MSE | MASTER OF SCIENCE IN ENGINEERING

Forschungsprojektarbeit des Profils Information and Cyber Security

Entwicklung eines fortschrittlichen ICS-Honeypot-Proxysystems

Ausgangslage

Industrial Control Systems (ICS) sind kritische Infrastrukturen, die in zahlreichen Bereichen wie Energieversorgung, Wasseraufbereitung, Produktionsanlagen und Verkehrssystemen eingesetzt werden. Mit der zunehmenden Vernetzung dieser Systeme steigt auch das Risiko von Cyberangriffen erheblich. In der Schweiz betreiben sowohl grosse Unternehmen als auch KMUs solche Systeme, oft ohne ausreichende Sicherheitsmassnahmen. Honeypots sind eine bewährte Methode, um Angriffsmuster zu erkennen und zu analysieren, jedoch sind traditionelle IT-Honeypots für ICS-Umgebungen unzureichend. An der FHNW besteht durch enge Zusammenarbeit mit Industriepartnern und Forschungsprojekten im Bereich Cybersecurity eine umfassende Expertise zur Entwicklung spezialisierter Sicherheitslösungen für kritische Infrastrukturen. Dennoch fehlt es gerade bei kleineren und mittleren Unternehmen an angepassten, praxistauglichen Lösungen für die ICS-Sicherheitsüberwachung.

Zielsetzung / Methodik / Vorgehen

Für Betreiber von Industrial Control Systems soll ein innovativer ICS-Honeypot entwickelt werden, der als Proxy fungiert und vor bestehende Systeme geschaltet werden kann. Im Gegensatz zu herkömmlichen Honeypots, die lediglich simulierte Dienste anbieten, soll diese Lösung native ICS-Funktionalitäten nach aussen anbieten, während sie gleichzeitig Befehle abfängt oder nur innerhalb eines definierten Bereichs zulässt. Zunächst wird eine Analyse gängiger ICS-Protokolle (Modbus, Profinet, EtherNet/IP, etc.) durchgeführt, um die Kommunikationsmuster zu verstehen. Darauf aufbauend wird ein intelligentes Proxy-System konzipiert, das legitime Anfragen erkennt und gefährliche Befehle identifiziert. Für die Entwicklung sind fundierte Kenntnisse in Netzwerktechnik, Protokollanalyse und Sicherheitsarchitekturen erforderlich. Das System soll in der Lage sein, Angriffe zu protokollieren, Alarme auszulösen und gleichzeitig den regulären Betrieb nicht zu beeinträchtigen. Ein wesentlicher Teil der Aufgabe besteht darin, eine Balance zwischen Sicherheit und Betriebskontinuität zu finden. Zur Validierung muss ein Testumgebung mit realen ICS-Komponenten aufgebaut werden, in der verschiedene Angriffsszenarien simuliert und die Effektivität des Honeypot-Proxys evaluiert werden können.
Verlangte Skills: Kenntnisse in Netzwerksicherheit, Programmierung (Python, C/C++).

Teilaufgaben

Das Projekt kann in 3 Phasen durchgeführt werden: Fortlaufende Projekte 7 (Analyse der ICS-Protokolle, Konzeptentwicklung), 8 (Implementierung des Proxy-Systems, Aufbau der Testumgebung) und 9 (Evaluation, Optimierung und Dokumentation des Systems unter realistischen Bedingungen)

Studienart: [ ] Vollzeitstudium
[ ] Teilzeitstudium 50%

Projektorganisation: Einzelarbeit (im Umfeld eines Projektteams)

Projektfinanzierung: -

Arbeitsort: Windisch

Advisor: Prof. Dr. Christopher Scherb