Fraunhofer
IIS

FRAUNHOFER-INSTITUT FÜR INTEGRIERTE SCHALTUNGEN IIS

CYBERSICHERHEIT FÜR DAS IoT

Sicherheitslücken identifizieren und anwendungsspezifische Maßnahmen treffen

Fraunhofer-Institut für Integrierte Schaltungen IIS

Institusleitung
Prof. Dr.-Ing. Albert Heuberger
(geschäftsführend)
Dr.-Ing. Bernhard Grill

Am Wolfsmantel 33
91058 Erlangen

Kontakt:
Moritz Loske
Nordostpark 84
90411 Nürnberg
Telefon: +49 911 58061-9335
cybersicherheit@iis.fraunhofer.de

www.iis.fraunhofer.de/sicherheit

Neue Herausforderungen im IoT

Im Internet of Things kommt es zu einer Verschmelzung der realen mit der digitalen Welt. Dadurch verschwindet der bisherige, verlässliche Schutzwall zwischen diesen Welten immer mehr, sodass Cyberangriffe reale Auswirkungen im Alltags- oder Berufsleben haben können.

Aufgrund der Rahmenbedingung eingeschränkter Ressourcen in cyberphysischen Systemen im Internet of Things oder in Sensornetzwerken lassen sich herkömmliche Sicherheitsmechanismen wie Firewalls, Intrusion Detection Systems oder auch AntiViren Software oft nicht anwenden.

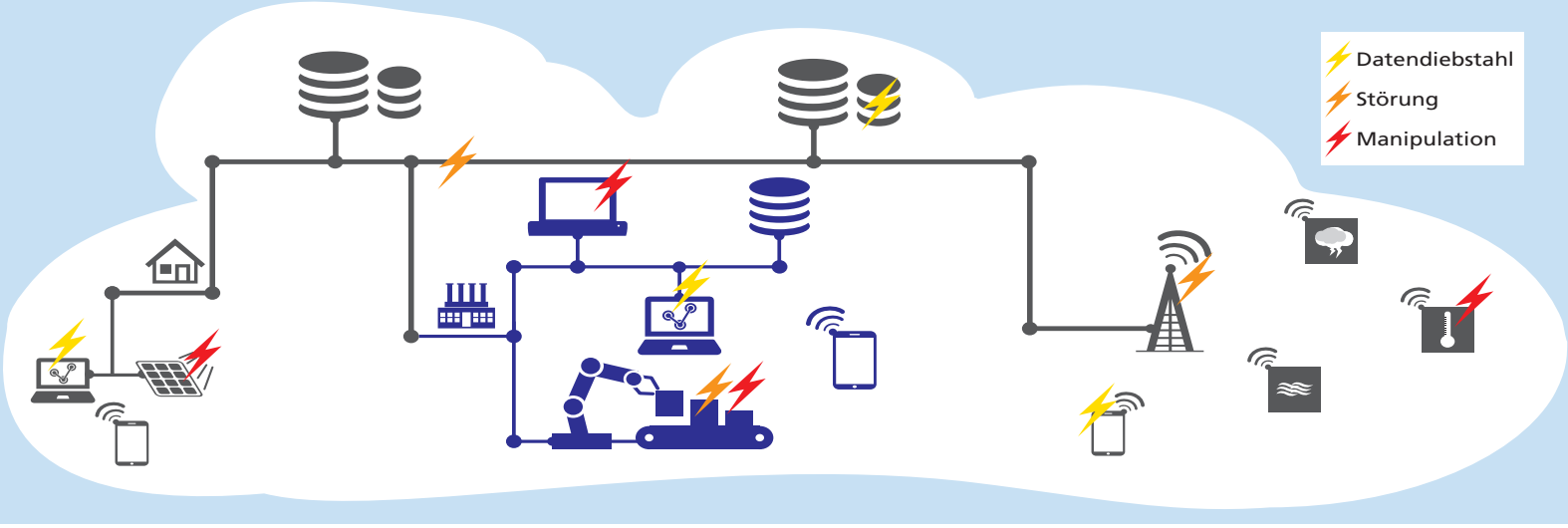
In den letzten Jahren wurde nahezu jedes dritte Unternehmen in Deutschland über digitale Wege angegriffen. Die zunehmende Vernetzung von Maschinen und Geräten mit den IKT-Systemen erhöht die Angriffsmöglichkeiten auf Unternehmen.

Cybergefahren bei Condition Monitoring

Condition Monitoring ist ein Verfahren zur Zustandsüberwachung, das in der digitalen Automation eingesetzt wird und mit dem der Zustand der Produktionsmittel permanent überwacht und analysiert wird.

Dadurch erhält man nicht nur einen Mehrwert in den Prozessabläufen und längere Maschinenlaufzeiten, sondern auch viele neue Einfallstore für ungebetene Gäste über die neuen Sensornetze und Cloudanbindungen.

Über diese externen Zugänge zu den Maschinen entstehen gefährliche Einfallstore, durch die Daten unerwünscht nach außen dringen oder schädliche Daten in das Unternehmen gelangen können. Jeden Sensor einzeln vor möglichen Cyberangriffen zu schützen, kostet Geld, Energie und Datenrate.



Sicher vernetzt im Industrial IoT

Aber es gibt Möglichkeiten, sich und sein Netzwerk effektiv zu schützen. Die Schutzmaßnahmen fangen bereits bei der Installation an. Jedes angeschlossene Gerät muss als mögliches Einfallstor für das gesamte System gesehen werden. Die übergreifende Vernetzung von Einzelgeräten, welche innerhalb eines digitalisierten Betriebs vorhanden sind, sorgt dafür, dass das gesamte Netzwerk lediglich so robust wie das am schwächsten gesicherte Gerät ist.

Natürlich benötigt auch das Komplettsystem ausreichende Sicherheitsmechanismen wie Firewall, Zugriffsrechte und Verschlüsselung. Gerade im Zuge der Vernetzung zahlreicher Systeme, sollten regelmäßige Updates aller relevanten Einzelgeräte zur Gewohnheit werden. Auch hier sollte man auf die Authentizität der Updates achten.

Anwendungsbasierte Cybersicherheit von Condition Monitoring

Besonders bei Anlagen und Maschinen, die zur Zustandsüberwachung per Fernzugriff vernetzt sind, bestehen hohe Sicherheitsrisiken. So entsteht eine Vielfalt von Gefährdungsmöglichkeiten, wodurch sensible Daten ausgespäht bzw. gezielt betrügerische Informationen in den Datenverkehr eingeschleust werden können. Dabei ist zwischen Schutz von Daten gegenüber Manipulation, einem Störangriff und gegen Diebstahl zu unterscheiden.

Aus diesem Grund bietet das Fraunhofer IIS anwendungsbasierte Cybersicherheitsmaßnahmen an. Wir beschäftigen uns mit verschiedensten Sicherheitsmaßnahmen, analysieren Ihr System hinsichtlich potenzieller Gefahren und erarbeiten optimale und kostengünstige Lösung zum Schutz ihrer Daten. Der Fokus liegt hierbei auf der Erarbeitung von Lösungen, die dem Bedrohungspotenzial und dem möglichen Schaden Rechnung tragen.

Einen Schutz gegen Datenmanipulation erhält man z. B. durch den Einsatz kryptographischer Signaturverfahren oder Hashfunktionen. Aber auch der Einsatz eines Blockchainverfahrens kann einen zusätzlichen Schutz bieten. Die gezielte und situationsgerechte Anwendung von kryptographischen Verfahren auf die Übertragung kritischer Zustandsdaten kann böswillige Eingriffe von außen wesentlich erschweren bzw. verhindern.

Unsere Forschungsthemen

- Sichere Vernetzung von Systemen
- Anwendungsorientierte Sicherheitskonzepte
- Security Usability – Sicherheit nach Maß
- Schlüsselaustausch und -management: Energieeffizient und ressourcenschonend
- Sichere Authentifizierung und Identitäten

Unser Angebot

Das Fraunhofer IIS fokussiert sich bei seinen Forschungsarbeiten auf die zwei Bereiche »Internet of Things und vernetzte Sensorsysteme« und »Systemsicherheit eingebetteter Systeme«. Wir beschäftigen uns mit der ganzheitlichen Sicherheit vernetzter und verteilter Systeme im IoT, wofür hierfür sichere schmalbandige Kommunikationskanäle erforscht werden, besonders für industrielle Prozesse.

- Technologieberatung und -entwicklung im Bereich Cybersicherheit
- Zuverlässige Sicherheitskonzepte entlang der Informationswege
- Absicherung des kompletten Systems: Vom Sensor bis in die Cloud

Fraunhofer Lernlabor Cybersicherheit

Wir nutzen Ergebnisse, die im Rahmen des Projekts Lernlabor Cybersicherheit der Fraunhofer Gesellschaft entstehen. Es handelt sich hierbei um eine Zusammenarbeit zwischen Fraunhofer und ausgewählten Fachhochschulen. Fach- und Führungskräfte aus Industrie und öffentlicher Verwaltung erhalten eine kompakte Qualifizierung in hochwertigen Laboren mit Anwendungsbezug und aktueller IT-Infrastruktur.

Das richtige Maß an Sicherheit

- Situations- und anwendungsgerecht
- Prozessorientiert und kostenoptimal
- Kontextbasiert
- Ganzheitlich