

# Drahtlos automatisieren und die Informationssicherheit unter Kontrolle haben

VON SVILEN IVANOV, MARTIN GERGELEIT UND RALF SCHUMANN

Die Anwendung drahtloser Steuerungen eröffnet neue Möglichkeiten für die intelligente Produktion und schafft gleichzeitig neue Risiken für die Informationssicherheit. Durch ein strukturiertes Vorgehen kann ein angemessener Schutz bei optimalem Mitteleinsatz erreicht werden.



FOTO: MARCUS WALTER/PIXELIO

Durch planvoll erstellte Sicherheitsrichtlinien kann ein angemessener Schutz auch für den Notfall erreicht werden. Dabei können einfache technische Lösungen genutzt werden, wie das Beispiel der fahrerlosen Transportsysteme zeigt.

In der Regel steht die drahtlose Kommunikation innerhalb einer Anwendung nicht im Mittelpunkt der Betrachtung, sondern wird oft als integraler Bestandteil einer Anlage mit beschafft. Dabei liefern verschiedene Hersteller unterschiedliche Security-Lösungen.

Darüber hinaus führen die längeren Lebenszyklen von Anlagen in der Automatisierung dazu, dass auch technisch nicht mehr aktuelle Drahtlos-Lösungen angeboten werden oder im Betrieb bleiben. Dies alles kann zu sehr heterogenen Security-Lösungen und bezüglich des tatsächlichen Schutzbedarfs unangemessenen Maßnahmen führen. Mitunter werden damit ver-

steckte Betriebskosten für die Informationssicherheit verursacht.

## Die Wireless Security Policy als Grundlage

Um angemessen und kosteneffizient handeln zu können, bedarf es einer Sicherheitsrichtlinie für die drahtlose Kommunikation. Eine „Wireless Security Policy“ definiert klare Regeln sowie die dazu gehörigen Rollen und Verantwortungen im Unternehmen. Damit sorgt die Umsetzung der Richtlinie für einen nachvollziehbaren, angemessenen Stand der Informationssicherheit und für mehr Klarheit über den Betriebsaufwand und die Kosten der Gesamtlösung.

Eine wesentliche Voraussetzung für eine „Wireless Security Policy“ ist die Durchführung einer Risikoanalyse. Die Risikoanalyse umfasst im Wesentlichen:

- die Definition von Informationswerten mit Schutzzielen,
- die Ableitung von Bedrohungen, Schadensausmaß, Risiken
- die Auswahl von Sicherheitsmaßnahmen, um bestimmte Risiken zu minimieren.

Die Informationswerte sind die zu schützende Daten des Unternehmens, zum Beispiel die Steuerungsdaten, die drahtlos übertragen werden. Die Schutzziele beschreiben die Anforderungen des Unternehmens bezüglich des Schutzes der Infor-

mationswerte. Für die Steuerungsdaten sind die Schutzziele meist Verfügbarkeit und Integrität – das heißt, sie müssen zuverlässig ankommen und dürfen auf dem Weg nicht verändert werden (unbeabsichtigt oder bewusst).

In den meisten Unternehmen sind bereits Schutzmaßnahmen vorhanden. Sie müssen den Informationswerten und Schutzziele gegenübergestellt werden, um mögliche Bedrohungen mit dem Schadensausmaß zu identifizieren. Auf dieser Basis kann eine Risikobewertung durchgeführt werden.

Eine quantitative Risikobewertung erfordert die finanzielle Bewertung erwarteter Schäden sowie die Festlegung von Eintrittswahrscheinlichkeiten. Analog müssen auch die Auswirkungen möglicher Maßnahmen bewertet werden. In der Praxis ist eine solche quantitative Analyse oft nicht durchführbar oder zu aufwendig. Dagegen ist eine qualitative Bewertung der Risiken auf Basis von grob geschätzten Eintrittswahrscheinlichkeiten und Schadensausmaß meist realistischer und weniger aufwendig, aber dennoch hinreichend, um dringenden Handlungsbedarf aufzuzeigen, geeignete und effiziente Sicherheitsmaßnahmen zu identifizieren und den optimierten Einsatz des Sicherheitsbudgets zu unterstützen.

Die durch die Risikoanalyse vorgegebenen Maßnahmen werden in der „Wireless Security Policy“ festgehalten. Die Richtlinie ist in der Praxis meist eine Erweiterung bestehender Sicherheitsrichtlinien beispielsweise für Zugangskontrolle, physische Sicherheit, personelle Sicherheit. Für jede

Maßnahme sind folgende Vorgaben sinnvoll: Maßnahmenbeschreibung, zu schützende Informationswerte, Schutzziele, Vorgaben zu Maßnahmenumsetzung, Verantwortlicher, Vorgaben zu Maßnahmenprüfung.

### Ein beispielhaftes Vorgehen

Die Umsetzung der Vorgehensweise wird anhand eines Beispiels deutlich. Als Anwendung wird ein autonomes Transportsystem betrachtet, das Produktionsgüter vom Wareneingang auf die Produktionslinie transportiert. Das System besteht aus fünf autonomen Transporteinheiten, die Fahraufträge vom MES-System über WLAN erhalten. Der erlaubte Stillstand des Transportsystems beträgt maximal zwei Stunden – so lange reichen die zwischengelagerten Produktionsgüter aus.

In dieser Beispiel-Risikoanalyse wird der Informationswert „Fahraufträge“ mit den Schutzziele „Verfügbarkeit“ und „Integrität“ betrachtet. Als Bedrohung sei ein Angreifer angenommen, der sich Zugang zu dem WLAN-Netzwerk verschafft und mit ungültigen Fahraufträgen das System stört. Das Schadensausmaß ist Stillstand des Transportsystems und nach zwei Stunden Stillstand der Produktion.

Eine geeignete Schutzmaßnahme ist eine Zugangskontrolle des WLAN mit Authentifizierungs- und Verschlüsselungsverfahren. Die WLAN-Best-Practices empfehlen zwar die Verwendung einer zentralen Schlüsselverwaltung statt eines gemeinsamen Passworts. Allerdings gibt es in dem betrachteten Fall keine verfügbaren Ressourcen und kein Know-how, um einen zentralen Authentifizierungsserver zu betreiben. Deswegen wird in diesem Beispiel als Maßnahme eine Authentifizierung und Verschlüsselung mit einem gemeinsamen WLAN-Passwort vorgeschlagen, allerdings mit zusätzlichen spezifischen Regeln um die Nachteile einer solchen Lösung zu minimieren.

Die drahtlose Sicherheitsrichtlinie umfasst:

- Die WLAN-Authentifizierung und Verschlüsselung erfolgt auf Basis von WPA oder WPA2 unter Verwendung eines gemeinsamen WLAN-Passworts.
- Das Passwort muss mindestens 40 Zeichen lang sein und drei verschiedene Buchstabengruppen enthalten.
- Das Passwort wird durch eine Person bestimmt.
- Das Passwort wird an einem physisch geschützten Ort aufbewahrt.

#### INFORMATIONEN



## EU-Forschungsprojekt flexWARE

rt-solutions.de ist an dem EU-Forschungsprojekt flexWARE (Flexible drahtlose Automatisierung in Echtzeitumgebungen) beteiligt. Ziel des Projekts ist es, die Implementierung einer Plattform für Echtzeitkommunikation auf Basis des WLAN-Standards mit Aspekten der Verfügbarkeit, Sicherheit und Flexibilität zu kombinieren. Eines der angestrebten Ziele im Bereich der Informationssicherheit ist die Erstellung einer Vorlage für die Abbildung von Informationswerten, Bedrohungen und Risiken auf Maßnahmen speziell für die drahtlose Automatisierung. Damit lassen sich dann in der Zukunft Risikoanalysen leichter auch vom Endanwender durchführen.

[www.flexware.at](http://www.flexware.at)

- Der Zugang zum Passwort wird durch eine obere Instanz genehmigt und protokolliert.
- Kopien des Passworts dürfen nicht gemacht werden.

Für den Notfall „gestohlener Access Point“ (und damit gestohlenen Passwort) gibt es einen Wiederherstellungsplan.

Dieses Beispiel zeigt, dass durch planvoll erstellte Sicherheitsrichtlinien ein angemessener Schutz erreicht werden kann, ohne dabei zwingend die Nutzung der aufwendigsten technischen Lösung zu fordern.

### Kosteneffizienz durch planvolles Handeln

Auf Basis einer „Wireless Security Policy“ können der Betriebsaufwand und die Kosten für den laufenden Betrieb besser geschätzt werden. Damit lässt sich der Nutzen von drahtlosen Steuerungen besser abwägen. Wenn die Risikoanalyse gründlich durchgeführt ist, haben die Investitionen für Informationssicherheit einen erkennbaren Gewinn. ●

Svilen Ivanov  
Leiter Industrielle Kommunikation  
rt-solutions.de GmbH  
Tel.: +49 221 9372437  
[ivanov@rt-solutions.de](mailto:ivanov@rt-solutions.de)

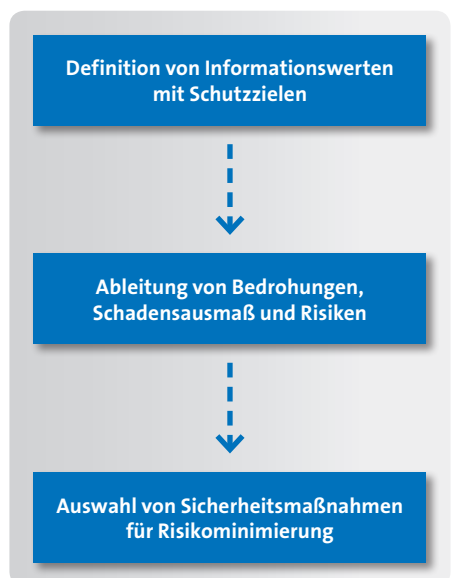


BILD: RT-SOLUTIONS.DE

Die Risikoanalyse ist wichtig, um einen angemessenen Schutz der Informationswerte zu erreichen.