PROTECTOR

12|2022
Dezember
50. Jahrgang

ASW Bundesverband –
Allianz für Sicherheit in der Wirtschaft e.V.

schlütersche
www.sicherheit.info

Ehrgeizig

Wie Milestone Systems zum globalen Marktführer werden will | **8**

Sparsam

Wie sich mit Zutrittskontrolle effizient Energie einsparen lässt | **24**

Hilfsbereit

Wie Kritis-Unternehmen in der Krisenvorsorge unterstützt werden | **50**

Gut geplant ist halb gewonnen!

Wie Standards Healthcare-Einrichtungen effizienter und sicherer machen | **12**

Foto: Getty Images/Fuse

Foto: Legic

Das Legic XDK Secure Sensor Development Evaluation Kit stellt gewissermaßen das „Schweizer Taschenmesser der IIoT-Lösungen" dar.

Vertrauensvoll vernetzt

Wie man mit dem Ansatz „Security-by-Design" Vertrauen in das industrielle IoT bilden kann und muss.

ANTHONY FITZE & CARL FENGER

In industriellen Umgebungen führen unzählige implementierte Sensoren und die sichere Erfassung und Verarbeitung von Daten von festen und mobilen Anlagen zu Effizienzsteigerungen und besseren geschäftlichen Entscheidungen. Damit wird vieles leichter: die Optimierung von Prozessen, Verringerung von Fehlern, Unterstützung von Audits und Durchsetzung von Qualitätskontrollen.

Sensoren einfach mit dem Internet zu verbinden, reicht nicht aus. Die Funktionsfähigkeit der durch das „industrielle Internet der Dinge" verbesserten Prozesse hängt von einem gemeinsamen Nenner ab: Vertrauen. Wenn den Daten, Sensoren und den Menschen, die auf sie zugreifen, nicht vertraut werden kann, verlieren IIoT-Implementierungen ihre Wirksamkeit. Ohne Vertrauen in Benutzer, Sensoren und ihre Interaktionen, können die Ergebnisse kostspielig und sogar katastrophal sein.

Drei Säulen des Vertrauens im IIoT

Das Vertrauen in IIoT-Daten beruht auf der Verbindung verifizierter Nutzer mit vertrauenswürdigen Sensoren/Objekten, damit ihre Interaktionen zuverlässig, transparent und nachvollziehbar sind. Die Verwirklichung dieses Ziels beruht auf drei Grundsätzen:

1. Verantwortlichkeit: Benutzer müssen identifizierbar und zur Verantwortung zu ziehen sein, bevor sie Zugang zu Sensoren oder Infrastrukturen erhalten. Das heißt alle Aktionen müssen jederzeit nachvollziehbar sein. Die Zugriffsberechtigungen müssen zugewiesen werden auf Grundlage von Rolle, Ausbildung und Berechtigungen sowie kontextbezogener Kriterien wie Zeit, Standort, Umgebungsdaten. Berechtigungen müssen autonom durchgesetzt werden, online wie offline, um menschliche Fehler zu minimieren und den Betrieb rund um die Uhr zu unterstützen. Alle Aktivitäten müssen transparent, nachvollziehbar und überprüfbar sein.
2. Sicherheit: Die Konfiguration von und der Zugang zu Geräten darf nur durch befugte Benutzer erfolgen. Die Geräte müssen gegen Spoofing resistent sein. Sensoren sind die anfälligsten Komponenten eines IIoT-Systems. Daher muss die Sicherheit auf physischer Hardware-Ebene in Form eines integrierten Secure Elements für das Hosting von Verschlüsselungscodes und Benutzerberechtigungen implementiert werden.
3. Transparenz: Interaktionen zwischen Nutzern und Sensoren und die von ihnen erzeugten Daten müssen vertrauenswürdig und für validierte Nutzer transparent sein. Sie dürfen weder am Sensor noch in LANs, über Luftschnittstellen oder über das Netz, einschließlich des öffentlich zugänglichen Internets, für Unbefugte sichtbar, manipulierbar oder abfangbar sein.

Säule 1: Verantwortlichkeit

Um Verantwortlichkeit zu schaffen, müssen alle Nutzer eines IIoT-Systems verifiziert werden. Die Zugriffsrechte auf physische Bereiche, Maschinen, Funktionen, Fahrzeuge und Informationen müssen auf der Basis der Credentials der vertrauenswürdigen Benutzer erteilt werden. Credentials legen fest, wo

und wann sich Benutzer aufhalten dürfen, welche Maschinen und deren Funktionen je nach Ausbildung und Funktion genutzt werden dürfen, welche Lagerbehälter sie öffnen dürfen und so weiter.

Benutzer wechseln regelmäßig – täglich kommen und gehen Mitarbeitende, wechseln die Funktion oder absolvieren Trainings. Externe Auditoren oder Auftragnehmer benötigen zeitlich befristete Ad-hoc-Credentials. Berechtigungen müssen in Echtzeit und Over-the-Air erstellt und neu konfiguriert werden können. Das System muss im Online- wie im Offline-Modus funktionieren, da Netzwerkverbindungen nicht immer verfügbar oder zuverlässig sind.

Zu den wichtigen Anforderungen gehören Echtzeitaktualisierung von Credentials sowie das Hinzufügen und Entfernen von Mitarbeitenden per Knopfdruck. All dies kann durch eine mobile App etwa auf IOS-/Android-Smartphones oder -Tablets unterstützt werden.

Säule 2: Sicherheit

Vertrauenswürdige Daten stammen nur von vertrauenswürdigen Sensoren. Da bei IIoT-Implementierungen Tausende von Sensoren großflächig verteilt sind, müssen Implementierung, Konfiguration, Verwaltung und Auslesen einfach, schnell und kostengünstig sein. Ein einfaches Upgrade von Sensoren ist ebenfalls wichtig für die schnelle Nachrüstung von bestehenden Industrieanlagen. Der Aufbau eines vertrauenswürdigen Sensornetzwerks hängt von folgenden Attributen ab:

- Alle Sensordaten müssen geschützt werden durch die höchste kommerziell verfügbare Verschlüsselungsstufe wie AES (Advanced Encryption Standard).
- Die Verschlüsselungscodes müssen bei der Initialisierung unsichtbar und im Betrieb unzugänglich sein. Schlüssel und andere sensible Daten müssen in einem physisch und elektronisch unzugänglichen, in den Sensor integrierten Secure Element gespeichert werden. Während der Initialisierung des Sensors dürfen die Schlüssel weder im Speicher noch bei der Übermittlung für Menschen lesbar sein.
- Sensor Spoofing muss unmöglich sein (zum Beispiel durch böswilliges Ersetzen eines Sensors durch einen manipulierten Sensor). Ein einzigartiger, unsichtbarer Verschlüsselungscode, der in ein Secure Element im Sensor integriert ist, verhindert dies: Ohne Schlüssel reagieren Sensoren nicht.
- Drahtloser Zugang ist unerlässlich. Da Sensoren oft in schwer zugänglichen Bereichen installiert sind, ist eine verschlüsselte Wireless-Kommunikation über RFID, Bluetooth Low Energy oder NFC per Smartphone erforderlich.
- Firmware-Update Over-the-Air ist unerlässlich. Konfiguration und Aktualisierung der Sensoren vor Ort müssen möglich sein. Werksseitige Programmierung ist zu vermeiden, damit Implementierungs- und Logistikkosten niedrig bleiben. Da keine Fremdhersteller beteiligt sind, erhöht dies die Sicherheit.
- Sensoren und der Zugang zu ihnen müssen online wie offline funktionieren. Das System muss auch ohne Netzwerkverbindung funktionieren, um unterbrechungsfreien Betrieb sicherzustellen.
- Sensoren müssen modular, serienmäßig zu produzieren und vor Ort konfigurierbar sein. Dadurch werden die Lieferketten für Sensoren rationalisiert und die Manipulationsmöglichkeiten während der Herstellung minimiert. Es ermöglicht auch einfachere angepasste Konfigurationen vor Ort, während der Administrator der IIoT-Implementierung unabhängig von den Sensorlieferanten agieren kann.

Säule 3: Transparenz

Wenn das Vertrauen in die Benutzer und die Sicherheit der Sensoren hergestellt ist, wird Transparenz erreicht, da verifizierte Benutzer sicher Daten von vertrauenswürdigen Geräten über ein verschlüsseltes Netzwerk zur Verarbeitung durch ein Managementsystem sammeln oder verwalten. IIoT-Implementierungen bestehen aus Sensoren, die großflächig verteilt oder in mobilen Containern installiert sind, welche sich irgendwo befinden können. So ist entscheidend, dass den Daten vertraut werden kann, während sie Wireless-, Mobilfunk- und Internetverbindungen durchlaufen.

Da kein Netzwerk zu 100 Prozent gegen das Abfangen von Daten geschützt werden kann, muss eine End-to-End-Verschlüsselung eingesetzt werden. Die verwaltete AES-Verschlüsselung ist das leistungsfähigste, kommerziell erhältliche Verschlüsselungsprotokoll. Bei ihr ist Hacken zwecklos, selbst bei Netzwerken, die für das Abfangen von Daten anfällig sind. Die Nutzdaten in jedem Datenpaket können nämlich ohne den Verschlüsselungscode nicht gelesen werden. Die Schlüssel sind weder bei der Übermittlung noch im Speicher sichtbar.

Sicherer Gatekeeper am IIoT-Edge

Mit einer sicheren End-to-End-IIoT-Plattform, die auf Mobile Credentialing-, Managed Encryption- und Secure Element-Technologien basiert, lassen sich Verantwortlichkeit, Sicherheit und Transparenz erreichen. Dynamisch aktualisierbare Benutzer-Credentials in Kombination mit standort- und anderen kontextbezogenen Informationen wie Sensordaten machen Aufgaben einfacher, effizienter und sicherer und verbessern gleichzeitig die Prozessqualität, Integrität, Verantwortlichkeit und den Komfort. Im Folgenden einige spezifische Anwendungsfälle:

- Automatisierung der Logistik: Eine vertrauenswürdige IIoT-Plattform ermöglicht einen sicheren, transparenten Warenverkehr sowohl innerhalb von als auch zwischen Standorten.
- Building Management: Die Verknüpfung von Personen mit einer verifizierten Identität ermöglicht eine vertrauenswürdige Überwachung von Gebäudeanlagen und Interaktionen zwischen Nutzern und Systemen.
- Industrieanlagen: Die Verknüpfung von Personen mit einer verifizierten Identität, gefolgt von einer dynamischen Erteilung von Berechtigungen und dem Zugang zu Geräten, sorgt für vertrauenswürdige Interaktionen und Verantwortlichkeit.

Die Legic IIoT Sicherheitsplattform kann in jede Anwendung und Infrastruktur integriert werden. Die sichere, verwaltete Kryptografie in Kombination mit Secure Element-Technologie, mobilem Credentialing und Bluetooth-, NFC-, WLAN- oder RFID-Kommunikation dürfte zu den sichersten IIoT-Lösungen mit bester Verantwortlichkeit für lebenswichtige und geschäftskritische Systeme zählen. ■

Legic Identsystems AG:
www.legic.com