Handelsblatt Journal

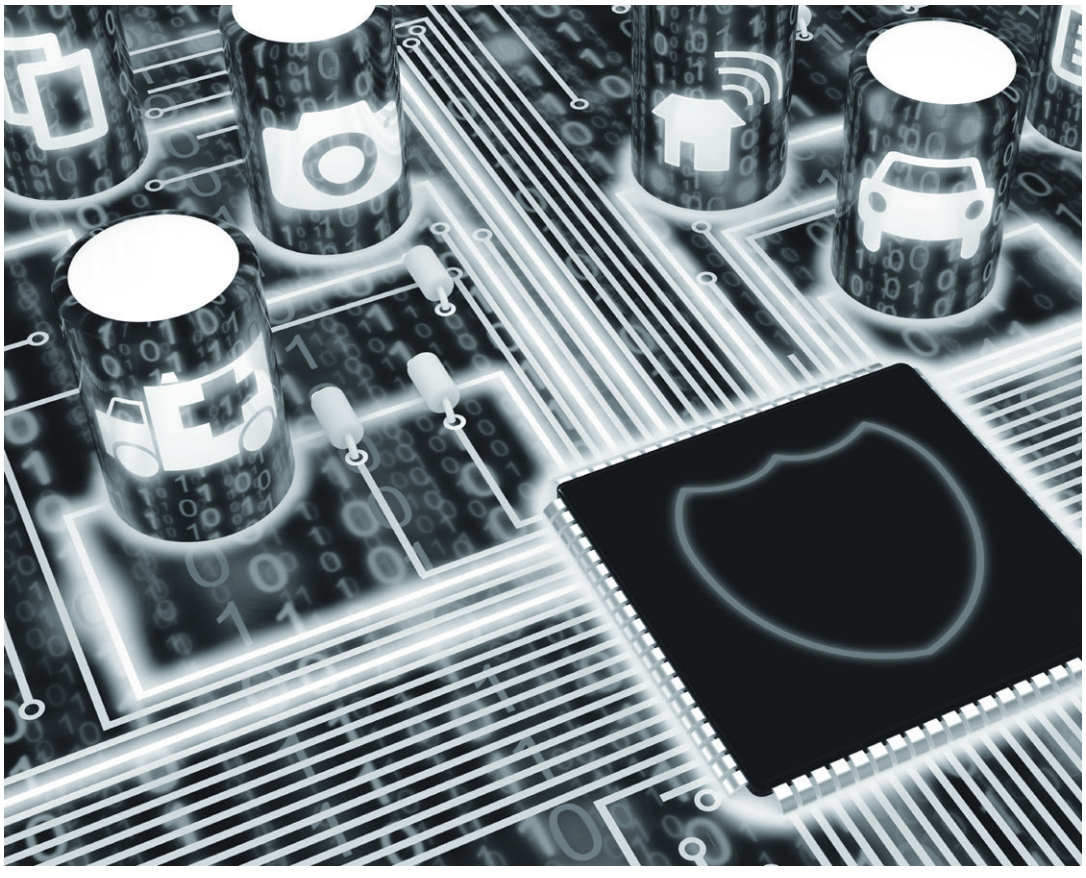
Eine Sonderveröffentlichung der EUROFORUM Deutschland SE

MÄRZ 2017 | WWW.HANDELSBLATT-JOURNAL.DE

Unsere Zukunft mit Künstlicher Intelligenz S. 3

EUROFORUM
an informa business

Medienpartner
Handelsblatt
Substanz entscheidet.



IoT-Sicherheit muss die Eingebetteten Systeme einschließen

von Prof. Dr. Axel Sikora

Das Internet der Dinge (Internet of Things, IoT) verbindet die physische Welt der Eingebetteten Systeme und der smarten Sensoren und Aktoren mit den leistungsfähigen Rechner- und Speicherressourcen des Internets. Dabei gewinnt die Datensicherheit, die landläufig als Security bezeichnet wird, aus zwei Gründen an Bedeutung. Zum einen muss gewährleistet werden, dass die in den physischen Sensoren entstehenden Daten vor unberechtigtem Zugriff geschützt werden, weil sie potenziell Rückschlüsse auf Produktionsprozesse, Lagerbestände oder auch persönliches Benutzerverhalten erlauben können. Zum anderen wird in diesen IoT-Systemen nicht mehr nur beobachtet, sondern auch gesteuert und geregelt. Die Resistenz gegen Angriffe auf die Security wird somit auch zu einer grundlegenden Voraussetzung für die funktionale Sicherheit der Systeme (Safety).

Bis in die Gegenwart finden sich reihenweise Systemangriffe auf und über Eingebettete Systeme. Bekannt sind z.B. so genannte Botnetze über ungesicherte Webcams, ungewollte Fernsteuerungen von Heizungsanlagen über deren Sicherheitslücken, die Möglichkeiten, vernetzte Autos zu „übernehmen“ und fernzusteuern, oder auch der Angriff auf die DSL-Router der Deutschen Telekom. All dies sind nur ein paar wenige Beispiele für Angriffe auf die vermeintlich schwächsten Glieder der Sicherheitskette, die dann auch Zugriff auf die darüber liegenden Systeme und Anwendungen ermöglichen.

Prof. Dr. Axel Sikora,
Leiter, Institut für verlässliche Embedded Systems und Kommunikationselektronik (ivESK) an der Hochschule Offenburg und den Bereich Software Solutions bei der Hahn-Schickard Gesellschaft für Angewandte Forschung e.V.

Eingebettete Systeme basieren in der Regel auf sehr kostengünstigen Mikrocontrollern oder Hardware-Schaltungen und verfügen damit meist über nur sehr beschränkte Energie-, Rechner- und Speicherressourcen. Dabei sind sie aber oft viele Jahre und Jahrzehnte im Einsatz. Traditionell wurden sie als Stand-Alone-Geräte betrieben und kaum abgesichert. Sie werden nun aber im IoT-Zeitalter vernetzt und damit all den Risiken von Cyber-Angriffen ausgesetzt, ohne dafür vorbereitet zu sein.

Erfreulicherweise ist jedoch zu beobachten, dass sich in der letzten Zeit vor dem Hintergrund einer steigenden Nachfrage die Aufmerksamkeit der Security-Spezialisten zunehmend auch auf Eingebettete Systeme richtet. Einige positive Beispiele untermauern dies:

Immer mehr Halbleiterhersteller entdecken, dass sie durch die Integration von kosten- und energieeffizienten Hardware-Beschleunigern und sicheren Speicher- und Ausführungseinheiten wichtige Alleinstellungsmerkmale im immer enger werdenden Markt der Mikrocontroller erreichen können.

Die Security wird vermehrt von Unternehmen in ihre Entwicklungsprozesse mit einbezogen. Die Unternehmen folgen dabei oft den Prozessen, wie sie für die funktionale Sicherheit seit Jahren existieren.

Standards (auch im Feldbusbereich) schließen zunehmend auch die Security in ihre Aktivitäten mit ein. Beispiele - an denen auch das Team des Autors beteiligt ist - sind die Entwicklung eines „Security Profiles“ der PROFINET Working Group „PN CB/PG10 PN Security”, die Aktivitäten der Special Interest Group des CAN in Automation e.V. „SIG application layer TF security“ für die Entwicklung von Ende-zu-Ende-Sicherheitslösungen für den CAN-Bus, sowie die gemeinsame Arbeitsgruppe der OPC Foundation und der M2M Alliance e.V. für die Beschreibung von durchgängigen Sicherheitslösungen für OPC UA-basierte Systeme.

Bewährte Protokolllösungen, wie beispielsweise TLS, lassen sich zunehmend auch in Eingebetteten Systemen implementieren, um infrastrukturunabhängige Ende-zu-Ende-Sicherheitslösungen einsetzen zu können.

Der Staat sieht immer stärker die Notwendigkeit, die Absicherung der IoT-Systeme einzufordern, wobei in Deutschland das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine relevante, aber ausbaufähige Rolle spielt. Beispiele hierfür sind sowohl die sehr konkrete Technische Richtlinie TR03109 für das Secure Smart Meter Gateway als auch das im Juli 2015 beschlossene IT-Sicherheitsgesetz, das sich aber vor allem mit - leider nur sehr ungenau definierten - Kritischen Infrastrukturen beschäftigt.

Auch wenn all diese Entwicklungen nun endlich in eine gute Richtung zeigen, so muss doch zusammenfassend festgestellt werden, dass diese in der Regel „zu spät kommen und zu wenig sind“. Die „Spirale der Gewalt“ im Cyberwar dreht sich zunehmend schneller und so sind weitere massive Anstrengungen auf allen Ebenen notwendig, um hier nicht abgehängt zu werden.