IT-Sicherheit für Kritische Infrastrukturen – State of the Art

Ergebnisse des Förderschwerpunkts IT-Sicherheit für Kritische Infrastrukturen ITS|KRITIS des BMBF

Steffi Rudel, Ulrike Lechner

Das hybride Labor als Testumgebung für IT-Sicherheit

David Kotarski, Stephan Arndt, Christof Thim

Forschungsprojekt:
Aqua-IT-Lab

IT-Sicherheitsassessments im Hybridtestlabor

Kleine und mittlere Versorger scheuen häufig das Testen der IT-Sicherheit an laufenden Systemen wie z. B. bei Penetrationstests oder Sicherheitsassessments vor Ort. Zu hoch sind die Risiken von Seiteneffekten und ungeplanten Ausfällen der Versorgungsinfrastruktur. Dem begegnet der Gedanke des hybriden Testlabors, welches die kritischen Komponenten der Versorgungsinfrastruktur abbildet und risikolos mit festgelegter Zielrichtung analysierbar macht.

Laborarchitektur

Das Labor besteht aus vier Komponententypen, welche in Abbildung 1 dargestellt sind. Zunächst werden Kopf-SPS, also industrielle Steuerungseinheiten, physisch vorgehalten. Sie dienen dazu, zeitkritische Steuerungscodeanteile auszuführen. In Versorgungssystemen spielen diese Kopf-SPS zumeist eine aktiv steuernde Rolle und sind somit ein besonders schützenswerter Bestandteil der IT-Infrastruktur.

Neben den Hardwarekomponenten werden periphere Komponenten, wie passive Pumpensteuerungen, Sensorik etc., über simulierte SPS abgebildet. Diese Steuerungssimulation ist analog zum realen Versorgungssystem über entsprechende Protokolle an die Hardwarekomponenten angebunden.

Weiterhin können zur Überwachung und Steuerung reale Leit- und Monitoring-Systeminstanzen verwendet werden, um z. B. die Übernahme des Prozessleitsystems abzubilden.

Zur Steuerung der Simulation wird ein Command-and-Control-Server verwendet, mit dem die simulierten Slaves durch einen Nutzer manipuliert werden können. So ist es beispielsweise möglich, die Auswirkungen eines durch Angreifer manipulierten oder blockierten Datenverkehrs zwischen Kopf-SPS und dezentraler Peripherie zu simulieren, indem entsprechende Einstellungen über den Command-and-Control-Server vorgenommen werden.

Auch eine Simulation von weiteren Versorgungseffekten, wie beispielsweise der Wasserdruck in Rohrnetzen, soll durch Anbindung einer Softwaresimulation an die Logging-Datenbank in das Szenario integriert werden. Ziel ist die Aufdeckung von Effekten, wie geplatzte Leitungen durch unzulässige Druckverhältnisse, die bei Manipulation des Steuerungs-Datenverkehrs vielleicht auftauchen könnten.

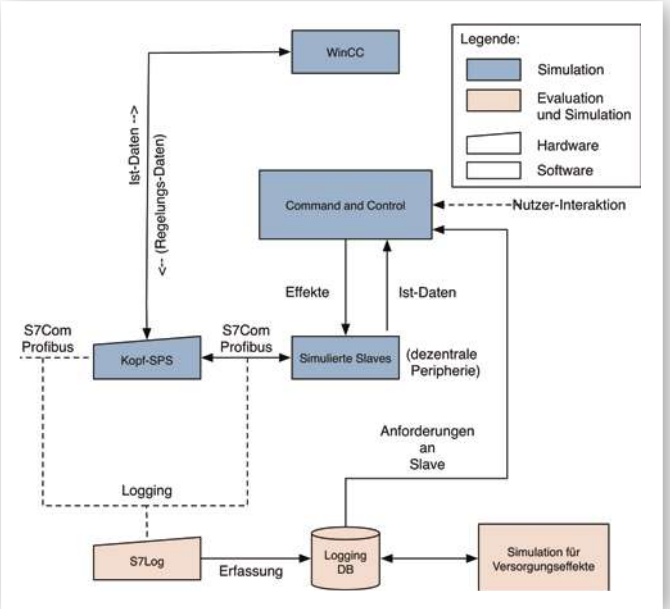

Abb.1: Grundarchitektur des hybriden Testlabors

Für die Nachvollziehbarkeit der Versuche und zur späteren Auswertung ist es vorgesehen, jegliche Kommunikation zwischen SPS-Komponenten und Simulation über einen Logging-Dienst aufzuzeichnen, und in einer Datenbank abzuspeichern. Das Logging soll hierbei durch eine weitere, dedizierte SPS übernommen werden, um den Programmablauf der Simulation nicht für das Aufzeichnen von Logging-Daten verändern zu müssen.

Der Laboraufbau kann je nach Untersuchungsziel variiert werden. Hier werden zwei mögliche Szenarien beschrieben, welche im Projekt Aqua-IT-Lab behandelt wurden.

Szenario 1: Angriff auf die standortübergreifende Kommunikation

Im ersten Szenario wird eine standortübergreifende Kommunikation nachgebaut und auf typische Angriffsvektoren, wie beispielsweise das unbefugte Eindringen in die Infrastruktur, geprüft. Abbildung 2 verdeutlicht das zu untersuchende Szenario. Es wurde von einem unserer Forschungspartner übernommen, um einen realitätsgetreuen Aufbau zu garantieren.

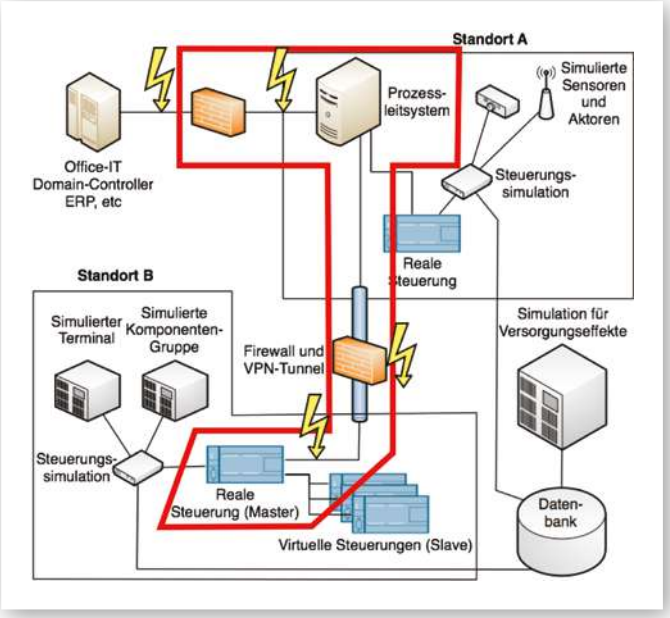

Abb. 2: Laboraufbau Szenario 1

Die zwei Standorte, die hier dargestellt werden, sind ein Prozessleitsystem (Standort A), mit dem eine Leitwarte simuliert wird, sowie ein Standort mit einer SPS, die eine zu überwachende Anlage in der Infrastruktur abbildet (Standort B). Beide Standorte sind mittels VPN-Gateways miteinander verbunden und kommunizieren damit verschlüsselt im öffentlichen Teil miteinander. Der Pentest-PC stellt den Angreifer da, er ist mit mehreren Netzwerkkarten an verschiedenen Zugangspunkten verbunden, sodass mehrere Arten von Angreifern zeitgleich ohne Änderung der Konfiguration simuliert werden können.

Der erste untersuchte Angriff erfolgt von außerhalb des Unternehmens. Hierbei ist das Ziel des Angreifers, von außen in den verschlüsselten VPN-Verkehr einzudringen oder Lücken in der Konfiguration der beiden Firewalls aufzuspüren. Dabei wird die identische Hardware wie beim Untersuchungsgegenstand eingesetzt. Die Konfiguration dieser Hardware ist ebenfalls ein Abbild des Produktivsystems. Somit können alle erzielten Erkenntnisse auf das zu überprüfende System überführt werden.

Der zweite simulierte Angreifer geht von einer Kompromittierung der internen Verbindung aus und stellt somit eine interne Bedrohung dar. Dabei werden die ebenfalls nachgestellten Systeme (Prozessleittechnik und SPS) jeweils auf Schwachstellen untersucht. Auf beiden Systemen läuft die identische Konfiguration wie auf dem Produktivsystem von einem Forschungspartner, damit die Übertragung der Erkenntnisse gesichert bleibt.

Szenario 2: Resilienz des Versorgungssystems

Im zweiten Szenario steht die Untersuchung der Effekte, die ein interner Angreifer auf eine Infrastruktur im Bereich der Wasserversorgung haben kann, im Fokus. Im Gegensatz zum ersten Szenario liegt der Fokus daher nicht auf der Sicherheit von Lösungen zur Abschirmung des internen Netzes vor externen Angriffen oder den Zugriffskontrollen, die für interne Prozessleit- oder SPS-Systeme vorhanden sind, sondern es soll eine Untersuchung stattfinden, welche Auswirkungen verschiedene Arten von Angriffen auf die Gesamtinfrastruktur haben.

Der Versuchsaufbau besteht zu diesem Zweck aus der Nachbildung verschiedener Sektionen realer Wasserwerke. Im Mittelpunkt der Architektur steht die Kopf-SPS, auf der die Steuerungslogik für den zu untersuchenden Teilabschnitt liegt, sowie die Peripherie, die von dieser SPS gesteuert wird (Abbildung 3).

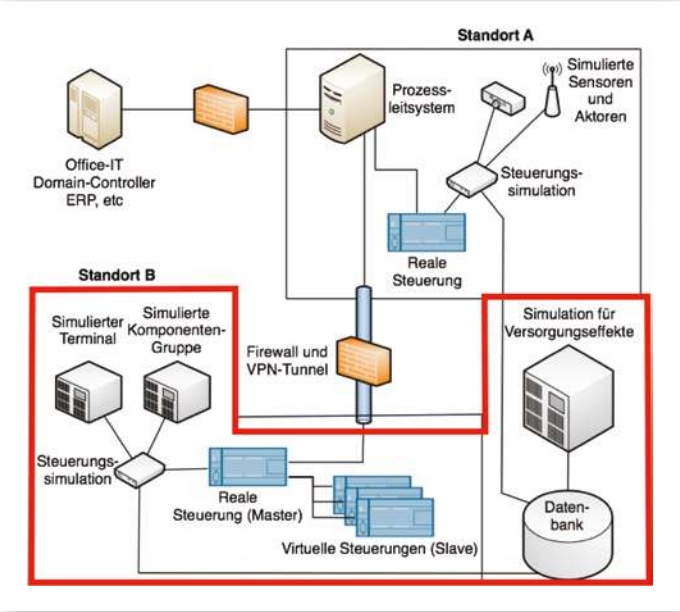

Abb. 3: Laboraufbau Szenario 2

Da aus Kostengründen die nachzubildenden Sektionen nicht komplett als Hardware bereitgestellt werden können, werden die peripheren Komponenten des Wasserwerkes durch eine Softwarelösung simuliert. Diese Systeme werden häufig über reine Slave-Sensoren oder -aktoren implementiert, welche keine oder nur sehr rudimentäre Steuerungslogik enthalten. Sie hängen von den Steuerungsbefehlen der Kopfsysteme ab, also den Steuerungen, auf denen die eigentliche Steuerungslogik ausgeführt wird. Diese sind in Hardware vorhanden, um eine möglichst detailgetreue Simulation der nachgebildeten Sektionen garantieren zu können und auch hardwarespezifische Latenzen berücksichtigen zu können. In diesem Aufbau werden die originalen Steuerungsprogramme für die Simulation und die Hardwarekomponenten verwendet.

Der Sicherheitstest bezieht sich nun auf den Zugriff auf die SPS und die Überprüfung der Robustheit des verwendeten Codes. Dabei wird davon ausgegangen, dass der Angreifer bereits den Sicherheitsperimeter überschritten hat und sich im gleichen Netz wie die SPS befindet.

Anders als in Szenario 1 kommt hierbei die gesamte Laborinfrastruktur zum Einsatz. Nicht nur die Möglichkeit des Zugriffs und der Manipulation, sondern die Wirkung kompromittierter Anlagen im Versorgungssystem wird untersucht. Die Kopfstationen bilden den Schwerpunkt der Überprüfung. Gelingt es dem Angreifer, dort einzudringen oder die Steuerungssignale zu manipulieren, sind die Auswirkungen auf den simulierten Steuerungen und später die Effekte in der Versorgungssimulation direkt zu beobachten. So können der Umfang und die Ausdehnung des Versorgungsausfalls besser abgeschätzt werden. Dies erleichtert die Planung reaktiver Maßnahmen und sensibilisiert für Investitionen in Prävention. Das mitlaufende Logging zeigt im Nachgang die Lücken auf und ermöglicht eine Detailanalyse des Angriffs. Hieraus können sowohl Versorger als auch Penetrationstester Muster der Angriffe erlernen. Der IT-Verantwortliche ist damit in der Lage, auffälliges Verhalten der Anlage schneller zu erkennen und früh Gegenmaßnahmen einzuleiten.

Wie in den Szenarien gezeigt werden konnte, eignet sich der hybride Ansatz, um ohne große Risiken in einem begrenzten Testumfang Sicherheitsassessments durchzuführen. Er bildet somit für Versorger einen Ansatzpunkt zur Vertiefung der Analysen aus dem Schnelltest. Weiterhin können IT-Sicherheitsunternehmen mithilfe des Labors radikaler testen und auch Ausfälle einzelner Komponenten und Regelkreise provozieren. Die hierdurch erzielten Effekte erhöhen die Sensibilität der Versorger bei der Absicherung ihrer Steuerungs-IT.

Für die weitere Forschung bildet die Infrastruktur die Möglichkeit, Seiteneffekte von Angriffen genauer zu betrachten und über einen längeren Zeitabschnitt die Wirkung im Versorgungssystem zu untersuchen. Auch die Nutzung als HoneyPot zur Analyse externer Angreifer und zur Identifikation ihrer Angriffsmuster ist denkbar.