Industrielles Identity-and-Access-Management - Konzept für die sichere Gerätevernetzung

06.03.2018 | **Fachartikel, Zutrittskontrolle**

Das Internet-of-Things (IoT) wächst exponentiell. Immer mehr Geräte, Sensoren und Maschinen treten mit einander in Verbindung und legen die Basis für eine Industrie 4.0. Während mittlerweile eine Vielzahl von Lösungen für den Transport und die Verarbeitung der gesammelten Daten auf dem Markt zu finden ist, bereitet das Thema Sicherheit vielen Unternehmenslenkern nach wie vor Kopfzerbrechen. Denn der Weg ins IoT ist verbunden mit neuen Sicherheitsrisiken und potenziellen Bedrohungen, vor denen sich die Betriebe schützen müssen. Im Rahmen des nationalen Referenzprojekts zur IT-Sicherheit in Industrie 4.0 – kurz IUNO – wurde vor diesem Hintergrund ein Konzept für ein industrielles Identity-und-Access-Management (IAM) auf Gerätebene entwickelt. Basierend auf den drei Teilbereichen Authentifizierung, Kommunikationsregeln und Kommunikationsüberwachung garantiert es den sicheren Austausch zwischen Maschinen.

Hochprofessionelle Cyberangriffe sind längst zur Realität deutscher Unternehmen geworden und stehen den Zukunftschancen, welche in der Vernetzung der Produktion schlummern, gegenüber. Eine besonders große Gefahr für die vernetzten Produktionsanlagen geht von neuartigen, auf industrielle Kontrollsystem ausgelegte Attacken einher. Sie zielen darauf ab, Anlagen und Steuerungsmechanismen zu manipulieren bzw. zu sabotieren um wertvolle Daten, Know-how und Betriebsgeheimnisse zu ergaunern.

Dass in diesem Szenario etablierte Sicherheitkonzepte keinen effektiven Schutz gewährleisten, darüber sind sich Experten längst einig. Die Berater der accessec GmbH empfehlen darum die Entwicklung neuer und vor allem auch praxistauglicher Schutzkonzepte und -werkzeuge, welche auf der Identifizierung von Bedrohungen und Risiken für die verschiedenen Szenarien einer intelligenten Fabrik beruhen. Die Erarbeitung möglichst allgemein verwendbarer Lösungen für Herausforderungen der IT-Sicherheit im industriellen Anwendungsfeld hat sich das Forschungsprojekt IUNO1 auf die Fahnen geschrieben. Die entwickelten Lösungen sollen als Blaupausen für die sichere Industrie 4.0 herangezogen werden können.

Auf Basis dieser Anforderungen richtet sich das im Kontext des Projektes entstandene Konzept für ein industrielles IAM auf die Erarbeitung einer Methode zum Erkennen von Bedrohungen und Überwachen von Geräten im Netzwerk. Das Konzept basiert auf den drei Teilbereichen Authentifizierung, Kommunikationsregeln und -überwachung und will helfen, sowohl Fehler im Produktionsnetz als auch Angriffe auf die IT-Sicherheit frühzeitig zu identifizieren und geeignete Maßnahmen einzuleiten.

Welches Gerät darf ins Netz?

Teil eins des Konzepts bildet die Authentifizierung und Verwaltung der Identitätsangaben der IoT-Geräte. Eine zentrale Rolle spielt hierbei der Aufbau einer Public-Key-Infrastruktur (PKI). Dabei ist für den Authentifizierungsprozess vor allem auch die Art der Zertifikatserzeugung sowie die Speicherung auf das Trusted-Platform-Module (TPM) relevant. Der Prozess (Abbildung 1) zum Erstellen eines Zertifikats lässt sich wie folg beschreiben: Im ersten Schritt bedarf es der Erstellung eines Schlüsselpaars - bestehend aus einem privaten und einem öffentlichen Schlüssel. Der öffentliche Schlüssel wird im zweiten Schritt zusammen mit weiteren Informationen wie dem Namen und anderen Parametern des Schlüsselinhabers als so genannter Certificate-Signing-

Request (CSR) an die Zertifizierungsinstanz (engl. Certificate-Authority, CA) geschickt. Aufgabe der CA ist es dann im dritten Schritt die Überprüfung Richtigkeit der übermittelten Angaben durch geeignete Maßnahmen. Die CA bestätigt nun dem CSR diese Information mit ihrer Signatur und schickt diese als fertiges Zertifikat (X.509) zurück zum Antrag stellenden Gerät. Das Ergebnis: Das Gerät enthält ein verschlüsseltes Zertifikat, das nun zur sicheren Authentifizierung sowie Kommunikation mit anderen Geräten zur Verfügung steht.

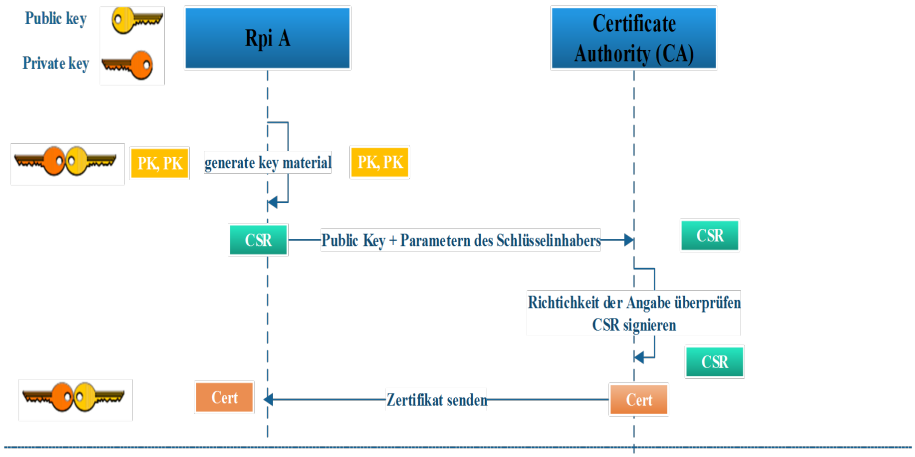

Abbildung 1: Architektur der Certificate Signing Request (CSR)

Technisch wird die Zugangskontrolle durch die Einrichtung zweier logischer Ausgänge eines Ports ermöglicht - jeweils einen zum Authentifizierungsserver und zum lokalen Netz. Dabei ist standardmäßig zunächst ausschließlich der Ausgang zum Authentifizierungsserver freigeschaltet. Dadurch ist ein Nachrichtenaustausch nur hiermit möglich. Die Freischaltung des Ausgangs des Switch-Ports zum lokalen Netz erfolgt erst nach der erfolgreichen Authentifizierung des Geräts. Während der Port-Nutzung kann der Authentifizierungsserver jedoch jederzeit zu einer erneuten Authentifizierung auffordern, welche im Falle eines Scheitern zur Deaktivierung des Ausgangs zum lokalen Netz führt. Eine Deaktivierung erfolgt auch bei jeder Entfernung des Kabelsteckers um den Missbrauch eines authentifizierten und freigeschalteten Ports zu verhindern.

Ein weiteres Verfahren umfasst die Erstellung einer Signatur anhand eines asymmetrischen Schlüssels. Liegt hierbei bereits eine Zertifizierung der CA vor, so ist zusätzlich die Authentizität des Geräts gesichert. Zudem findet auch zwischen den Geräten eine bidirektionale Authentifizierung statt.

Wer darf mit wem welche Daten austauschen?

Das Aufstellen von Kommunikationsregeln zwischen den Geräten sowie deren Überwachung bildet den zweiten und dritten Bereich des Konzepts. Dabei gilt die Grundregel: Autorisierten Geräten ist der Austausch von Daten gestattet. Darüber hinaus ist im IAM-System die Definition individueller Regeln möglich um stets nachvollziehen zu können WER kommuniziert, WIE die Kommunikationsparteien authentisiert werden, WER mit WEM kommunizieren darf und auf WAS zugegriffen werden darf.

Für die Integration des IAM-Systems und eine einfache Gestaltung der Kommunikation ist der Einsatz des Protokolls für die Machine-to-Machine-Kommunikation Open Platform Communication Unified Architecture (OPC UA) vorgesehen. Hierfür muss jedes Gerät über einen OPC-konformen Treiber verfügen, welcher sich ohne großen Anpassungsaufwand in beliebig große Steuerungs- und Überwachungssysteme integrieren lässt. (vgl. Abbildung 2) OPC UA eignet sich zudem auch für die Verwendung von Echtzeitdaten bzw. -überwachung sowie für Datenarchivierung und Alarm-Meldungen. Eine zusätzliche Erhöhung der Sicherheitsstufe wird durch die Einbindung eines Security-Information-and-Event-Management (SIEM)-Systems als Überwachungsinstanz erreicht. So alarmiert es den Leitstand im Falle einer Unregelmäßigkeit, etwa wenn sich ein unbekanntes oder unerwünschtes Gerät im Netz befindet.

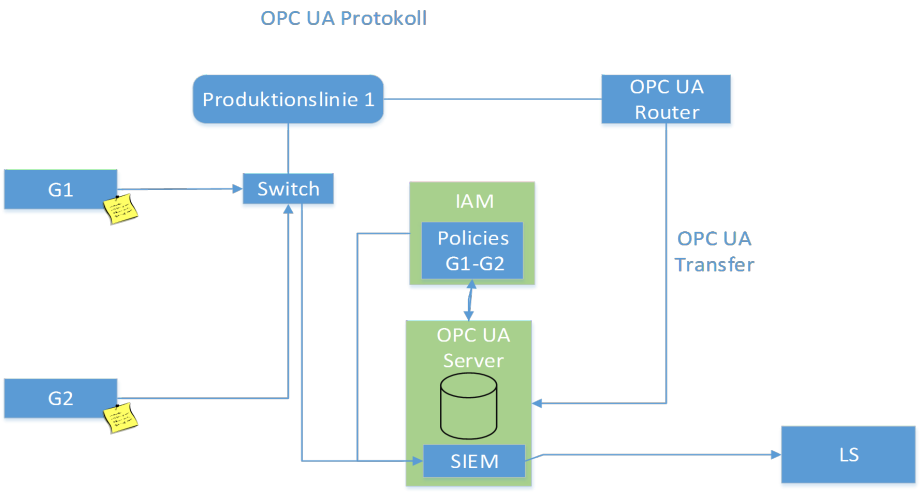

Abbildung 2: Architektur zur sichere Kommunikation auf Gerätebene

Sichere Kommunikation auf Geräteebene

Das Internet-der-Dinge, welches Maschinen, Sensoren und Netzwerke miteinander verbindet, bildet den Grundstein für Industrie 4.0. Unternehmen, die von den neuen Chancen profitieren wollen, stehen vor allem auch vor der Herausforderungen, ihre Produktion – ihre Maschinen und Daten – vor neuen Bedrohungsszenarien zu schützen. Das entwickelte Konzept zeigt: Ein industrielles Identity-and-Access-Management auf Gerätebene ist nicht nur möglich, sondern notwendig. Auf Basis von Zertifikaten kann der sichere Austausch von Geräten im Netzwerk gelingen und da-mit der Aufbau eines von Angriffen geschützten Industrie-4.0-Systems. Nicht zuletzt mit dem Auf-bau auf einem zukunftsorientierten Architekturdesign beantwortet das Konzept sämtliche wissenschaftliche Fragen an die sichere Vernetzung von Maschinen. Lediglich die Umsetzung bzw. Optimierung des konkreten Einsatzes des OPC UA-Protokolls für den Transfer der Produktionsdaten zwischen Komponenten im Netzwerk steht noch aus.

Autor: Caleb Ketcha, Security Engineer, accessec GmbH

Weitere Informationen: **https://www.iuno-projekt.de/ueber-iuno**

Autor: Caleb Ketcha