Problemstellung

Mit der fortschreitenden Digitalisierung der kritischen Infrastruktur (KRITIS) in Deutschland kommt der Informationssicherheit aller beteiligten Systeme eine zentrale Rolle zu. Betreiber müssen ihre informationstechnischen Systeme langfristig sicher betreiben, auf Sicherheitsvorfälle angemessen reagieren und zusätzlich Maßnahmen zur Angriffserkennung treffen. Da die Komplexität der Steuerungs- und Überwachungsaufgaben innerhalb der Systeme zunimmt und die Anzahl und Intensität von Hackerangriffen auf die Datenkommunikation in kritischen Infrastrukturen steigt, muss die Wirksamkeit der Sicherheitsmaßnahmen daher alle zwei Jahre durch eine unabhängige Prüfstelle nachgewiesen werden.

Die SCADA-Systeme, die in der Energiewirtschaft und der Wasserversorgung eingesetzt werden, fallen in den Bereich der Operational Technology (OT) und erfordern daher spezielle OT-Sicherheitslösungen. Derzeit verfügbare Lösungen für OT-Security entsprechen jedoch eher adaptierten Verfahren und Maßnahmen aus der IT-Sicherheit, weshalb hier im Zusammenhang mit den speziellen Anforderungen der OT hinsichtlich Zuverlässigkeit, Verfügbarkeit sowie funktionaler Sicherheit noch einige Schwächen für den Einsatz in den SCADA-Systemen der KRITIS vorliegen. Außerdem können manche Teilsysteme aufgrund der harten Echtzeitanforderungen aktuell überhaupt nicht abgesichert werden, da die Anlagenverfügbarkeit eine höhere Priorität besitzt als die abgesicherte Kommunikation der einzelnen Geräte. Die Entwicklungen im Bereich des Edge Computing bedürfen ebenfalls innovativer Sicherheitsfunktionen speziell für die OT, um insgesamt ein höheres Sicherheitsniveau zu erreichen.

Klassische Security-Lösungen haben durch die zugrundeliegende Kryptografie nur eine begrenzte Lebensdauer, die die operative Einsatzdauer von Geräten in SCADA-Systemen, im Bereich mehrerer Jahrzehnte, deutlich unterschreitet. Dies führt dazu, dass die Sicherheitsmaßnahmen im Laufe der Zeit veraltet und unsicher werden können. Außerdem ist es schwierig, bestehende SCADA-Systeme zu aktualisieren oder zu modernisieren, da sie stark integriert sind und selbst kleine Änderungen Auswirkungen auf das gesamte prozesstechnische System haben können. Um diese Probleme zu lösen, müssen innovative Konzepte entwickelt werden, damit die Sicherheit und die Verfügbarkeit über die gesamte Missionszeit eines SCADA-Systems gewährleistet sind. Eine umfassende Sicherheitsstrategie ist notwendig, um ein hohes Sicherheitsniveau aufrechtzuerhalten und sicherzustellen, dass die kritischen Infrastrukturen zuverlässig und sicher betrieben werden können.

Zielsetzung des Forschungsvorhabens

Um die Bedrohungen von Cyberangriffen gegen kritische Infrastrukturen zu minimieren und die derzeitigen Probleme verfügbarer Sicherheitslösungen zu beheben, hat das Gesamtvorhaben das Ziel, einen ganzheitlichen Ansatz für OT-Security in kritischen Infrastrukturen zu entwickeln. Im Wesentlichen sollen die Forschungs- und Entwicklungsarbeiten des Vorhabens langfristig Beiträge für zwei Schwerpunkte liefern:

1. Schwächen und Lücken derzeitiger Maßnahmen der OT-Security verbessern
2. Langlebigkeit von Maßnahmen der OT-Security steigern

Um die für das Forschungsprojekt relevanten OT-Systeme umfänglich abzudecken, soll ein übergeordnetes Sicherheitskonzept entstehen, welches die spezifischen Anforderungen und Rahmenbedingungen der OT-Systeme der KRITIS berücksichtigt. Zudem soll der aktuelle Stand der Technik (bereits eingesetzte Technologien und insbesondere auch aktuelle Normen und Standards für OT-Security) gezielt erweitert und ergänzt werden, um die identifizierten Herausforderungen und Schwächen anzugehen. Mit dem Hintergrund der langen Missionszeit der OT-Systeme sollen die

Forschungsarbeiten des Projekts gezielt so ausgelegt werden, dass neben Neuinstallationen auch bestehende Systeme nachgerüstet werden können (Retrofit), um eine Übergangsstrategie zu schaffen.

Die konkreten Ergebnisse der Forschungs- und Entwicklungsarbeiten sollen zwei Ausprägungen besitzen. Einerseits sollen neue Technologien für OT-Security entwickelt und bestehende Technologien verbessert werden. Diese können dann nach Projektende in Produkt- und Systementwicklungen verwertet werden sowie in Standardisierungsprozesse einfließen. Andererseits sollen mehrere Prototypen von Security-Modulen entstehen, welche als Demonstratoren für die entwickelten Technologien dienen und die technische Umsetzbarkeit darlegen sowie als Grundlage für Verifikationsarbeiten dienen. Diese sollen im Nachgang des Projekts zudem als eigenständige Produkte industrialisiert werden. Die Entwicklung der Projektlösungen in Deutschland bzw. Europa soll zudem nationale Lösungsansätze für die Absicherung der kritischen Infrastruktur fördern und Abhängigkeiten ins Ausland minimieren.

Im Forschungsprojekt werden die OT-Systeme in zwei Ebenen aufgeteilt: die zugrundeliegende Prozessebene und die übergeordnete Leitebene. Beide Ebenen werden individuell und im Verbund betrachtet, um langfristig zur Sicherheit beizutragen. Um die Technologiedemonstration mithilfe der bereits erwähnten Security-Module optimal zu gestalten und alle Aspekte der beiden definierten Ebenen abzubilden, sind insgesamt drei Skalierungsstufen der Module geplant. Diese Strukturierung berücksichtigt die individuellen Anforderungen der Teilbereiche der OT-Systeme sowie das Zusammenspiel als Gesamtsystem.

Auf Basis der generellen Zielsetzung wurden fünf konkrete Forschungsaspekte und Themenschwerpunkte herausgearbeitet, welche im Rahmen des Forschungsprojekts bearbeitet werden:

1. OT-Security innerhalb der KRITIS für Entwicklungen der IT/OT-Convergence
2. OT-Security innerhalb der KRITIS für kritische Datenströme auf Prozessebene
3. Spezialisierte Angriffserkennung für OT-Systeme der KRITIS
4. Crypto-Agilität für langfristige Gerätesicherheit in OT-Systemen der KRITIS
5. Crypto-Agilität für langfristige Kommunikationssicherheit in OT-Systeme der KRITIS

Im Kontext der angewandten Forschung werden bei den Forschungsarbeiten an diesen Themenschwerpunkten innovative technologische Ansätze entwickelt, um die Sicherheitsfunktionen für die OT-Systeme kritischer Infrastrukturen kurz- und langfristig zu verbessern. In den technischen Arbeiten des Projekts werden dann entsprechend die Security-Modulprototypen zur Demonstration der Technologien entwickelt, um deren Umsetzbarkeit darzulegen und die Ergebnisse verifizierbar zu machen.