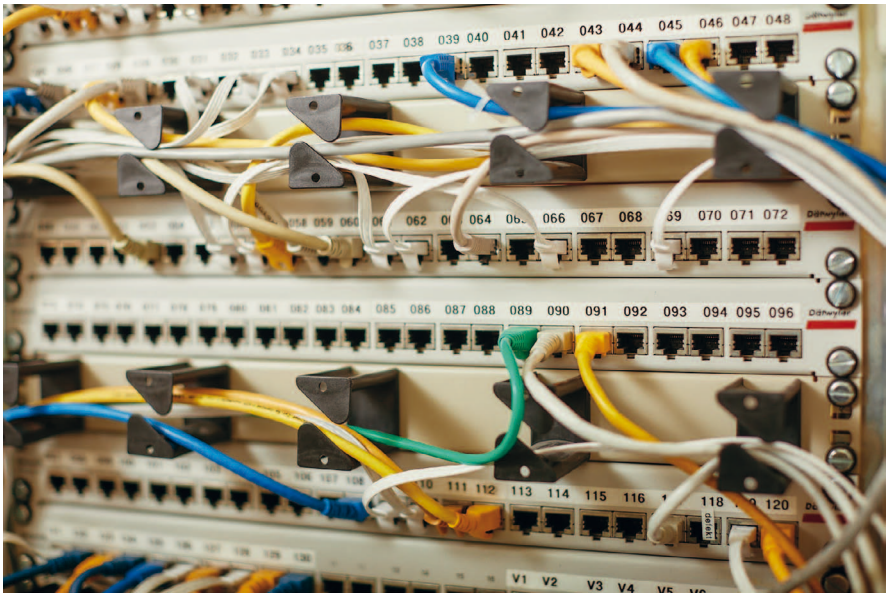
Anomalieerkennung in Produktionsnetzen

Smarter Schutz für smarte Fabriken



© genua GmbH

Eine Herausforderung an die IT Security in der Industrie 4.0 ist, das klassische IT-Sicherheitskonzepte für OT-Netze meistens nicht anwendbar sind. Fünf Ansatzpunkte für den Schutz von OT-Netzen sowie ein Best Practice für Anomalieerkennung in vier Phasen beschreibt dieser Beitrag. Mit diesem Vorgehen lassen sich gewachsene OT-Netze zuverlässig absichern.

Mit der Industrie 4.0 werden Produktionsnetze und Services „smart“: Maschinen und Anlagen, industrielle Steuerungssysteme (Industrial Control Systems, ICS) sowie Automationslösungen sind online vernetzt, was zu flexiblen und effizienteren Produktionsnetzen führt. Zugleich wird die bisherige physische Trennung der OT von IT-Systemen und Office-Netzen für den Datentransfer oder für Fernwartungszugriffe aufgehoben. Das bringt eine höhere Anfälligkeit für Angriffe von Cyberkriminellen auf OT-Netze, Logistikprozesse oder Gebäudeleittechnik mit sich. Eine wesentliche Herausforderung an die IT Security in der Industrie 4.0 besteht darin, das klassische IT-Sicherheitskonzepte für OT-Netze meistens nicht anwendbar sind. Viele Systeme laufen auf veralteten Betriebssystemen, Sicherheitsupdates oder nachträgliche Härtungsmaßnahmen sind häufig nicht umsetzbar. Höchste Verfügbarkeits- und Integritätsanforderungen lassen Eingriffe in laufende Systeme oftmals nicht zu. Risiken entstehen aber nicht nur durch die Onlineverbindungen. Über infizierte USB-Sticks, mobile Endgeräte wie dem Laptop des Servicetechnikers oder aufgrund einer fehlenden Segmentierung des OT-Netzes können auch offline betriebene Anlagen durch Schadprogramme infiziert werden.

Fünf Ansatzpunkte für den Schutz von OT-Netzen

Die Absicherung der Vertraulichkeit, Integrität und Verfüg-

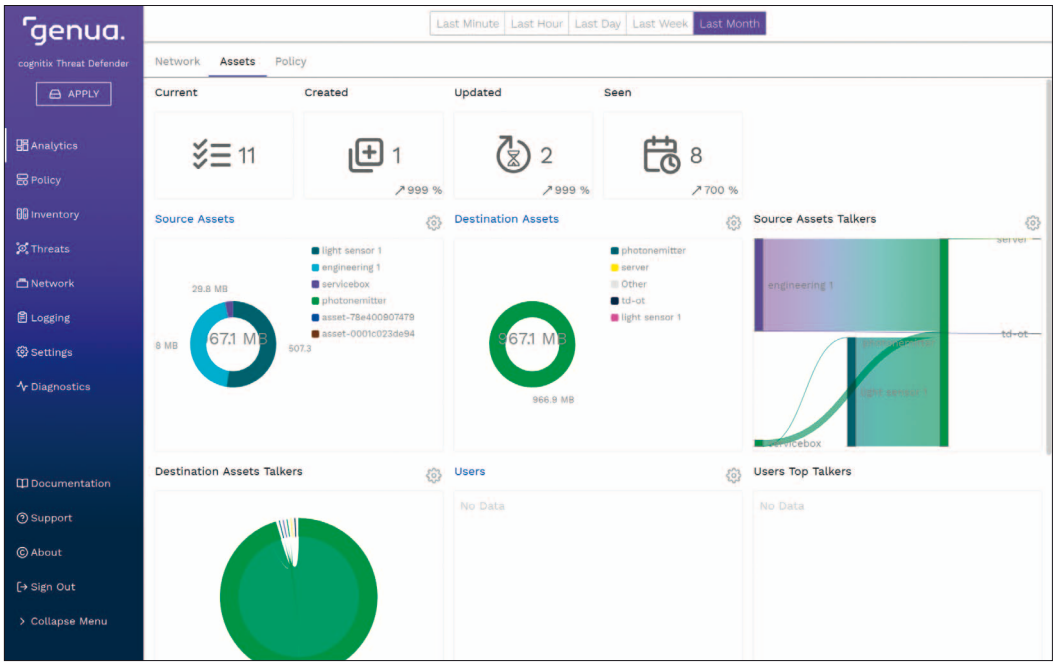


Bild 1: Wer spricht im OT-Netzwerk mit wem? Der cognetix Threat Defender zeigt aufsummiert, welche Assets in den letzten 30 Tagen wie viel Datenverkehr initiiert (Source Assets) bzw. beantwortet (Destination Assets) haben sowie den Datenverkehr zwischen den Assets.

Autor:
Arnold Krille, Abteilungsleiter Product Development cognitx Threat Defender
genua GmbH
www.genua.de

barkeit von OT-Netzen ergibt sich aus dem Zusammenspiel von Regeln, Verfahren, Maßnahmen und Tools. Definiert sind diese u. a. im Informations-Sicherheits-Management-System (ISMS gemäß ISO/IEC 27000) und der Norm für „Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme“ (IEC 62443). Insbesondere fünf Ansatzpunkte sollten Unternehmen kennen:

1. Defense-in-Depth-Prinzip (IEC 62443)

In der Norm IEC 62443 ist ein Defense-in-Depth- Prinzip („gestaffelte Verteidigung“) verankert. Es definiert den Schutz gegen Cyberangriffe (wie bei einer Zwiebel) in mehreren Schichten. Auch wenn eine Sicherheitsschicht überwunden wurde, ist nur ein Teil des Netzes betroffen. Das Gesamtsystem ist noch durch weitere Sicherheitsebenen geschützt. So ist es sinnvoll, die Netzbereiche in unterschiedliche Sicherheitszonen aufzuteilen und gestaffelte Schutzlevel zu vergeben.

2. Sicherheitszonen, Zonenübergänge und Schutzlevel

Eine notwendige Maßnahme ist daher, unterschiedliche Sicherheitszonen festzulegen und voneinander abzuschotten. Die Zonenübergänge und die Kommunikation zwischen den Zonen können durch Firewalls und entsprechende Filterregeln restriktiv geregelt werden. So lassen sich auch abgesicherte Schleusen-PCs einrichten, um beispielsweise USB-Sticks verwenden zu können. Für Zonen mit besonders hohem Schutzlevel ist der Einsatz von Datendioden empfehlenswert, die ausschließlich einen Einbahn-Datentransfer zulassen und den Informationsfluss in der Gegenrichtung abblocken.

3. Absicherung der Fernwartung

Sichere Fernwartungs-Lösungen erlauben den Zugang nur zu einer Sicherheitszone. Dies kann mit einem sogenannten Rendezvous-Server umgesetzt werden, der in der demilitarisierten Zone (DMZ) neben der Firewall installiert wird. Durch diese neutrale Zwischenebene wird eine direkte Verbindung mit dem Internet ausgeschlossen. Hierhin bauen sowohl der Wartungs-Service als auch der Maschinenbetreiber zum vereinbarten Zeitpunkt verschlüsselte Verbindungen auf. Erst mit deren Rendezvous auf dem Server in der DMZ entsteht die durchgängige Wartungsverbindung zur betreuten Maschine.

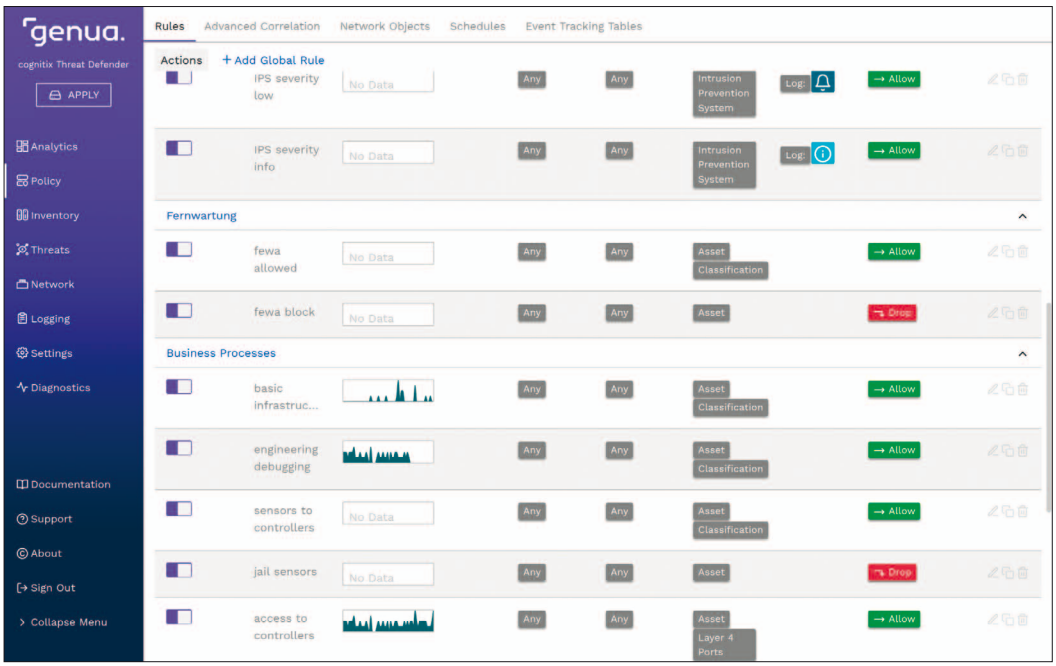


Bild 2: Wer darf mit wem sprechen? Das Bild zeigt den Ausschnitt eines Regelwerks. Zusammengefasst in abgeschlossene Policies (Richtlinien) sorgen aufeinander aufbauende Rules (Regeln) für Ordnung im Netzwerk.

4. Monitoring der Netzkommunikation (IDS/IPS)

Das Monitoring von OT-Netzen ist hier eine zusätzliche Schutzmaßnahme, um die Anlagenkommunikation zu überwachen und auf Auffälligkeiten zu untersuchen. Dafür haben sich Intrusion-Detection-Systeme (IDS) und Intrusion-Prevention-Systeme (IPS) etabliert, die bereits seit vielen Jahren in Office-Netzen eingesetzt werden. IDS-Systeme analysieren den Datenstrom im OT-Netz und alarmieren den Administrator bei einem verdächtigen Verhalten.

5. Neue Anforderungen an die Sicherheitstechnik

Die Cyber-Sicherheits-Empfehlung des BSI (BSI- CS 134) hebt die Anomalieerkennung als ein Mittel zum Schutz von Netzwerken besonders hervor: „Sie ermöglicht die Erkennung untypischen Verhaltens und somit neben technischen Fehlerzuständen und Fehlkonfigurationen auch die Detektion bisher unbekannter Angriffsformen auf solche Netze. Dies unterscheidet die Anomalieerkennung von anderen Maßnahmen, die auf der Erkennung bereits bekannter Angriffe beruhen.“ Die Forderung nach einer Anomalieerkennung findet sich auch im Entwurf „IT-Sicherheitsgesetz 2.0“ (IT-SiG 2.0). Die Betreiber kritischer Infrastrukturen werden demnach erstmals zum Einsatz von Systemen zur „Angriffserkennung“ verpflichtet.

Anomalieerkennung in vier Phasen

Bei der Absicherung von gewachsenen OT-Netzen ist ein schrittweises Vorgehen empfehlenswert. Die technologische Grundlage ist in diesem Fall der cognitix Threat Defender (cTD), eine IT-Security-Lösung, welche die Sicherheitslücke von IDS- und IPS-Systemen schließt. Sie überwacht den gesamten Netzwerkverkehr und analysiert auch das Verhalten der Netzkomponenten (Assets). Der cTD richtet ein überwachtes sicheres Netzwerk ein, in dem er Verhaltensmuster der Netzwerkgeräte erkennt und definierten Regeln zuordnet. Dabei werden bisher getrennte Funktionen wie Netzwerkanalyse, Intrusion Detection, Asset Tracking und eine dynamische Policy Engine in einem System zusammengeführt. Bei der Anomalieerkennung haben sich in der Praxis vier Phasen bewährt:

Phase 1 – Assets katalogisieren

In der ersten Phase werden die Kommunikationspartner innerhalb des OT-Netzwerks ermittelt. Der Netzwerkverkehr wird zum cognitix Threat Defender gespiegelt und alle aktiven Geräte im beobachteten Netzwerkbereich in einer Asset-Datenbank erfasst. Dabei werden für die Geräte Metadaten, wie zum Beispiel das verwendete Betriebssystem, identifiziert. Die Erfassung erfolgt rein passiv anhand des beobachteten Netzwerkverkehrs.

In dieser Phase werden bereits nach wenigen Stunden Fehlkonfigurationen, Netzwerkprobleme, veraltete Gerätesoftware oder nicht erlaubte Geräte erkannt. So fällt zum Beispiel eine fehlerhafte Konfiguration einer Active-Directory-Synchronisation auf. Diese kann einen konstanten Hintergrund-Traffic erzeugen, der zu keiner merklichen Einschränkung führt. Dennoch kann dieser Anzeichen eines Fehlers sein, weil die richtige Konfiguration eines AD nur bei Änderungen der Daten eine Synchronisation dieser Änderungen erfordert und damit wesentlich weniger Netzwerkverkehr erzeugt.

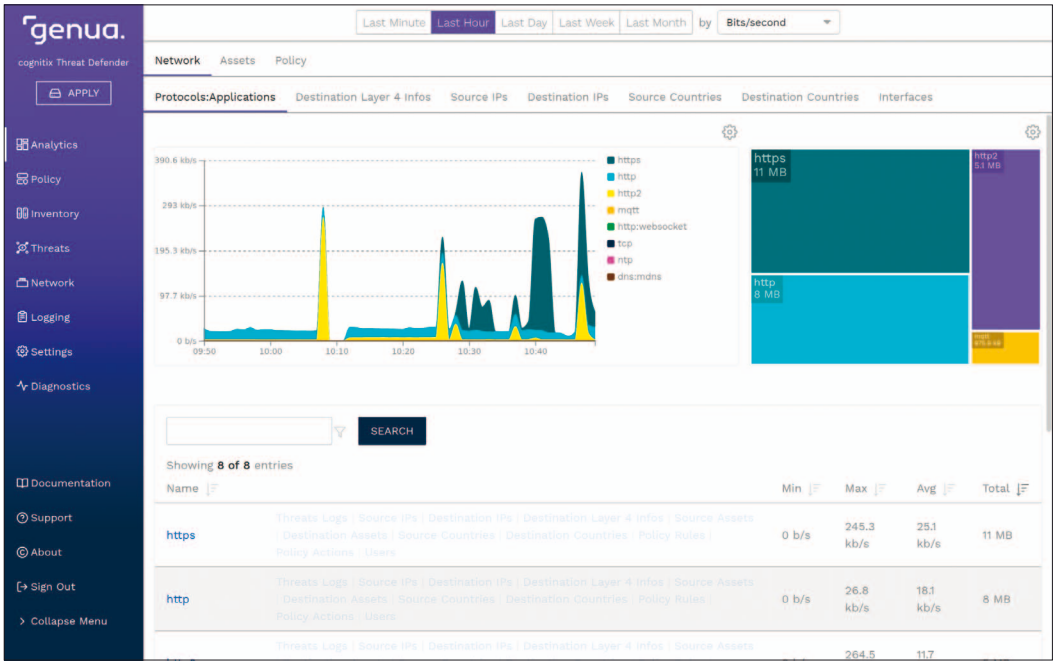


Bild 3: Verlauf und Summen der Nutzung der verschiedenen Layer-7 Protokolle für die letzte Stunde.

Phase 2 – Assets identifizieren

Im nächsten Schritt steht der Aufbau des Netzwerks im Fokus, um dort bisher unbekannte Geräte aufzuspüren und ggf. zu deaktivieren. Dazu wird die Asset-Datenbank manuell konsolidiert. Der Administrator des OT-Netzes ordnet die automatisch erfassten Assets einzelnen Geräten bzw. Geräteklassen zu. Dabei vergibt er aussagekräftige Namen und organisiert die Assets mittels Tags in domänenspezifischen Gruppen. Dieser manuelle Aufwand ermöglicht die Vereinfachung der Kommunikationsstrukturen und erleichtert die weitere Arbeit zur Analyse und Überwachung des Netzwerks.

Phase 3 – Kommunikationspfade abbilden

Anschließend wird die Kommunikation der Geräte untereinander analysiert, um die zulässige Kommunikation in der Netzwerk-Policy zu modellieren. Unerwünschte Kommunikationspfade, nicht benötigte Dienste oder unerwünschte Protokolle, wie Multicast, werden deaktiviert. Für diese zulässige Kommunikation werden nach und nach in einem iterativen Prozess Regeln angelegt, bis eine feingranulare Netzwerk-Policy entsteht.

Phase 4 – Stabilisierung

Die erstellte Policy wird validiert und das Netzwerk passiv überwacht. Dazu läuft das erstellte Modell über mehrere Wochen passiv im OT-Netz. Der Administrator wird per E-Mail, Slack oder Syslog benachrichtigt, wenn die Logging-Regel greift und somit neue, noch nicht abgebildete Kommunikation erfasst wird. Gegebenenfalls muss die Policy dann nachjustiert werden. Wahrscheinlicher ist es jedoch, dass der neuartige Netzwerkverkehr eine Anomalie darstellt, die auf ein Problem oder gar eine Störung bzw. einen Eindringling hinweist.

Aktives Blocking als Ausbaustufe

Diese vier Phasen erfolgen lediglich anhand eines gespiegelten Netzwerkverkehrs, so dass für das OT-Netz keinerlei Risiko durch Latenzen oder Datenverlust besteht. Erst in einer optionalen fünften Phase wird aktiv in den Netzwerkverkehr eingegriffen, um unerwünschte Kommunikation zu unterbinden. Für ein solches aktives Blocking sollten die in den Phasen 3 und 4 angelegten Regeln für die explizit erlaubte Kommunikation um Regeln ergänzt werden, die explizit verbotene und bei Bedarf auch jede unbekannte Kommunikation blockieren. Hierbei steigt mit der Sicherheit auch das Risiko für Unterbrechungen im OT-Netz, da nun keine unerwarteten Ereignisse mehr zulässig sind und von Threat Defender blockiert werden. ◀