Titel: Aqua-IT-Lab – Eine Testumgebung für Penetrationstest im Wassersektor
Autoren: Christof Thim, David Kotarski, Stephan Arndt

Einleitung

Die Wasserversorgung bildet das Rückgrat für das Funktionieren des Gemeinwesens und ist somit durch den Bund als Kritische Infrastruktur definiert. Entsprechend sollten Wasserversorgungsinfrastrukturen besonders im Hinblick auf Kompromittierung und Ausfall geschützt werden. Hierzu zählen zum einen Maßnahmen des Schutzes der natürlichen Ressourcen, der genutzten Bauwerke und des Versorgungsprozesses, sowie seit der Novellierung des IT-Sicherheitsgesetzes und der entsprechenden Verordnung auch die Informations- und Steuerungsinfrastruktur. Selten existieren noch sehr kleine Versorger, welche die Versorgung komplett ohne Informationstechnik durchführen. In den meisten Fällen werden Pumpen, Druckerhöhungsstationen und Kaskaden über IT-Komponenten gesteuert und überwacht. Bei deren Implementierung spielt Betriebs- und Ausfallsicherheit eher eine Rolle als IT-Sicherheit. Durch die gestiegene Anzahl Bedrohungen und die leichte Verfügbarkeit von Informationen z.B. über Suchmaschinen wie shodan.io oder censys.io sowie von Werkzeugen zum Einbruch in Informationssysteme sollten diese Infrastrukturen zeitnah durch die Versorger auf ihre Sicherheit überprüft und abgesichert werden.
Insbesondere kleine und mittlere Versorger geraten dabei schnell an die Grenzen ihrer personellen und finanziellen Leistungsfähigkeit. Das BMBF-geförderte Forschungsprojekt Aqua-IT-Lab nimmt sich den auftretenden Problemen an und stellt Werkzeuge für eben jene Versorger bereit, um ihre Infrastruktur zu überprüfen und abzusichern. Zunächst können über einen Schnelltest die grundlegende Fitness des Versorgers ermittelt und erste Maßnahmen ausgewählt werden. Spezifische Sicherheitsrisiken (Fehlkonfigurationen, Sicherheitslücken) können in einer Laborumgebung über Penetrationstests aufgedeckt werden.
Sowohl das Labor als auch der Schnelltest ergänzen die im Branchenstandard W1060 dargestellten Analysen und Maßnahmen. Dem Betreiber werden über beide Werkzeuge Informationen zur Verfügung gestellt, welche das Sicherheitsniveau seiner IT-Infrastruktur deutlich erhöhen können und dabei ressourceneffizient vorgehen. Der Aufbau und die Analysemöglichkeiten dieses Labors werden im folgenden Artikel genauer dargestellt.

Penetrationstests in kritischen Infrastrukturen

Obwohl Penetrationstests ein veritables Mittel zur Überprüfung der IT-Sicherheit sind, schrecken viele Versorger davor zurück, externe Hacker zu verpflichten. Dies hängt zum einen damit zusammen, dass gerade der Zugriff auf versorgungsrelevante Teile der Infrastruktur mit einem nicht zu unterschätzenden Risiko verbunden, dass der Testangriff tatsächliche Folgen in der Versorgung zeigt. Hinzu kommt, dass viele Hacker zwar auf Angriffsmöglichkeiten in der Büro-IT spezialisiert sind und auch die Folgen ihrer Aktivitäten abschätzen können, im Steuerungsumfeld sind jedoch recht wenige professionelle Hacker erfahren. Seiteneffekte der Angriffe können leicht zum Ausfall von zentralen Steuerungskomponenten führen. Weiterhin können die tatsächlichen Folgen einer erfolgreichen Attacke in der realen Umgebung nicht hinreichend überprüft werden. Da kein Betreiber das Risiko eingeht, zentrale Komponenten kompromittieren zu lassen oder einen Ausfall gezielt zu provozieren, werden Penetrationstests in kritischen Infrastrukturen häufig nicht mit letzter Konsequenz durchgeführt.
Diesen Risiken von Penetrationstests kann über die Nutzung einer Testumgebung begegnet werden. Viele größere Versorger verfügen zu Testzwecken über einen teilweisen Nachbau der steuerungsrelevanten Komponenten. Kleinen und mittleren Versorgern fehlen zum einen die Mittel für das Vorhalten zusätzlicher Komponenten, zum anderen stehen ihnen selten die notwendigen personellen Ressourcen zum Aufbau der Testumgebung sowie zum Überprüfen der IT-Sicherheit zur Verfügung. Hier setzt der Gedanke des Testlabors an, welches die bestehende Infrastruktur in Teilen physisch und in Teilen simulativ abbildet und damit den Penetrationstestern eine geeignete Umgebung bereitstellt.

Beschreibung des Labors

Im Labor kann nicht die komplette Infrastruktur des Betreibers nachgestellt werden. Vielmehr ist das Labor hybride aufgebaut. Dabei werden einige, gezielt ausgewählte Komponenten in Form baugleicher Hard- und Software im Labor genutzt. Die anderen Komponenten werden als Softwaresysteme realisiert. Hierdurch wird erreicht, dass bestimmte, besonders exponierte, aktiv steuernde bzw. zeitkritische Elemente der Versorgungs-IT in der Form aufgenommen werden, wie sie auch im Feld anzutreffen sind. Andere Komponenten, welche eher passiv genutzt werden oder nicht im Fokus der Sicherheitsuntersuchung stehen, werden simuliert bzw. virtualisiert.

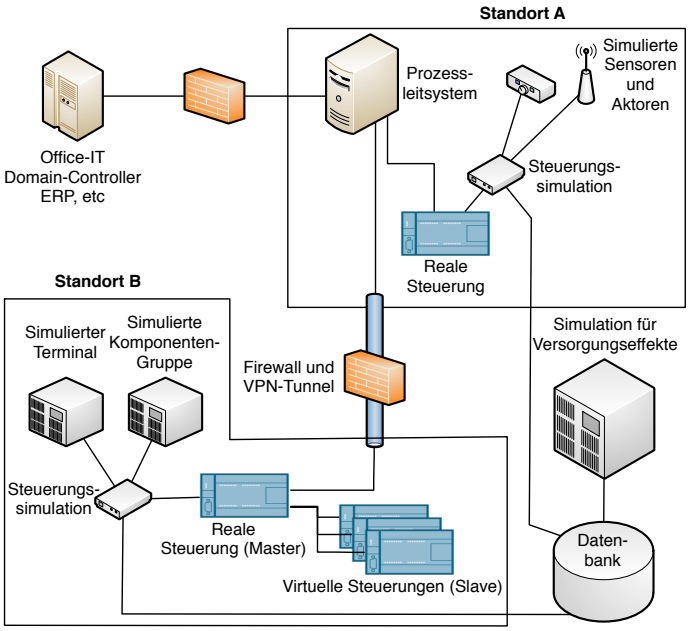

Abbildung 1: Exemplarischer Aufbau des Testlabors

Die Entscheidung, welche Komponente physisch und welche softwaretechnisch abgebildet wird, hängt zum einen vom Ziel der Überprüfung und zum anderen von einer Risikoanalyse sowie einer Aufwand-Nutzen-Abwägung ab. Bei Black-Box-Tests, welche allein das Eindringen in die Infrastruktur zum Ziel haben, werden die Netzzugangspunkte physisch bereitgestellt und Systeme hinter den Absicherungen simuliert. Ist das Ziel hingegen eine Code-Revision, wird eine physische Abbildung der relevanten Steuerungssysteme (SCADA, SPS, etc.) realisiert. Andere Aspekte wie z.B. passive Elemente der Versorgung, welche nur Steuerungssignale von den Master-SPS erhalten, können simulativ abgebildet werden.
Die Risikoanalyse und die Komplexitätsabwägung der Simulation verfeinern die Entscheidung, was hardwaretechnisch in das Labor eingebunden wird. Jene Komponenten, welche komplexen Steuerungscode ausführen und aktiv Entscheidungen treffen, werden als reale SPS mit entsprechendem Steuerungscode verwendet. Dies sind insbesondere Masteranlage bzw. Steuerungsköpfe an den einzelnen Außenstellen, welche aufgrund ihres zeitkritischen Antwortverhaltens und der Komplexität und Spezifik der Steuerungsprogramme schwer in eine Softwaresimulation zu übertragen sind. Weiterhin würden spezifische Schwachstellen kaschiert, die nur durch die Verwendung der realen SPS und des realen Steuerungscodes vorliegen.
Alle weiteren relevanten Komponenten werden simuliert. Dafür wurde ein Python-Programm auf Basis von PyProfibus entwickelt. Die Simulation beinhaltet drei Haupt-Komponenten: einen Multiplexer, einen Publisher und mehrere Slavesteuerungen. Die Verbindung zu den realen Komponenten wird über den Multiplexer realisiert, welcher die Profibus-DP Kommunikation zwischen dem physischen Bus und den Slaves vermittelt. Der Publisher übermittelt die Werte der Slaves an einen Kommando-Server und eine Datenbank zur späteren Analyse. Den Kern bilden die Slaves (Profibus-DP-Slaves). Sie können unterschiedlich, entsprechend ihrer realen Nutzung konfiguriert werden. Es werden hierfür u.a. ihre Fähigkeiten, die Gruppennummer sowie die Anzahl

und Art der Anschlüsse definiert. Jedem Slave sind auch Inputs und Outputs zugeordnet. Die eigentliche Simulation der Umsetzung der Steuerungsbefehle der Master-SPS erfolgt in einer separat implementierten Simulationskomponente. Für jeden Slave werden zyklisch die Outputs aufgenommen, die dieser setzen soll, und entsprechend des Simulationscodes verarbeitet. Etwaige, an den Master zurückgemeldete Inputs werden ebenfalls in der Simulation berechnet. Die Berechnung erfolgt durch eine Umsetzung des Steuerungscodes in Python-Programmen. Da die Slaves keine komplexen Steuerungsaktivitäten durchführen, ist diese Umsetzung kosteneffizient durchzuführen. Die Kommunikation zur Masteranlage erfolgt für den Master transparent über einen Multiplexer, wobei der Master in regelmäßigen Abständen Steuerungsoutputs sendet und die vorliegenden Inputs im entsprechenden Telegram zurückgemeldet bekommt. Das Antwortverhalten beliebiger Profibus-DP Slaves kann dementsprechend abgebildet werden, sodass die original eingesetzte Hardware nicht benötigt wird.
Tabelle 1 stellt die Vorteile der Hard- und Softwareabbildung im Labor gegenüber.

Tabelle 1: Vorteile der Nutzung physischer und simulierter Komponenten

Hardwarekomponenten	Softwaresimulation
Echtzeitfähigkeit	Kostengünstig
Direkter Transfer bestehender Programme	Replizierbar
Keine Abstraktion bei den Ergebnissen	Beliebig konfigurierbar

Zur Überprüfung der Sicherheit werden eine Reihe von Werkzeugen eingesetzt. Die Überprüfung des Netzwerkes findet u.a. über NMAP, Wireshark und Burp Suite statt. Die Authentifizierung wurde über Hydra getestet. Bekannte Schwachstellen und die dazugehörigen Exploits konnten über METASPLOIT, NESSUS sowie Nikto ermittelt werden. Hinzu kam eine Reihe von Spezialwerkzeugen, welche durch das beteiligte Sicherheitsunternehmen verwendet werden. Die Ergebnisse der Überprüfung werden protokolliert und im Nachgang bewertet. Bewertungskriterien waren die potenziellen Auswirkungen, welche die Ausnutzung der Schwachstelle haben kann und die Komplexität des Angriffs.

Überprüfte Szenarien

Während des Projektes Aqua-IT-Lab wurden zwei Szenarien untersucht, um die Anwendbarkeit der Simulation für die Sicherheitsanalyse zu überprüfen. Beide basieren auf einem ähnlichen Setup mit einer Leitstelle und einer angebundenen Außenstelle.

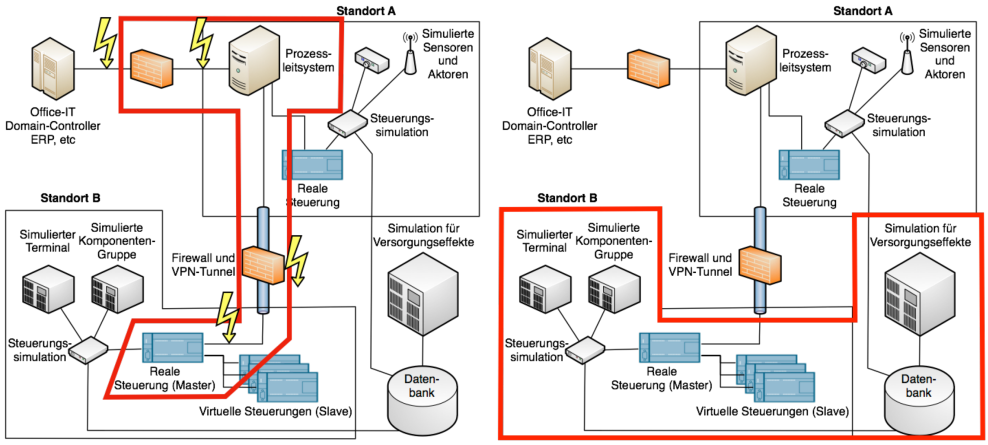

Abbildung 2: Darstellung des Umfangs der überprüften Szenarien: a) Kommunikationswege; b) Steuerungscode

Im ersten Szenario standen die Kommunikationskanäle und die Erreichbarkeit der Anlagen im Fokus. Hierfür wurden zwei Einstiegspunkte für den externen Angreifer definiert (siehe Abbildung

2a):

1. Die Erreichbarkeit der Anlagen aus dem Internet, die Sichtbarkeit und Sicherheit des VPN-Tunnels sowie die Konfiguration der eingesetzten Firewall wurde durch den Zugang des Angreifers komplett außerhalb des Firmennetzes überprüft.
2. Die Prüfung der firmeninternen Sicherheit erfolgte über einen zweiten Zugangspunkt in einer Außenstelle, zu der sich der Angreifer Zutritt verschaffte. Darüber versucht er in das über die Rückkanäle zur Leitwarte Steuerungsnetz einzudringen.

Da die Netzwerkgeräte und die Zielsysteme im Zentrum der Untersuchung standen, wurden sie als Hardwarekomponenten genutzt und ihre Konfigurationen von den Originalgeräten übertragen. Konkrete Versorgungseffekte wurden nicht betrachtet und daher auf die Nutzung simulierter SPS verzichtet.
Die Ergebnisse des ersten Tests zeigen, dass die genutzte Konfiguration der Firewall und des VPN keinen sinnvollen Angriffspunkt darstellt. Einzig das Angebot eines nicht genutzten und konfigurierten Dienstes nach außen wurde als potenzielle Gefährdung kritisiert. Am zweiten Zugriffspunkt (Außenstelle) erhielt der Angreifer Zugriff auf das gesamte Netz im Test. Hier wurden schwache Passwörter und alte Patchstände im Steuerungssystem als Schwachstellen identifiziert. Ein Angreifer hätte damit die Möglichkeit gehabt, Code auf dem System auszuführen oder die gesamte Anlage zu stoppen. Die Steuerungen selbst wiesen kein adäquates Sicherheitsniveau (Lese/Schreibschutz) auf, so konnten z.B. Anmeldedaten extrahiert werden und der Betrieb über Denial-of-Service-Attacken gestört werden. Insgesamt zeigt sich, dass die Ressourcen zur Erstellung und Implementierung eines umfassenden Sicherheitskonzeptes fehlen. So bleibt Passwort- und Patchmanagement und eine regelmäßige Überprüfung der Konfiguration auf der Strecke.

Im zweiten Szenario soll die Resilienz der Steuerungskomponenten überprüft werden. Hier ist der Zugriff auf das Steuerungsnetzwerk vorausgesetzt (Abbildung 2b). Dieses Szenario dient dazu, den Worst-Case abzubilden und die Effekte bei kompromittierten Steuerungen zu überprüfen. Als Angriff wird die Manipulation von Werten innerhalb der SPS-Konfiguration oder die Beeinflussung der Kommunikationspakete zwischen dem Leitstand und den SPS geprüft. Vier unterschiedliche Angriffstypen werden überprüft:

1. Replay-Angriffe: Vom Angreifer aufgezeichnete Kommunikation im Steuerungssystem wird zu einem späteren Zeitpunkt wiedergegeben. Ohne Verständnis des Protokolls können Kommunikationsstörungen können hervorgerufen werden.
2. Man-in-the-Middle-Angriffe: Der Angreifer manipuliert den Datenverkehr zwischen beiden Kommunikationspartnern. Er gibt der Leittechnik z.B. falsche Pegelstände oder Drehzahlen zurück und provoziert somit neue Steuerungsbefehle, die zum Ausfall der Komponenten führen können.
3. Denial/Degradation of Service (DoS) Angriffe: Die Kommunikation zwischen den Steuerungsgeräten wird über zusätzliche Netzwerklast verzögert. Komponenten können ausfallen, da sie keine Steuersignale oder Statusinformationen erhalten.
4. Authentication Bypass Angriffe: Der Passwortschutz der SPS wird umgangen. Der Angreifer lauscht auf den Datenverkehr der Authentifizierung legitimer Netzteilnehmer und verwendet deren Authentifizierungtoken weiter. Er kann direkten Zugriff auf die Steuerung erhalten.

Im zweiten Szenario kommt eine Mischung aus physischen und simulierten SPS sowie einer Effektsimulation zum Einsatz, um die Auswirkungen der Manipulation im Versorgungsnetz abzubilden. Als physische Komponenten werden die Mastersteuerungen auf S7-3xx Basis genutzt. Bei den simulierten Steuerungen handelt es sich um passive Elemente, wie z.B. Wasserstandssensoren oder Klappensteuerungen. In der Effektsimulation wird das betroffene Versorgungsnetz abgebildet und die entsprechenden Komponenten als Input genutzt.
Anders als im ersten Test liegen noch keine Ergebnisse vor, da die Tests und Auswertungen noch andauern.

Möglichkeiten und Grenzen der Umgebung

Das im Projekt Aqua-IT-Lab entstandene Testumgebung bietet kleinen und mittleren Versorgern die Möglichkeit, ohne großes Risiko und erhebliche finanzielle Aufwendungen ihre Infrastruktur tiefen IT-Sicherheitstests zu unterziehen. Es wird eine realitätsgetreue Darstellung der Infrastruktur über die Verwendung realer Steuerungskomponenten und realen Steuerungscodes erzielt. Periphere, passive Komponenten werden hingegen effizient in einer Simulation abgebildet. Der Versorger erhält somit eine Umgebung, in welcher er Penetrationstester ihr gesamtes Repertoire nutzen lassen und die Effekte beobachten kann.
Der Ansatz hat jedoch Grenzen, weshalb einen Test oder zumindest ein Audit der Ergebnisse vor Ort nicht ersetzt werden kann. So kann nur eine begrenzte Anzahl von Systemen abgebildet werden. Komplexe Angriffsvektoren, die über mehrere Komponenten hinweg funktionieren, sind nicht adäquat abbildbar. Auch betriebswirtschaftliche Systeme, welche gegebenenfalls an die Steuerungsinfrastruktur angebunden sind, lassen sich bisher nicht hinreichend einbinden. Angriffe, welche sich auf den Faktor Mensch konzentrieren (Social Engineering), können über eine Simulationsumgebung nicht abgedeckt werden.
Es zeigt sich jedoch insgesamt, dass der Gedanke einer Testumgebung effektiv in einer Kombination aus Hard- und Softwarekomponenten realisiert werden kann. Damit ist es möglich, das Sicherheitsniveau der Nutzer erheblich zu steigern, indem dieser auf Expertise und harte Infrastrukturtests zurückgreifen kann.