IT-Sicherheit und ihre Anforderungen an moderne cyber-physische Systeme

Intelligente und vertrauenswürdige Energiespeicher

In einer modernen Industriegesellschaft entsteht mit zunehmendem Wachstum der Bedarf an immer intelligenteren Versorgungs- und Netzstrukturen. Dank gestiegenem Verantwortungsbewusstsein liegt dabei angesichts der Knappheit der Ressourcen oft ein besonderes Augenmerk auf der Nachhaltigkeit der Rohstoffe. Ein sehr spannendes Beispiel dafür liefert aktuell das Ruhrgebiet. Dort wird derzeit eine bislang ziemlich einzigartige Form der Wärmespeicherung erforscht: Die tiefen Stollen stillgelegter Zechen sollen die Wärmeenergie verschiedenster Erzeuger im Sommer speichern und in kälteren Jahreszeiten wieder abgeben. Wichtigstes Element der dafür nötigen, komplexen Steuerungen sind sogenannte cyber-physische Systeme. Durch ihre physische Komponente haben sie direkten Einfluss auf die reale Welt. Eine Manipulation ihrer Cyber-Komponente könnte deshalb dort immensen Schaden anrichten. So ist dieses Energieprojekt auch gleichzeitig ein IT-Sicherheitsprojekt erster Güte.

Befeuert durch die Energiewende stellt sich in Deutschland nicht zuletzt der Energiesektor täglich neuen Herausforderungen. Neue Wege werden beschritten, sowohl in Sachen Gewinnung als auch bei der Speicherung von Energie. Eine besonders große Herausforderung ist beispielsweise die nachhaltige Verarbeitung von Wärmeenergie. Im Ruhrgebiet liegen zahlreiche alte Zechenanlagen brach, und ihre alten Stollen eignen sich hervorragend als moderne Energiespeicher. Mit Wasser geflutet können sie Wärme speichern, die über den Sommer erzeugt und nicht verbraucht wurde. Steigt der Bedarf der Bevölkerung an Wärmeenergie im Winter, können die regionalen Wärmenetze die Energie direkt aus den Stollen nutzen, so der Plan.

Die überflüssig erzeugte Wärmeenergie stammt dabei sowohl von den Netzbetreibern selbst, als auch von sogenannten Prosumenten. Prosumenten (ein inzwischen etablierter Kunstbegriff aus den Worten Konsumenten und Produzenten) sind sowohl Verbraucher als auch Erzeuger von Energie. Privathäuser, die eine Solaranlage besitzen, decken ihren Eigenbedarf an Energie und speisen die überschüssige Energie in das Netz. Die Verwaltung der Energiebestände erfolgt dabei automatisiert, wobei Endnutzer die volle Einsicht auf den Nutzen ihrer Anlage haben. Gebäude, die eine solche Form der Automatisierung betreiben, werden in der Regel Smart Buildings (intelligente Gebäude) genannt. Der Bedarf an Smart Buildings steigt sowohl im privaten als auch wirtschaftlichen Zweig, und die Zusammenführung solcher Smart Buildings zu einem intelligenten Versorgungsnetz stellt hohe Anforderungen an die IT-Sicherheit.

In intelligenten Netzen kommen cyber-physische Systeme (CPS) zum Einsatz, um spezielle Anlagen zu steuern. CPS sind hochkomplex, bestehen in der Regel aus einer Vielzahl mechanischer Aktoren und Sensoren sowie aus Softwarekomponenten, die mittels IoT-Komponenten (Internet of Things) über Netze, wie dem Internet, miteinander kommunizieren. Das Einspeisen von Fehlinformationen in solche Netze hat durch die physischen Komponenten der cyber-physischen Systeme also stets Auswir-

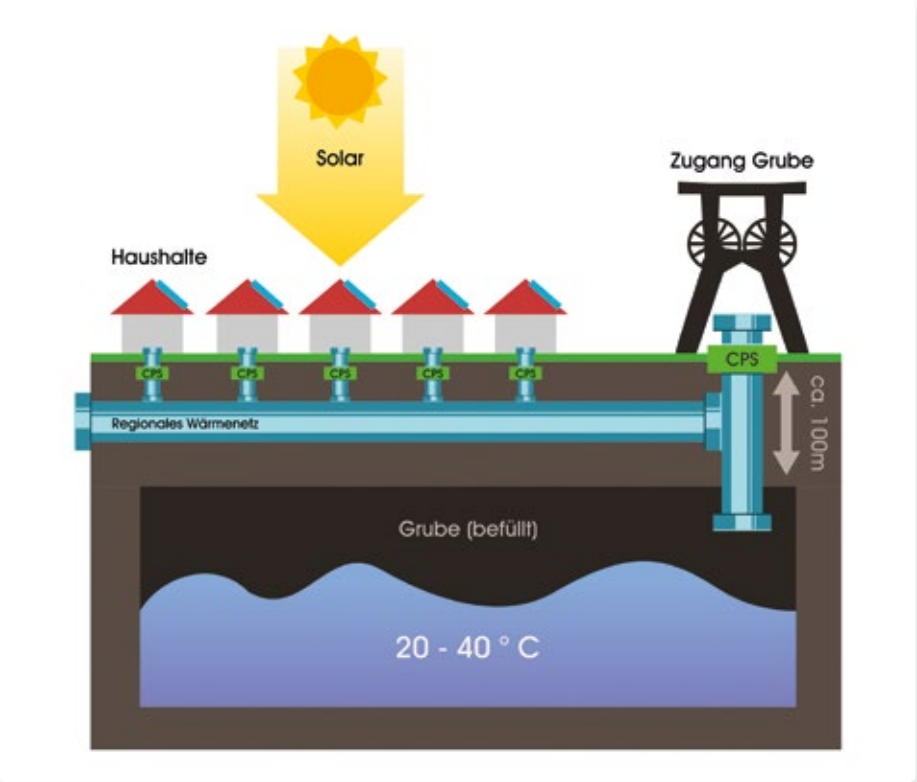

Bild 1: Speichern von solarthermischer Energie in der Grube.

kung auf die reale Welt. Die Absicherung der Kommunikation von CPS sowie die Wahrung der Integrität jedes CPS in einem Netz hat damit oberste Priorität für einen sicheren und vertrauenswürdigen Betrieb.

Cyber-physische Systeme

Cyber-physische Systeme (CPS) sind Mehrkomponentensysteme, die sich durch den Einsatz mechanischer sowie rechnerischer Elemente auszeichnen. In der Regel repräsentieren sie eine Entität aus der realen Welt, vom einzelnen Aktivbauteil bis hin zu ganzen Industrieanlagen. Durch das Vernetzen werden CPS oft im Kontext von IoT-Geräten gebracht. Dies ist im Prinzip richtig, denn CPS, die über unsichere Netzwerke, wie dem Internet, kommunizieren, enthalten tatsächlich Komponenten, die analog zu klassischen IoT-Geräten funktionieren. CPS haben jedoch durch ihre mechanischen Bauteile grundsätzlich immer auch Auswirkungen auf die reale Welt. Der Funktionsumfang eines CPS wird durch Sensorik und Aktorik bestimmt. So können CPS auch auf ihre Umgebung eingehen, indem die Aktorik durch Auswertung der Sensordaten erfolgt. Kommunizieren CPS über das Internet miteinander und sind durch ihre Funktionsbestimmungen voneinander abhängig, können Fehlinformationen eines einzelnen verteilten CPS ungeahnte Auswirkungen auf das Gesamtsystem haben.

CPS finden sich in vielen verschiedenen Einsatzbereichen. So werden CPS in der Energieindustrie, in sogenannten Smart Grids (intelligente Stromnetze) genutzt. Auch in der Logistik, Umwelttechnik, Automobilindustrie und Medizin werden CPS verwendet. Da die Prozesse weitgehend autonom ablaufen, sind CPS eine kosteneffiziente Möglichkeit, die Automatisierung und Digitalisierung voranzutreiben. Der immer größer werdende Wunsch nach Gebäudeautomatisierung verspricht einen lukrativen Markt für CPS sowohl für private Anbieter, als auch für öffentliche Betreiber durch die Verteilung in Haushalten zur Steuerung von Versorgungsnetzen.

Das durch die „ruhrvalley"-Initiative geförderte Projekt „Smart Solar Geothermal Energy Grid Ruhr – GeoSmaGriR" verfolgt das Ziel, die im Ruhrgebiet verfügbaren Wärmenetze durch eine intelligente Energiespeicherung zu erweitern. In diesem Kontext befasst sich das Projekt mit CPS, die in privaten Haushalten eingeführt werden sollen, wobei hier speziell Konzepte für den Einsatz bei Prosumenten erarbeitet werden. So soll solarthermische Energie, die bei der Aufnahme im Sommer überproduziert wird, auf absehbare Zeit im inneren der alten Grubenanlagen bis auf Abruf gespeichert werden (Bild 1). Für diesen Zweck werden eigenständig CPS entwickelt und durch das Institut für Internet-Sicherheit auf ihre sichere und vertrauenswürdige Nutzung in nicht vertrauensvollen Netzen hin untersucht und bewertet. In eigener Herstellung werden durch die beteiligten Projektpartner Smart Device Controller (SDC) entwickelt, CPS, die an die Sicherheitsanforderungen eines modernen CPS angepasst sind.

Für die Koordination eines verteilen SDC-Netzes eignet sich ein Cloud-System, das die Infrastruktur als Ganzes erfasst und Sensordaten der Haushalte empfängt sowie auswertet. Diese autonomen Prozesse verteilen dann im Umkehrschluss Steuerbefehle an die einzelnen SDC, um Aktorenzustände zu ändern.

Grubenspeicher

Im Ruhrgebiet existieren mehr als 200 ehemalige Schachtanlagen, die über entsprechend große wassergefüllte Hohlräume, aufgrund von verbliebenen Schächten und Strecken sowie Restporositäten, in den Abbaubereichen verfügen. Das vorhandene Grubenwasser kann über Produktions- und Injektionsbohrungen erschlossen und als saisonaler Wärmespeicher genutzt werden, wobei das Grubenwasser mit ungestörten Untergrundtemperaturen von etwa 20 °C bis 40 °C im Sommerhalbjahr aufgeheizt wird. Für die ehemalige Zeche Dannenbaum in Bochum kann – bei einer geschätzten effektiv nutzbaren Grubenwassermenge in der Größenordnung von etwa 500.000 Kubikmeter und einer Temperaturdifferenz (ΔT) von 40 °C zwischen Ein- und Ausspeicherung – ein zentraler

Wärmespeicher mit einer Kapazität von 25 GWh/a und einer Leistung von 6 MW betrieben werden. Zeche Dannenbaum ist für das Projekt GeoSmaGriR exemplarisch. In der Gesamtheit aller Schachtanlagen existiert insgesamt ein gewaltiges Potenzial zur Speicherung von Wärmeenergie im Ruhrgebiet.

Mögliche Angriffsszenarien

Sind SDC in kritischer Infrastruktur verbaut, kann ein Eingriff in den geregelten Ablauf der Koordination dieser Geräte ein nicht unerhebliches Fehlverhalten zur Folge haben. Ein Lahmlegen einer oder mehrerer SDC muss dabei nicht immer im Vordergrund der Absicht der Angreifer stehen. Das gezielte Einspeisen von Fehlinformationen in den Kreislauf der Geräte ist ebenso fatal. Die folgenden Beispiele sollen einen Eindruck über die möglichen Konsequenzen eines solchen Eingriffs geben:

Gebäudeüberhitzung

In großen Gebäudeanlagen werden Smart Device Controller (SDC) über Smart Building Manager (SBM) gesteuert. Dazu werden die Sensordaten und die Aktorenzustände aggregiert, bevor sie in das Cloud-System einfließen. Diese Daten werden vom Backend-System verarbeitet und ausgewertet.

Die resultierenden Steueranweisungen an die Aktoren der aggregierten SDC werden anschließend wieder an den SBM weitergeleitet. Findet an dieser Stelle eine Manipulation des Datenverkehrs statt, zum Beispiel durch einen Man-in-the-Middle Angriff, kann der übertragene Befehl durch Angreifer manipuliert und die gesamte Heizungsanlage in einem Gebäude fremdgesteuert werden (Bild 3). Das bedeutet, die Räumlichkeiten werden im Sommer weit überhitzt, im Winter nicht beheizt, was zur kompletten Auskühlung führt. Ein gezielter Angriff könnte hier zum Beispiel die Evakuierung eines Gebäudekomplexes zum Ziel haben, sei es um Diebstahl zu begehen, Anlagen zur Spionage zu installieren oder den Betrieb eines Konkurrenten lahmzulegen.

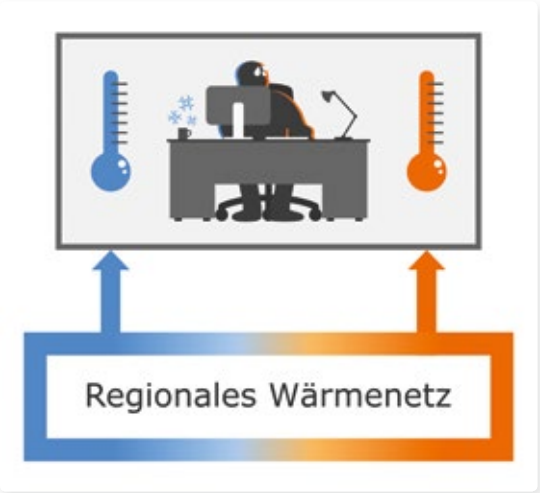

Bild 3: Eine Fremdsteuerung der Heizanlage kann fatale Folgen haben.

Auslesen einzelner SDC

Ähnlich zu Gebäudekomplexen können natürlich auch einzelne SDC betroffen sein.

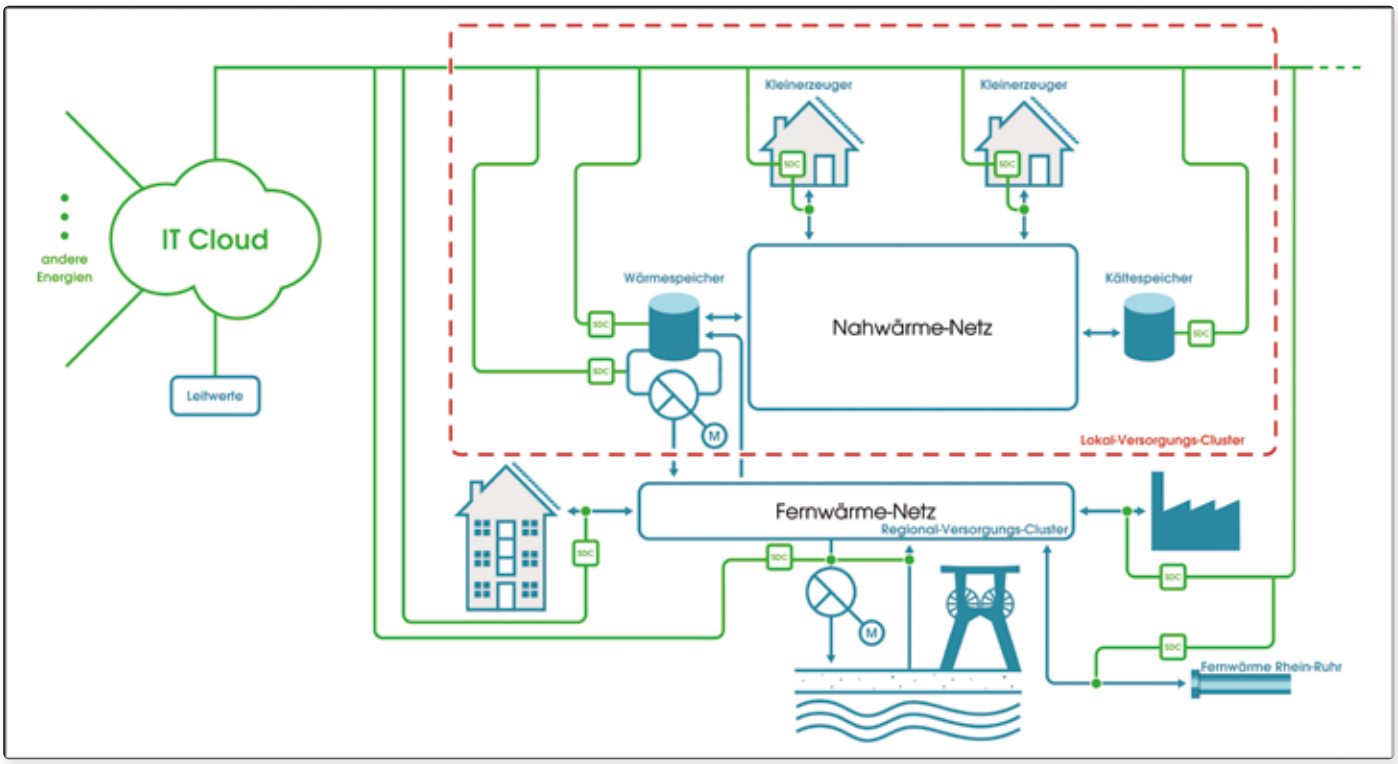

Bild 2: Kreislauf mit Smart Device Controllern und Smart Building Manager.

Sind einzelne Haushalte (Smart Homes) durch eigenständige SDC vertreten, ist nicht nur die Fernsteuerung der Heizanlage möglich – Angreifer sind vielmehr auch in der Lage, die Daten des Geräts direkt auszulesen. Dies fällt kaum auf, da kein Eingriff in die reale Welt stattfindet, jedoch das Heizverhalten eines Einzelnen mitgelesen wird. So lässt sich beispielsweise feststellen, ob aktiv Anforderungen am Heizkörper gestellt werden, die dann wiederrum durch die SDC geregelt sind. Durch Analyse des Heizverhaltens kann ein Angreifer nun Schlüsse für die Auswahl eines potenziellen Opfers ziehen. Wird zum Beispiel keine Aktivität oder Änderung am Heizverhalten im Winter festgestellt, steht dem Einbruch nichts mehr im Wege, denn die Bewohner sind anscheinend nicht zu Hause.

Überhitzung der Grubenanlage

Mit Wasser befüllte Schächte als zukünftigen Energiespeicher zu verwenden, erfordert eine genaue Untersuchung der Umgebung und stellt eine ganz eigene Herausforderung dar. Zur Kontrollflusssteuerung werden in den alten Zechenanlagen ebenfalls SDC installiert, diese kommunizieren über eine Cloud-Anwendung mit den Erzeugern und Verbrauchern. Überschüssige solarthermische Energie wird dem regionalen Wärmenetz im Sommer zugeführt und im Winter wieder abgerufen, die Steuerung dieses Prozesses läuft weitgehend autonom. Werden alte Zechenanlagen mit SDC ausgestattet, müssen besondere Anforderungen an die IT-Sicherheit dieser Steueranlagen gestellt werden. Erhalten etwa Unberechtigte Zugriff auf deren Steuerung, sind Sabotageakte nicht auszuschließen. So ließe sich durch Manipulation des Gruben-SDC die Wassertemperatur in den Schächten ungebremst erhitzen, bis eine kritische Temperatur jenseits 100° C erreicht wird. Ein Überhitzen der alten Schachtanlagen hat ungeahnte Folgen für die Stabilität dieser Stollen und somit für das gesamte Ruhrgebiet. Daher muss die Vertrauenswürdigkeit der SDC oberste Priorität haben.

False Data Injection

In komplexen verteilten Systemen ist es besonders wichtig, die Integrität der übermittelten Daten zu gewährleisten. SDC übermitteln zyklisch ihre Messwerte und erhalten durch ein Backend-System neue Befehle für die Einstellung ihrer Aktoren. False Data Injection (FDI), das gezielte Einspeisen von Fehlinformationen, kann dazu genutzt werden, Angriffe, wie die Manipulation der Heizwerte und Überhitzen der Grubenanlage, durchzuführen. Eine weitere Möglichkeit der FDI ist es, in verteilten Systemen Informationen zu verstecken. Die Information kann dabei im Geheimen durch die Einstellung der Aktoren eines SDC gespeichert werden, um sie später wieder auszulesen und mit Dritten zu kommunizieren. Dass auch eine solche Fehleinspeisung Konsequenzen für das Gesamtsystem hat und somit direkte Auswirkungen in der realen Welt erzeugt, ist alarmierend. Sie ist mit allen Mitteln zu verhindern.

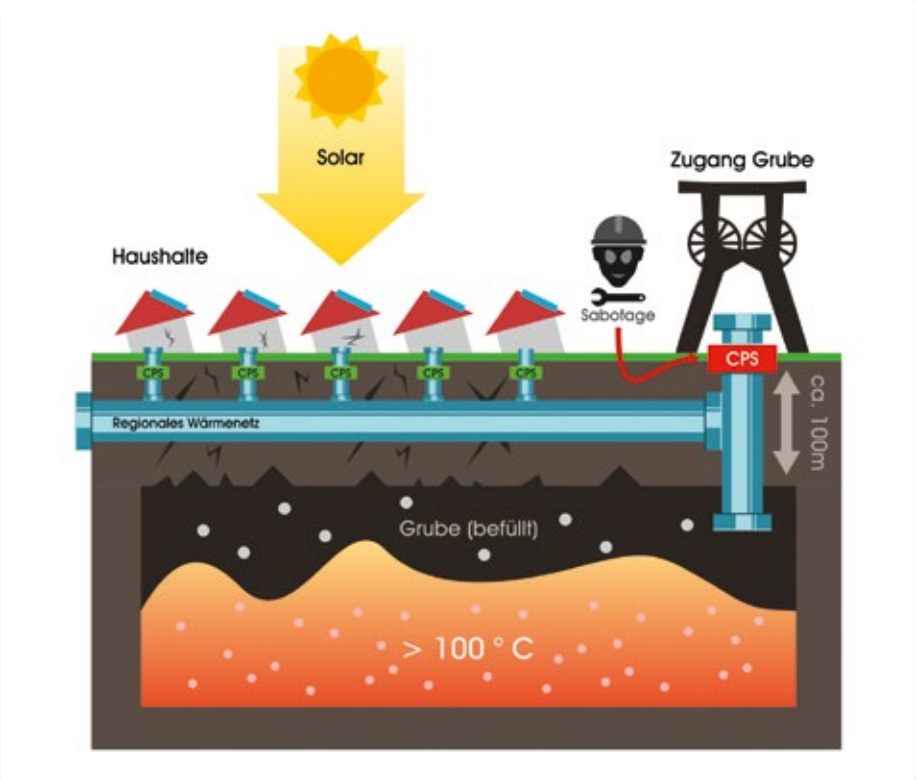

Bild 4: Die Sabotage an einer Grubenanlage zählt zu den schlimmsten Szenarien.

Anforderungen an die IT-Sicherheit

CPS sind wie die speziellen SDC in der Regel Teil einer größeren, verteilten Infrastruktur. Neben der Einsatzumgebung (Temperaturverhältnisse, Feuchtigkeit) sind daher vor allem solche Anforderungen zu berücksichtigen, die in einem verteilten Netz von größerer Bedeutung sind. Auch wenn CPS je nach Konfiguration selbst in der Lage sind, Entscheidungen auf Basis ihrer ermittelten Sensordaten zu treffen, werden sie meist nur teilautonom betrieben. Eine externe Instanz, wie etwa eine Cloud-Anwendung aggregiert die Daten eines, beziehungsweise mehrerer CPS und trifft nach Auswertung Entscheidungen über das Verhalten der Aktoren. Dies ist gerade dann sinnvoll, wenn der Eingriff durch die mechanischen Komponenten in die reale Welt abhängig vom Zustand anderer CPS ist, zum Beispiel ein elektrischer Motor erst angetrieben werden darf, wenn dies an anderer Stelle kein Problem verursacht. Dies stellt CPS generell vor die Anforderung der Verfügbarkeit, Erreichbarkeit und Datenintegrität. Da sich CPS vorwiegend durch ihre Kombination rechnerischer und physischer Bauteile auszeichnen, können bereits bewährte Strategien der IT-Sicherheit Anwendung finden. Dabei gilt ebenso wie

bei komplexen IT-Systemen, dass eine proaktive Sicherheitsstrategie [1] vorzuziehen ist, als im Nachhinein Fehler oder grobe Sicherheitslücken zu korrigieren. Die Auswirkung in der realen Welt durch das CPS ist dann im schlimmsten Fall bereits eingetreten. Es gilt primär, die Gefahr eines „Lying-Endpoints" zu minimieren, einem CPS, das vorgibt, richtig zu arbeiten, obwohl seine Sicherheitsmechanismen bereits umgangen wurden. In diesem Kontext lassen sich die bewährten Trusted-Computing-Funktionen [2] mit bereits erprobten Zugriffsmechanismen, wie Open Authentication 2.0 (OAuth2.0), für die Authentifizierung und Autorisierung der Endgeräte im Cloud System kombinieren.

Integritätssicherung

Eine gut programmierte Software auf dem CPS sorgt für einen reibungslosen Ablauf im Betrieb. Kritische Situationen lassen sich beispielsweise durch das Einprogrammieren fester Grenzwerte und die Implementierung von Fallback-Routinen vermeiden. So ließen sich beim SDC etwa direkt Gegenmaßnahmen einleiten, sobald das Wasser in der Grube eine kritische Temperatur erreichen würde. Das SDC läuft jedoch auch ohne Verbindung zur Cloud teilautonom, das heißt gewisse Steuerroutinen laufen auch ohne direkten Befehl durch die Cloud. Dies ist besonders dann notwendig, wenn eine Verbindung nicht garantiert werden kann, zum Beispiel durch die Umgebung, in der die Systeme operieren. Damit dieser Ablauf ungestört bleibt, muss dem CPS vertraut werden können, das heißt es darf keine Änderung am SDC durch Dritte erfolgt sein. Werden diese Routinen und Grenzwerte jedoch durch eine dritte Partei verändert oder sogar vollständig ausgetauscht, ist es dem Angreifer jetzt möglich, die volle Kontrolle über das Gerät zu erlangen und sogar falsche Daten zur Verschleierung an die Cloud zu senden. So ließe sich ungehindert Wärmeenergie in der Grube speichern, ohne dass Sicherheitsroutinen bei Überschreitung kritischer Temperaturen anlaufen.

Um der Software auf einem CPS vertrauen zu können, empfiehlt sich der Einsatz eines Trusted Platform Modules. Das Trusted Platform Module (TPM) ist ein Chip, der IT-Systeme um Sicherheitsfunktionen ergänzt. Er besitzt einen eigenen Kryptoprozessor, der Zufallszahlen erzeugt, kryptografische Operationen durchführt, geheime Schlüssel sowie Hard- und Softwarekonfigurationen sicher speichert und einiges mehr. Mithilfe des TPM ist es möglich, den Zustand ganzer CPS oder einzelner Softwarekomponenten zu attestieren, da er von der restlichen Hardware des CPS getrennt ist. Mittels Remote Attestation (RMA) ist es dem Cloud-System dann möglich, die Integrität einzelner CPS zu überprüfen. Durch die Nutzung einer Hash-Funktion werden die notwendigen Teile des CPS bis hin zur Abbildung des gesamten Boot-Prozesses in einem Referenzwert gespeichert. Bleibt dieser unverändert, gilt das CPS als vertrauenswürdig. Durch die RMA kann die Cloud die aktuelle Vertrauenswürdigkeit jedes einzelnen CPS messen. Es empfiehlt sich daher, auch im laufenden Betrieb zyklisch Integritätstests durchzuführen.

Life-Cycle-Management

Die Bereitstellung von CPS vor allem an private Haushalte, beziehungsweise unsichere Umgebungen, setzt einen vollständig durchgeplanten Life-Cycle (Lebenszyklus) voraus [3]. Auch der Einsatz von Hardwaresicherheit, wie etwa einem TPM muss berücksichtigt werden. Zusätzlich muss dem Personal vertraut werden können, das ein CPS in seiner vorgesehenen Arbeitsumgebung installiert. Denn verlässt das CPS erst einmal die Fabrik, kann nicht garantiert werden, dass kein Manipulationsversuch stattfindet. Dazu müssen vor allem die kritischen Phasen des Life-Cycles identifiziert werden. Dies sind alle Phasen, in denen das Gerät eine sichere Umgebung (zum Beispiel den Hersteller) verlässt, durch Dritte (zum Beispiel Techniker) bearbeitet wird, die erste Anmeldung an das Cloud-System, die Aufnahme der eigentlichen Arbeitsabläufe sowie die Stilllegung eines CPS. So lassen sich diese Phasen schon ab Fabrik mit einem speziellen Schlüssel ausstatten, der durch das TPM geschützt und vorab in der Cloud hinterlegt wird (Whitelisting). Zur Aktivierung des CPS ist dann etwa ein Geheimnis notwendig, das dem entsprechenden Techniker ausgehändigt wird. Dies erfolgt zum Beispiel in Form eines One-Time-Tokens, das nach der Aktivierung seine Gültigkeit verliert. Erst dann wird die Cloud-Verbindung möglich und ein weiteres Token zum Betrieb des Geräts kann ausgestellt werden. Die Authentifikation und Autorisierung erfolgt im Regelbetrieb per OAuth2.0. Wird der Betrieb des CPS eingestellt, müssen alle verbleibenden Token und Schlüssel wieder vom CPS und aus der Cloud entfernt werden.

Update Mechanismen und Integrität

Wird besondere Hardware, wie ein TPM, zum Schutz eines CPS eingesetzt, gibt es neue Herausforderungen bei der Bereitstellung von Systemupdates [4]. Da das TPM auf Referenzwerte über die Konfiguration der CPS angewiesen ist, muss eine Systemarchitektur geschaffen werden, die dies berücksichtigt, denn die RMA reagiert auf jede kleinste Änderung am System. Das einfache Überschreiben der bestehenden Software ist also nicht mehr möglich. Die Updates werden von der Cloud bereitgestellt und sind signiert, das heißt die CPS erkennen anhand der Signatur, dass es sich um offizielle Updates handelt. Da die hinterlegten Referenzwerte für die Integritätssicherung bei jedem Update ebenfalls erneuert werden müssen, muss der Update-Prozess wie eine Transaktion ablaufen, da sonst nicht-funktionale Zustände entstehen können. Zu diesem Zweck empfiehlt es sich, das komplette Systemimage zu spiegeln und das neue Image erst nach erfolgreichem Update einzuspielen. So ist sichergestellt, dass auch im Fehlerfall ein lauffähiges System bleibt und das Überschreiben der Software ebenso wie die Aktualisierung des Referenzwerts ohne Probleme beendet wurden. Schlägt eine Operation fehl, kann also einfach auf das alte Image zurückgegriffen werden.

Fazit

CPS als Teil der Infrastruktur des Wärmespeicher-Systems fordern ein hohes Maß an IT-Sicherheit, denn die Auswirkungen feh-

lerhafter CPSs können sich katastrophal auswirken. Die Liste an Sicherheitsanforderungen ist enorm, denn CPSs haben immer einen direkten Einfluss auf die reale Welt. Da CPS auf gängigen IT-Systemen beruhen, können bereits bewährte IT-Sicherheitsstrategien dabei helfen, ein möglichst gutes Sicherheitsniveau zu halten und somit vertrauensvolle Infrastrukturen zu schaffen. ■

Quellen:

[1] *D. Bothe, A. Speier, N. Pohlmann: „Proaktive Strategien als Fundament der IT-Sicherheit –Sicherheitsstandards in der Seitenlage?". IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 2/2016*

[2] *A. Speier, N. Pohlmann: „Eine Diskussion über Trusted Computing – Sicherheitsgewinn durch vertrauenswürdige IT-Systeme". IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag,*

[3] *A. Puesche, D. Bothe, S. Sachweh, N. Pohlmann: „Concept of a Life-Cycle Management with Tamper Resistant Distributed Cyber-Physical Systems", eingereicht.*

[4] *A. Puesche, D. Bothe, M. Niemeyer, S. Sachweh, N. Pohlmann, I. Kunold: „Concept of Smart Building Cyber-physical Systems Including Tamper Resistant Endpoints", eingereicht.*

DAVID BOTHE,
wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) der Westfälischen Hochschule Gelsenkirchen und Leiter des Forschungsbereiches „Vertrauenswürdige IT-Systeme"

PROF. DR. NORBERT POHLMANN
ist Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.