60870-5-104-Funktionsaufrufe einer OT-Monitoring-Lösung

um ein Gerät abzuschalten, Prozessdaten zu senden, Geräte direkt zu rekonfigurieren und weitere Maßnahmen auszuführen.

Angreifer können so von manipulierten Geräten Standardfunktionen des Modbus TCP nutzen. Es ist dadurch einfach, die SPS abzuschalten oder Geräte neu zu konfigurieren und falsche Prozessdaten an die Aktoren zu senden. Das gilt nicht nur für Modbus TCP, auch andere Industrieprotokolle, wie Profinet, EtherCat, Bacnet, nutzen Ethernet und sind nicht ausreichend sicher.

Erkenntnis – Erkennen – Reagieren

Angriffserkennung, auch OT-Monitoring genannt, für vernetzte Automatisierungsgeräte und Produktionsanlagen ist nicht das gleiche wie ein IT-Monitoring. In der OT müssen bestimmte Funktionen gewährleistet sein, zum Beispiel das Erfassen und Anzeigen der Industrieprotokolle, Packet Inspection, die Analyse zur Nutzungsart der Daten und Funktionsaufrufe in den einzelnen Produktionsanlagen. Hinzu kommt, dass der Hersteller der Angriffserkennung über genügend Erfahrung in den Branchen verfügen sollte und die unterschiedlichen Einsatzszenarien kennen muss. Hierzu ist umfangreiches Wissen auf dem Gebiet der Automatisierung notwendig.

Das ITSiG 2.0 fordert von den Betreibern auch die Integration von entsprechenden organisatorischen Prozessen. Das beginnt mit der Risikoanalyse und somit der Identifikation von Maßnahmen im Falle der Erkennung von Angriffen. Diese Maßnahmen definieren sich nach dem BSI-Grundschutz, EnWG Sicherheitskatalog oder den vom BSI anerkannten branchenspezifischen Sicherheitsstandards.

Ein weiterer Aspekt bei der Auswahl einer OT-Monitoring-Lösung ist die Möglichkeit der qualifizierten Alarmierung. Dabei geht es um die Erkennung von Verhaltensmustern der Angriffsszenarien sowie um eine zielgerichtete und sichere Alarmweiterleitung. Größere Unternehmen nutzen in der Regel übergeordnete Managementsysteme wie eine Security-Information-and-Event-Management-(SIEM)-Lösung [2] oder ein Information-Security-Management-System (ISMS). Hier gilt es bei der Auswahl des OT-Monitoring-Systems auf die Möglichkeit zur Integration und des sicheren Datenaustausches zu achten. Für kleinere Organisationen, wie zum Beispiel Stadtwerke oder Wasser-/ Abwasserverbände, sollten diese Alarme in den Leitständen und Alarmierungssystemen sicher integrierbar und für das Betriebspersonal schnell verfügbar sein.

Zudem sind für die Umsetzung einer Angriffserkennung kompetente Partner mit einer langjährigen Historie in der Automatisierung wichtig. In der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen, ist für die Vielzahl der IT-Systemhäuser im Bereich der OT-Security eine große Herausforderung. Mit Kooperationen sollte diese Anforderung erfüllbar sein. Erfahrung lässt sich nicht anlesen und die Besonderheiten der Automatisierung müssen zwingend in ein Projekt eingebracht werden.

Fazit

Insgesamt bleibt für den OT-Bereich festzuhalten:

_____ Eine Angriffserkennung in vernetzten Automatisierungen benötig die tiefe Kenntnis der speziellen Protokolle.
_____ Im ITSiG 2.0 wird nach dem „Stand der Technik“ Angriffserkennung verpflichtend gefordert.
_____ Angriffserkennungen für die Büro oder IT-Infrastruktur lassen sich nicht 1:1 einsetzen.
_____ Die speziellen Anforderungen einer Angriffserkennung für vernetzte Automatisierungslösungen und Produktionsanlagen müssen abgedeckt werden. ■

Jens Bußjäger ist Geschäftsführer der Achtwerk GmbH & Co. KG (www.irma-security.de).
Dipl. Ing. Dieter Barelmann ist Geschäftsführer der VIDEC Data Engineering GmbH (https://videc.de).

Literatur
[1] Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, 18. Mai 2021, www.bgbl.de/xaver/bgbl/start.xav?startbk=-Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf
[2] SECurity Assessment für „Industrie 4.0“-Infrastrukturen durch Virtualisierung und Simulation (SECi40), www.sec-i40-project.de/de_start.html