Cyberattack Attribution Using AI-Enhanced Intrusion Detection with alert Correlation in Industrial Networks

In der sich ständig weiterentwickelnden Landschaft der industriellen Cybersicherheit bleibt die Zuordnung von Cyberangriffen eine entscheidende Herausforderung. Die mangelnde Anpassungsfähigkeit klassischer Intrusion Detection Systeme (IDS), gepaart mit hohen Fehlerquoten bei der kontextlosen Anomalieerkennung, und das Fehlen standardisierter forensischer Schnittstellen behindern eine effektive Reaktion. Diese Forschungsarbeit befasst sich mit diesen Herausforderungen, indem sie einen KI-gestützten Ansatz für die Zuordnung von Cyberangriffen in industriellen Netzwerken vorschlägt. Mit der zunehmenden Vernetzung der Industrie unterstreichen die Schwachstellen kleiner und mittlerer Unternehmen (KMU) den dringenden Bedarf an fortschrittlichen und zugänglichen Sicherheitsmaßnahmen

Eckdaten

Kurztitel

CAIDAN

Forschungsschwerpunkt

Digital Technologies

Laufzeit

01.10.2023 - 30.09.2026

Fördergeber

Bundesministerium für Bildung und Forschung

Projektträger

VDI/VDE Innovation + Technik GmbH

Projektleitung

Prof. Dr. Michael Heigl

Ziele

Ziel dieser Forschung ist es, die industrielle Cybersicherheit durch die Integration von KI in Systeme zur Erkennung von Eindringlingen zu revolutionieren. Unser Ziel ist es, eine genaue Zuordnung von Cyberangriffen in Echtzeit zu erreichen, das Situationsbewusstsein zu verbessern und operative Risiken zu mindern. Durch die Bewältigung der Herausforderungen, die sich aus der Komplexität von Netzwerken und den Schwachstellen kleiner und mittlerer Unternehmen ergeben, wollen wir einen skalierbaren, transparenten und effektiven Rahmen schaffen. Zu den wichtigsten Innovationen gehören ein hybrides System zur Erkennung von Anomalien auf der Grundlage des Datenkontexts, ein Korrelationsrahmen für präzise Warnungen und standardisierte forensische Bereitschaft. Diese Forschung zielt auf eine ressourceneffiziente, rechtzeitige Erkennung von Cyberangriffen, eine unbestreitbare Zuordnung und eine verbesserte Sicherheit der Infrastruktur ab.

Das Ergebnis wird die erfolgreiche Entwicklung und Integration eines KI-gestützten Intrusion Detection and Attribution Network zeigen. Durch umfassende Tests wird CAIDAN eine genaue Zuordnung von Cyberangriffen in Echtzeit, ein verbessertes Situationsbewusstsein und eine verbesserte Infrastruktursicherheit in verschiedenen Industrienetzen demonstrieren und seine Wirksamkeit und Anpassungsfähigkeit unter Beweis stellen.


Bundesministerium
für Bildung
und Forschung

CIM
LOGISTICS
SOFTWARE
SPECIALISTS

TGα

TECHNISCHE
HOCHSCHULE
DEGGENDORF
THD

TRUFFLEPIG
FORENSICS

UNIA
Universität
Augsburg
University