Andreas Amrein

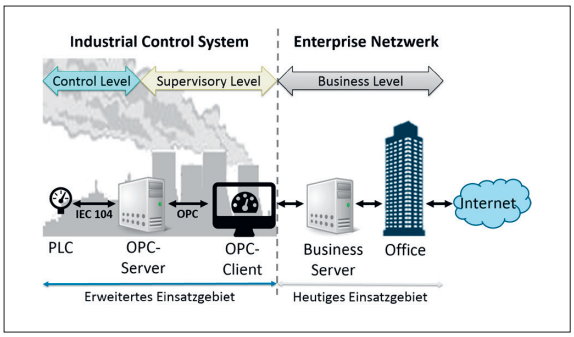
Micha Reiser

Diplomanden	Andreas Amrein, Micha Reiser
Examinator	Prof. Dr. Peter Heinzmann
Experte	Dr. Thomas Siegenthaler, CSI Consulting AG, Zürich, ZH
Themengebiet	Sicherheit
Projektpartner	Dr. A. Wespi, IBM Research, Rüschlikon, ZH

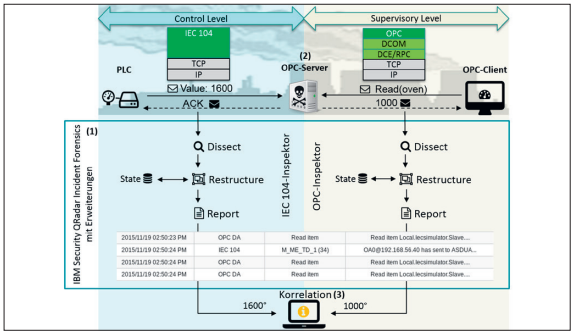
Multilevel Security Monitoring und Analytics in Industrial Control Systems

Erweiterung der IBM Security QRadar Incident Forensics Plattform zur Verarbeitung von Netzwerkverkehr aus industriellen Anlagen wie Stromversorgung oder Produktionsanlagen

Stromerzeugung, ein Beispiel für eine industrielle Anlage



ICS- und Enterprise-Netzwerk mit Unterteilung in die drei Levels «Control», «Supervisory» und «Business»



Integration der Erweiterungen in IBM Security QRadar Incident Forensics (1). Ein durch den OPC-Server (2) veränderter Wert wird erkannt (3).

Ausgangslage: Prozesse in industriellen Anlagen sind weitestgehend automatisiert. Die Steuerung und Kontrolle solcher Anlagen erfolgt mittels Industrial Control Systems (ICS). Immer häufiger werden ICS mit den Enterprise-Netzwerken und dem Internet verbunden. Dadurch werden diese zum Ziel von Cyber-Angriffen. Abbildung 2 unterteilt die Netzwerke in drei Levels. Der «Control Level» verbindet Feldgeräte von unterschiedlichen Herstellern mit einem Server. Der «Supervisory Level» schliesst mehrere Netzwerke aus dem «Control Level» zusammen und steuert diese mit einem einheitlichen, Feldgerät-Hersteller-unabhängigen Netzwerkprotokoll. Der «Business Level» repräsentiert das Firmennetzwerk. Ziel der vorliegenden Bachelorarbeit ist die Erfassung und Korrelation von Daten vom «Supervisory»- und «Control»-Level. Die Lösung ist in ein IBM-Produkt zu integrieren.

Vorgehen/Technologien: Für die forensische Analyse von Netzwerkverkehr betreibt IBM die «IBM Security QRadar Incident Forensics»-Plattform. Diese unterstützt verschiedene Netzwerkprotokolle und bietet eine Schnittstelle für Erweiterungen. Diese Arbeit erweitert die Plattform um die Netzwerkprotokolle IEC-104, DCE/RPC, DCOM und OPC (Abb. 3). Diese Erweiterungen sind in C++ geschrieben.

Ergebnis: Mit den implementierten Erweiterungen kann der Zusammenhang zwischen dem «Control Level» und dem «Supervisory Level» bei ICS untersucht werden. Damit wird das Kundensegment der «IBM Security QRadar Incident Forensics»-Plattform auf Betreiber von ICS vergrössert. Die Plattform soll bei einem grossen Stromproduzenten eingesetzt und getestet werden. Erste Analysen zeigen, dass ein kausaler Zusammenhang zwischen den untersuchten Levels besteht und dass es mittels Vergleich möglich ist, Cyber-Angriffe zu erkennen.