Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IN DER PRODUKTION

Monitoring und Anomalieerkennung in Produktionsnetzwerken

Ist das normal?

Moderne Produktionsnetzwerke besitzen heute eine mit den klassischen IT-Netzen vergleichbare Topologie und verwenden zunehmend Protokolle, die auch auf TCP[1]/IP[2] aufsetzen. Diese Protokolle werden nicht nur von intelligenten Steuergeräten gesprochen, auch Sensoren und Aktoren kommunizieren zunehmend darüber; die Vielzahl dieser Komponenten und der Verbindungen untereinander bewirkt eine anwachsende Komplexität solcher Netze. Die Anbindung industrieller Netzelemente und Netzsegmente erfolgt über Switche, zur Absicherung der Segmentgrenzen und Netzübergänge werden Firewalls und andere Überwachungslösungen eingesetzt. Überwachung ist in diesem Kontext das Protokollieren und Analysieren der im Netz auftretenden Daten und Datenströme und dient im Wesentlichen der Erkennung von Auffälligkeiten, die Einfluss auf technische und wirtschaftliche Belange nehmen können. Exemplarisch sind dies Funktionalität, Qualität, Verfügbarkeit, aber auch Sicherheit sowohl im Hinblick auf Safety[3] als auch auf Security[4]. Heutige industrielle Netzwerke ähneln in ihrer Struktur den Office-IT-Netzen und sind häufig mit ihnen verbunden. Die damit einhergehenden Bedrohungen – vergleichbar mit denen der klassischen IT – erfordern den Fokus auf die Security. Die Verwendung von Komponenten der klassischen Office-IT im Produktionsnetz ist vorteilhaft in Bezug auf Kosten, Betrieb und Benutzerfreundlichkeit, jedoch erweitern diese Komponenten auch die potenzielle Angriffsfläche [vgl. [1]]. Monitoring und Anomalieerkennung werden daher zur Notwendigkeit in Bezug auf Prävention, Detektion und Reaktion.

Diese Cyber-Sicherheits-Empfehlung erläutert die Grundprinzipien des Monitorings und der Anomalieerkennung und gibt darüber hinaus eine Hilfestellung bei der Produktauswahl.

1 Monitoring

Monitoring ist ein Überbegriff für alle Arten der unmittelbaren systematischen Erfassung, Beobachtung oder Überwachung eines Vorgangs oder Prozesses mittels technischer Hilfsmittel oder anderer Beobachtungssysteme (vgl. [2]).

1 TCP: Transmission Control Protocol – Übertragungssteuerungsprotokoll der Internetprotokollfamilie
2 IP: Internetprotokoll
3 Safety: physische Sicherheit, Betriebssicherheit
4 Security: Schutz von Daten und Informationen, Schutz vor Angriffen

Monitoring wird in nahezu allen Bereichen von Wirtschaft, Industrie, Umwelt und vielen weiteren praktiziert und eingesetzt und ist auf Prozesse und Abläufe jeder Art anwendbar. Es ist die Erweiterung und Vertiefung des Protokollierens.

Monitoring in der Informationstechnik ist das kontinuierliche Überwachen von Prozessen, Geräten, Kommunikationsbeziehungen und Diensten innerhalb eines Netzwerkes. Dazu gehören neben den im Netz übertragenen Daten auch von Netzwerkkomponenten erzeugte Logdaten [3], beispielsweise von Switchen oder Firewalls. Die Umsetzung geschieht mit Monitoring-Hardware und -Software.

Monitoring im industriellen Umfeld und im Kontext dieser Cyber-Sicherheits-Empfehlung ist nicht auf die bloße Zustandsüberwachung (Condition Monitoring, Process Monitoring, Alarmüberwachung) beschränkt. Es beinhaltet zudem die Beobachtung der Kommunikation zwischen Automatisierungskomponenten, zu Aktoren, Sensoren sowie von und zu Fernwirkkomponenten. Dazu gehört auch das Auslösen von Meldungen und Alarmen bei Erkennen besonderer Ereignisse. Des Weiteren sind auch Leit- und Steuerungssysteme wie MES[5], ERP[6] und Historians mit einzubeziehen.

2 Wie funktioniert Monitoring

Monitoring ist in der Regel ein eigenständiger Prozess, der alle Geräte in einem Netzwerk gleichermaßen – also unabhängig von Hersteller, Typ und Funktion – überwachen sollte. Daten und Informationen werden an einem oder mehreren zentralen Punkten gesammelt oder von einem zentralen Punkt abgefragt, mit technischen Verfahren analysiert und in Form von Zustandsberichten dargestellt. Monitoring-Lösungen erlauben darüber hinaus die Festlegung von Schwellwerten, die möglichen Zustandsberichte des Monitorings reichen daher von einfachen Signalisierungen (z.B. Rot/Grün-Leuchte bei Erreichen eines Schwellwertes) bis hin zu komplexen Diagrammen, Statistiken und Risikoeinschätzungen. Netze werden damit transparent.

Zum effizienten Einsatz ist es neben der Auswahl der geeigneten Lösung erforderlich, die zu überwachenden Prozesse und Abläufe zu analysieren und die entsprechenden Kriterien für das Monitoring festzulegen.

3 Anomalien

Anomalien sind unerwartete Abweichungen von Regeln(vgl. [4]), im Kontext der Produktion also Abweichungen von "normalen Betriebszuständen". Diese treten meist in einem Fehlerfall auf. Sie können allerdings auch ein Hinweis auf einen Angriff bzw. eine Manipulation innerhalb eines Produktionsnetzwerkes sein. Das gilt insbesondere dann, wenn Ereignisse erstmalig auftreten, Prozesse sich anders verhalten oder Geräte miteinander kommunizieren, die es bisher nicht getan haben. Somit lassen sich über die Auswertung von Anomalien auch bisher unbekannte Angriffsmuster detektieren. Die Anomalieerkennung ist daher ein geeignetes Verfahren, Betriebszustände zu erfassen, Warnungen zu erzeugen und im Bedarfsfall eine effektivere Forensik zu ermöglichen. Die Anomalieerkennung gehört zu den grundsätzlichen Methoden der Angriffserkennung (Intrusion Detection) (vgl. [5]). Sie ist allerdings kein statisches System, das auf Basis fester bzw. bekannter Gefährdungsmuster (z.B. ein indizierter Computervirus) agiert. Vielmehr bewertet die Anomalieerkennung kontinuierlich die Standardkommunikation des jeweiligen Netzwerkes neu und erlaubt so eine dynamische Anpassung an Veränderungen der Gefährdungsvektoren und damit die Detektion bislang unbekannter Verhaltensmuster im Netzwerk, die noch in keiner Viren- oder Fehlerzustandsliste verzeichnet sind.

5 MES: Manufacturing Execution System – Produktionsleitsystem
6 ERP: Enterprise Resource Planning – Systeme zur Ressourcenplanung und Abbildung von Geschäftsprozessen

4 Was sind Anomalien?

Anomalien in Produktionsnetzwerken sind eine dynamische Kategorie an potenzielle Störungsfaktoren. Diese sind unter anderem:

- Außergewöhnliche bzw. ungewöhnliche Aktivitäten im (ICS[7])-Netzwerk
  - Anschluss eines neuen Gerätes
  - DHCP[8]-Requests
  - Datenpakete eines bisher unbekannten Gerätes
  - Datenverkehr zwischen Geräten, die bisher nicht untereinander kommuniziert haben
  - Datenverkehr mit einem bisher nicht verwendeten Protokoll
  - Datenverkehr mit einem unüblichen oder nicht vorgesehenen Protokoll
  - Auftreten von Ereignissen zu ungewöhnlichen Zeiten
  - Verwendung unerwarteter Adressen (öffentliche IP-Adressen etc.)
  - allgemein auffällige Ereignisse wie Adress-Scans oder Port-Scans
  - Änderungen der Netzwerkqualität wie hohe Bandbreitennutzung, Erhöhung der Round-Trip-Zeiten, Verringerung der TCP-Fenstergröße, etc.
- Außergewöhnliche Ereignisse in produktionstypischen (ICS-)Protokollen
  - ungewöhnliche Fehlermeldungen
  - nicht unterstützte Funktionsaufrufe
  - bisher nicht verwendete Funktionsaufrufe
  - fehlerhafte Datenpakete
  - unbekannte Funktionscodes
  - Protokoll folgt nicht der Norm
  - unerwarteter Wechsel von einem Protokoll zu einem anderen
- Außergewöhnliche Veränderungen in Prozessdaten (z.B. Sensordaten, Steuerdaten)
  - Werte außerhalb definierter Bereiche
  - veränderte Häufigkeit
  - veränderte Zykluszeiten
  - sich verändernde Varianz innerhalb bestimmter Zeiträume

5 Wie funktioniert Anomalieerkennung?

Um Anomalien zu erkennen, muss zuvor der "Normalzustand" eines Systems – hier eines Produktionsnetzes – bekannt sein. Dazu werden – idealerweise passive – Sensoren (Netzwerk- oder Wiretaps) im Netzwerk bzw. im Netzwerksegment platziert, mittels derer über einen längeren Zeitraum die Daten im Netz erfasst werden können (Trainingsphase). Alternativ kann auch ein Switch mit Spiegelport (Mirroring) eingesetzt werden. Daten in diesem Sinne sind alle informationstechnischen Signale im Netzwerk, also Nutzdaten, Protokolldaten, Paketdaten usw.

7 ICS: Industrial Control System – industrielle Steuer- und Regelungssysteme
8 DHCP: Dynamic Host Configuration Protocol – automatische Zuordnung von Namen zu Netzwerkadressen

Das System sammelt alle auftretenden Informationen und lernt dadurch die Netzwerktopologie, die Kommunikationsbeziehungen, das Zeitverhalten und gegebenenfalls die Inhalte der Kommunikation. Diese gewonnenen Daten lassen sich nach verschiedensten Kriterien analysieren, kategorisieren und bewerten. Mit dieser Datenbasis als Grundlage werden nun Schwellwerte und Triggerpunkte definiert, um außergewöhnliche Zustände und Vorgänge, die vom bisher gelernten "Normalen" abweichen, zu erkennen. Da jedes erstmalig auftretende Ereignis als Anomalie angesehen wird, ist es hilfreich, im Vorfeld und während der Trainingsphase mögliche Problembereiche festzulegen, auf die besonders geachtet werden soll, um die Zahl der Falschalarme (false positives) zu reduzieren. Im laufenden Betrieb wird diese Grundeinstellung kontinuierlich an die jeweils aktuellen Begebenheiten angepasst, beispielsweise wenn im Rahmen von Erweiterungen Geräte hinzukommen oder sich das Zeitverhalten einer Kommunikationsbeziehung gewollt ändert. Dies bedingt eine kontinuierliche Beobachtung und Bewertung, zumal ein potenzieller Angreifer darauf bedacht sein wird, seine eigenen Aktivitäten als normales Betriebsverhalten zu tarnen.

Zweckmäßigerweise wird ein Erkennungssystem als eigenständige und unabhängige Komponente in das zu überwachende Netzwerk integriert und verfügt zudem über Schnittstellen zu Signalisierungs-, Melde- und Alarmsystemen und weiteren aktiven Sicherheitskomponenten.

6 Anforderungen an Systeme zur Anomalieerkennung

Entsprechend den Anomaliebeispielen in Abschnitt 4 können mehrere Anforderungskategorien festgelegt werden, die ein System zur Anomalieerkennung möglichst erfüllen sollte.

6.1 Kategorie: Allgemeine Anforderungen

- Übersicht über alle Geräte, die im Netzwerk kommunizieren
- Identifikation aller im Netzwerk vorkommenden Protokolle
- Identifikation der im Netzwerk bestehenden Kommunikationsbeziehungen
- Erfassung der Netzwerkbelastung über die Zeit (Datenaufkommen, Kommunikationszeiten, etc.)
- Einrichtung und Anpassbarkeit von Erkennungskriterien
- Festlegung mehrerer Eskalationsstufen
- übersichtliche und anpassbare Visualisierung
- benutzerfreundliche Signalisierung und Darstellung von Ereignissen
- Darstellung der Korrelation von Ereignissen
- Integration in bereits bestehende Signalisierungs-, Melde- und Alarmsysteme
- Skalierbarkeit, z.B. erweiterbare Speicherkapazitäten
- Statistiken
- Filterfunktionen
- Exportfunktionen für weiterführende, ggf. forensische Analysen (z.B. anomaliespezifische Netzwerkmitschnitte)
- Benutzer- und Rollenmodell für den Zugriff auf das System
- Updatefähigkeit
- eigene Protokollierungsfunktionalitäten

6.2 Kategorie: Außergewöhnliche bzw. ungewöhnliche Aktivitäten im (ICS)-Netzwerk

Basisanforderungen:

- Identifikation neuer Geräte im ICS-Netz
- Identifikation der Kommunikation zwischen zwei Geräten, zwischen denen bisher keine Kommunikation stattgefunden hat
- Identifikation der Kommunikation zwischen zwei Geräten über einen TCP/UDP[9]-Port, der bisher nicht verwendet worden ist
- Identifikation neuer Protokolle oder der Veränderung von Protokollen zwischen einzelnen Komponenten
- Identifikation von Verbindungen in unsichere Netzwerke, z.B. Internet
- Identifikation unsicherer Kommunikationseigenschaften, z.B. fehlende Verschlüsselung

Weitere Anforderungen:

- Identifikation von Schwankungen in der Datenmenge und Häufigkeit
- Darstellung ungewöhnlicher Aktivitäten
- detaillierte Darstellung/Präsentation, ggf. mit Drill-Down-Möglichkeiten[10]
- Relevanz- und Risikobewertung erkannter Anomalien

6.3 Kategorie: Außergewöhnliche Ereignisse in produktionstypischen (ICS-)Protokollen

Basisanforderungen:

- Identifikation von Fehlermeldungen, wie zum Beispiel
  - ungültige oder nicht unterstützte Funktionsaufrufe bzw. Funktionscodes
  - ungültige Adresse, ungültiges Ziel
- Adresse oder Ziel nicht erreichbar / nicht verfügbar (z.B. Timeouts)
- Identifikation ICS-spezifischer Funktionscodes, die bisher nicht verwendet wurden
- Identifikation von Formatfehlern in ICS-Protokollen
- Feststellen, ob ein Zugriff (z.B. Schreiben/Lesen) auf eine Adresse erfolgt, die von diesem Gerät üblicherweise nicht genutzt wird

6.4 Kategorie: Außergewöhnliche Veränderungen in Prozessdaten (z.B. Sensordaten, Steuerdaten)

Basisanforderungen:

- Abweichungen innerhalb festgelegter Wertebereiche
- Veränderungen in der Häufigkeit
- Veränderungen im Zeitverhalten
- Tendenzveränderungen innerhalb von Wertebereichen

9 UDP: User Datagram Protocol – Übertragungsprotokoll der Internetprotokollfamilie
10 Drill-Down-Möglichkeiten: Schrittweise Verfeinerung für eine unterschiedliche Detailtiefe

7 Aktiv oder Passiv?

Ein Unterschied zwischen Aktiv und Passiv besteht darin, ob Anwendungen zum Monitoring und zur Anomalieerkennung die erforderlichen Daten rückwirkungsfrei erfassen (Passiv) oder selbst Daten im zu überwachenden Netz erzeugen (Aktiv), beispielsweise durch eigene Anfragen im Netzwerk, durch Mechanismen zur Erkennung neuer Teilnehmer im Netz oder der aktiven Abfrage von Systemzuständen, Firmware-Versionen und Logdaten. Die Begriffe Aktiv und Passiv beziehen sich im Besonderen auf die im Netzwerk eingesetzten Sensoren für die Datenerfassung und die Anbindung der Systeme.

7.1 Aktive Systeme

Aktive Systeme erzeugen Datenverkehr in dem zu überwachenden Netz. Dieser Datenverkehr beinhaltet beispielsweise:

- Abfrage von Logdaten
- Abfrage von Gerätetypen, Firmwareständen, Zuständen und Messdaten
- Prüfen eines Netzwerksegments auf vorhandene Teilnehmer durch Pings oder ARP-Anfragen

Aktive Systeme erfordern in der Regel nur wenige oder keine Eingriffe in das Netzwerk, sie werden über vorhandene Zugänge eingebunden. Spiegelports von vorhandenen Switchen können ebenfalls zur Erfassung dienen. Das System ist dann so zu konfigurieren, dass selbsterzeugte Daten von den zu überwachenden Daten unterschieden werden können. Gegebenenfalls sind auch Einflüsse auf das Zeitverhalten im Netzsegment zu berücksichtigen. Ein Angreifer, der in der Lage ist, Daten im Netzwerk zu manipulieren, kann natürlich somit auch das Monitoringsystem beeinflussen. Produktionsnetzwerke sind häufig zeitkritisch – Daten müssen in einem vorgegebenen zeitlichen Raster übertragen werden. Zusätzliche Datenpakete können zu Abweichungen führen und Störungen im Ablauf verursachen. In typischen heterogenen Produktionsnetzen mit teilweise sehr lang bestehenden Firmware- und Hardwareständen ist ein aktives Abfragen selbst eine Gefahrenquelle für die Stabilität, dies ist ebenfalls zu berücksichtigen. Zudem sollten aktive Systeme die Protokolle anderer aktiver Geräte im Netzwerk unterstützen und dürfen nicht die Gewährleistung von Anlagen negativ beeinflussen.

7.2 Passive Systeme

Passive Systeme verwenden Netzwerk- oder Wiretaps und arbeiten rückwirkungsfrei, d.h. sie haben keinen Einfluss auf Daten und Zeitverhalten im Netz und über sie werden keine Daten in das Netz gesendet. Zur Installation von Netzwerk- oder Wiretaps ist unter Umständen die Auftrennung des Netzwerks oder eines Netzwerkpfades erforderlich. Dies sollte daher nur zu einem geeigneten Zeitpunkt, beispielsweise vor der Inbetriebnahme oder innerhalb eines Wartungsfensters, erfolgen. Eine Abfrage von Geräten ist mit passiven Netzwerksensoren nicht möglich.

8 Fazit

Die Begrifflichkeiten Monitoring und Anomalieerkennung werden meist synonym verwendet. Genauer betrachtet bauen beide jedoch aufeinander auf. Durch ein Monitoring wird die Grundlage geschaffen, Anomalien in den Beobachtungen feststellen zu können. Insofern sind die Grenzen beider Verfahren zueinander fließend und sie verwenden überwiegend gleiche Methoden und Mechanismen.

Monitoring macht zunächst einmal die Teilnehmer und Kommunikationsbeziehungen in einem Produktionsnetzwerk transparent und kann damit den allgemeinen Zwecken der Inbetriebnahme und Wartung dienen. Als Überwachungslösung ist Monitoring ein geeignetes Mittel, um zum einen Vorgänge dahingehend zu prüfen, ob vorgegebene Verhaltensweisen eingehalten werden und zum anderen Abweichungen von festgelegten Mustern zu erkennen.

Anomalieerkennung ist ein Mittel zum Schutz von Netzwerken aller Art. 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.

Neben den technischen Systemen des Monitoring und der Anomalieerkennung sind weitere technische und organisatorische Prozesse für die Auswertung der vom System gelieferten Ergebnisse und Meldungen sowie für die darauf zu erfolgenden Reaktionen erforderlich.

Mit der zu beobachtenden Zunahme von Angriffen auf Produktionsnetzwerke und Netze in Kritischen Infrastrukturen werden Maßnahmen zur Erkennung solcher Angriffe mehr denn je erforderlich. Sie müssen zudem den komplexen Strukturen gerecht werden und erfordern daher entsprechende Systeme. Monitoring und Anomalieerkennung sollten jedoch nicht als alleinige Sicherheitslösungen, sondern immer im Verbund mit weiteren Schutzmaßnahmen eingesetzt werden. Monitoring ist nach ISO/IEC 27001[6] [7] (und damit verbunden mit der ISO/IEC 62443-4-2[8]) ein Bestandteil eines "Information and Security Management Systems" (ISMS).

9 Weitere Informationen

Als weiterführende Literatur zu den Cyber-Sicherheitsbedrohungen industrieller Anlagen bietet sich u. a. das Dokument "Top 10 ICS Bedrohungen und Gegenmaßnahmen" an. Als Grundlage für die Absicherung von Steuerungen und Industrieanlagen eignen sich das ICS Security Kompendium des BSI und weiterführend die BSI-Standards 200-1 bis 200-3 mit den entsprechenden Grundschutzbausteinen. Diese und weitere Dokumente sind verfügbar unter:

https://www.bsi.bund.de/ICS

Fragen, Hinweise und Anregungen zu dieser Empfehlung können an das nachstehende Postfach gesendet werden:

ics-sec@bsi.bund.de

10 Literatur- und Quellennachweis

[1] Mattis Mantere: Network Security Monitoring and Anomaly Detection in Industrial Control System Networks, 2015
[2] Wikipedia: Monitoring, 2018
[3] Bundesamt für Sicherheit in der Informationstechnik: Mindeststandard Logging, 2018
[4] Wikipedia: Anomalie, 2017
[5] Winter, Lampesberger, Zeilinger, Hermann: Anomalieerkennung in Computernetzen, 2011
[6] ISO/IEC 27001:2013: 9.1 Monitoring, measurement, analysis and evaluation, 2013
[7] ISO/IEC 27001:2013: Annex A: A.12.4 Logging and monitoring, 2013
[8] ISO/IEC 62443-4-2: Technical security requirements for IACS, Foundational Requirement (FR) 6, Timely response to events, 2017

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.