Logging & Monitoring

Problembeschreibung und Ursache

Logging und Monitoring spielen eine wichtige Rolle bei der Optimierung der Arbeitsabläufe, Erkennung der Fehler sowie ggf. der sicherheitsrelevanten Ereignisse. Vorfälle bzw. Ereignisse, die auftreten können, unterscheiden sich von Eintrittswahrscheinlichkeit und Schadenshöhe. Je nachdem welches Monitoringsystem im Unternehmen verwendet wird, kann dieses eine entscheidende Rolle bei der Gefahrenabwehr und den automatisierten Reaktionen darauf haben.

Logging

Logging bzw. Log-Files ermöglichen einen Einblick in die Vergangenheit. Die Ereignisse, die bis zum Zeitpunkt der Einsicht passiert sind, werden in den Logdateien gespeichert. Logging dient u. a. zur Aufzeichnung von Fehlern der Prozesse. Die Auswertung der gewonnenen Daten wird in der Regel manuell durchgeführt.

Monitoring

Monitoring hingegen ermöglicht eine Überwachung der Systeme, die festellen kann, ob diese Systeme das erwartete Verhalten während des Betriebs hat und gleichzeitig unerwartete Ereignisse erkennt und je nach Monitoringsystem kann diese sogar automatisch behoben werden.

Arten von Monitoring

In dem Level ,,Logging und Monitoring” werden zwei Arten von Monitoring näher betrachtet und miteinander verglichen, um einen Überblick über die Vor- und Nachteile der zwei Arten zu gewinnen und am Ende zu entscheiden, welche der zwei Arten mehr Sicherheit in Bezug auf OT-Systeme anbietet.

Regelbasierte Überwachung

Für das regelbasierte Monitoring werden Schwellenwerte in den zu überwachenden Funktionen und Systeme definiert und festgelegt. Dadurch werden Alarme bei Grenzüberschreitungen von den vordefinierten Werten ausgelöst.

KI-unterstützte Überwachung

Für das KI-unterstützte Monitoring werden die Logdateien gefiltert und harmonisiert, danach werden Logs für mehrere Zeitfenster gezählt. Anschließend wird ein Modell durch die aus dem vorherigen Schritt gewonnen Daten trainiert, in dem die Einträge von den verschiedenen Zeitfenstern miteinander verglichen und berechnet werden.

Dieses Dokument orientiert sich an:

- *Elektrische Bahn-Signalanlagen Teil 104: Leitfaden für die IT-Sicherheit auf Grundlage IEC 62443, insbesondere die Komponente Überwachung der Leistungsfähigkeit*
- *KI heute – Künstliche Intelligenz anwendbar - https://www.opitz-consulting.com/podcast-ki-heute*
- *Automatisierte Anomalie-Erkennung in komplexen Anwendungslandschaften - https://www.youtube.com/watch?v=X42WtQWWzKo*