Embedded Systems und Security

Wie viel Sicherheit ist sicher genug?

Vernetzte und leistungsfähige Embedded-Systeme durchdringen nicht nur zunehmend unseren Alltag – sie übernehmen auch immer mehr vielfältige, anspruchsvolle und sicherheitskritische Aufgaben in Industrie, Infrastruktur und Gesundheitsversorgung. Entwickler und Anbieter der Systeme sind deshalb gut beraten, sich systematisch mit dem Thema (Angriffs-)Sicherheit zu befassen.

Von Oliver Roth,
CEO von Grossenbacher Systeme

Als Embedded-Systeme nicht vernetzt waren und zur Bedienung unkritischer Gerätschaften wie Mikrowellenherde oder Werkzeugmaschinen eingesetzt wurden, war Security – die Sicherheit vor Cyberangriffen – kaum ein Thema.

Heute, da gerade Systeme auf Arm-Basis in Industrie, Gebäudeautomation, Infrastruktur oder im Gesundheitswesen komplexe Steuerungs- und Bedienaufgaben übernehmen, hat sich das grundlegend geändert. Vor dem Hintergrund hybrider Bedrohungen im Zusammenhang mit dem Ukrainekrieg bekommt die Angriffssicherheit sensibler Systeme zusätzliche Brisanz.

Sicherheit ist ein Must-have

Im Internet of Things sind Sicherheitsfunktionen jedoch auch in friedlichen Zeiten eine unabdingbare Voraussetzung für den zuverlässigen Betrieb von Embedded-Systemen. Wegen der für diese Systeme typischen Ressourcenknappheit (Rechenleistung, Leistungsaufnahme) muss die Sicherheit zudem meist in die Kernfunktionalität integriert werden.

Unternehmen wie die Grossenbacher Systeme AG, die Komponenten wie Gateways, Controller und Displays im Auftrag von Automatisierungs- und Medizintechnik-Anbietern entwickeln und fertigen, sollten ihr Leistungsportfolio deshalb um ein Element ergänzen: die Entwicklung und Umsetzung individueller Security-Konzepte.

Was darf Sicherheit kosten – an Geld und Systemressourcen?

Sicherheit ist nicht umsonst – sie muss aber auch nicht teuer sein. Um eine anwendungsbezogen hohe Sicherheit mit akzeptablen Kosten erreichen zu können, sollten nicht nur die Entwickler, sondern auch die Produkt- und Projektmanager auf Auftraggeberseite mit dem Spektrum der möglichen Sicherheitsmaßnahmen zumindest grob vertraut sein. Nur so können sie Vorschläge bewerten und Aufwand und Nutzen im Rahmen einer individuellen und projektbezogenen Risikoabschätzung in eine gute Balance bringen. Schließlich sind die Sicherheitsanforderungen so unterschiedlich wie die Einsatzbereiche der Embedded-Systeme. Diese Risikoabschätzung und den daraus folgenden Maßnahmenkatalog müssen Produktvermarkter (OEM) und Entwickler gemeinsam erarbeiten. In den meisten Fällen bieten sich vier Bereiche an, um das erforderliche Maß an Sicherheit zu erreichen.

Vier Kernbereiche der Sicherheit von Embedded-Systemen

Bereich Nummer eins ist das Härten (Hardening) des Betriebssystems. In vielen Fällen empfiehlt sich der Einsatz einer speziell angepassten, im Hinblick auf die Sicherheit optimierten und gleichzeitig möglichst schlanken Linux-Variante. Sie darf ausschließlich Komponenten enthalten, die für den Betrieb des Systems unbedingt erforderlich und zugleich nachweislich sicher sind. Generell gilt: Je weniger Komponenten enthalten sind, desto we-

niger Einfallstore für Bedrohungen existieren. Zudem muss das gehärtete System gegen Angriffe aus dem Netz geschützt und in seinem Systemverhalten so konzipiert sein, dass es selbst zu seinem Schutz beiträgt. Zum Beispiel lässt sich das System so programmieren, dass es selbst nach der Cloudapplikation sucht, statt sich finden zu lassen. Außerdem kann es auf sicheren Passwörtern bestehen und deren Erneuerung zumindest im Update-Intervall erlauben oder einfordern.

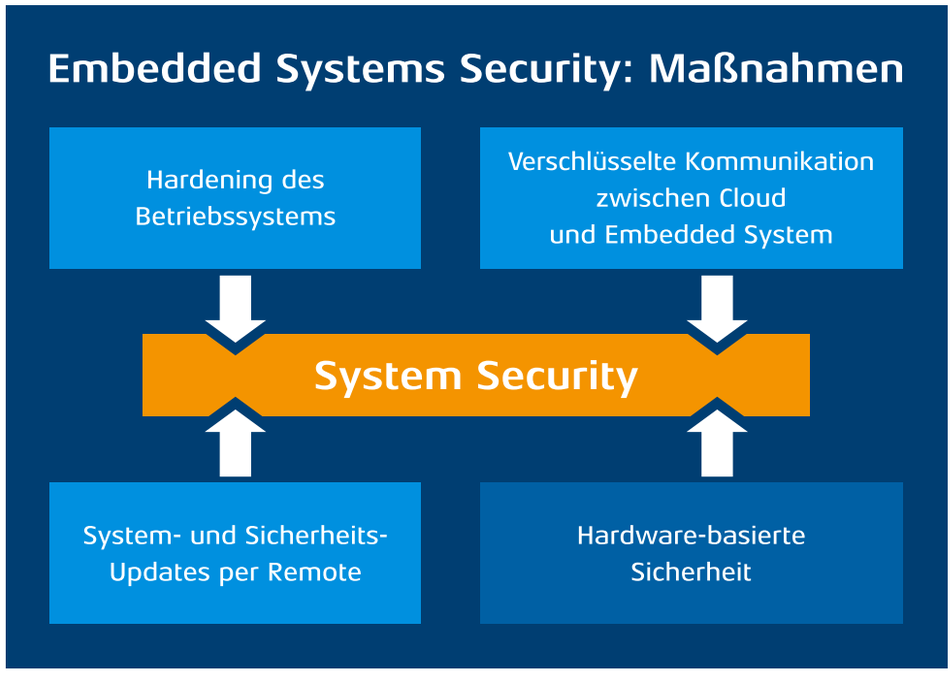
Für das Hardening kommen diverse Maßnahmen in Betracht:

- Root File System schreibschützen
- Unnötige Systemkomponenten entfernen
- Clevere Rechte- und Benutzerverwaltung
- Root Remote Access verbieten
- Regelmäßige Linux-Patches und -Updates
- Software Images verschlüsseln und signieren
- Netzwerkzugriffe kontrollieren, unbenutzte Ports präventiv schließen
- Secure-Boot-Prozess erstellen
- Sicherheitsmodule wie TPM oder CAAM verwenden
- Regelmäßige Penetration Tests

Kompetenz als wichtigste Ressource

Generell ist das Härten des Betriebssystems ein ergiebiges Feld, das auch die Themen Verschlüsselung und Update Management tangiert. Deshalb bieten sich hier zahlreiche Maßnahmen an, die effektiv und effizient sind. Anders gesagt: Sie schützen wirksam, ohne massive Kosten zu verursachen – sofern die Entwickler das entsprechende Know-how und Problembewusstsein mitbringen.

Der zweite Bereich ist die Verschlüsselung der Kommunikation (Kryptografie) zwischen dem Embedded-System und der Cloudapplikation. Hier sind verschiedene Sicherheitsstufen mit einfacher oder mehrfacher Verschlüsselung möglich. Allerdings reicht es nicht, kryptografische Algorithmen nur mathematisch sicher zu gestalten. Es ist oft relativ einfach, kryptografische Anwendungen mit physikalischen Angriffen zu brechen (z. B. den geheimen Schlüssel zu finden). Deshalb ist der Einsatz moderner Verschlüsselungstechnologien ein unbedingtes Muss.



Grafik: Grossenbacher Systeme

Um Embedded-Systeme »cybersecure« zu machen, bieten sich viererlei Maßnahmen an.

Der dritte Bereich ist die Remote-Update-Funktion: Das System muss sich im laufenden Betrieb und im Feld an neu entdeckte oder entstandene Bedrohungen anpassen lassen. Die dafür erforderlichen Updates müssen natürlich selbst ebenfalls gesichert sein und gesichert kommuniziert werden, damit sie nicht zu Einfallstoren für Malware werden. Das System sollte zudem von sich aus nach Updates suchen und diese nur von einem definierten Absender akzeptieren.

Mit Security Hardware geht mehr – aber muss sie wirklich sein?

Wer die bis hier genannten Maßnahmen konsequent umsetzt, erzielt bereits ein sehr hohes Maß an Sicherheit – nicht aber maximale Sicherheit nach dem Stand der Technik. Diese erfordert den Einsatz spezieller Hardware-Security-Komponenten wie etwa dedizierte Kryptografie-Chips oder spezielle Arm-Prozessoren. Ihre Integration ist jedoch frühzeitig bei der Konzeption eines Systems zu berücksichtigen und verursacht nicht unerhebliche Mehrkosten. Sofern keine bindenden Richtlinien existieren, sollte eine systematische Risikobewertung klären, ob so viel Sicherheit tatsächlich erforderlich ist. Abseits von Medizintechnik, Luft- und Raumfahrt oder ähnlich kritischen Bereichen ist das nur selten der Fall.

Sorgfältige Abwägung und Ehrlichkeit sind nötig

Doch selbst bei einer Beschränkung auf Software-Sicherheitsmaßnahmen bleiben genug Fragen zu klären: OEMs und deren Produktmanager fokussieren sich erfahrungsgemäß auf ihre Anwendung und den Kundennutzen – Security betrachten sie als notwendiges Übel, das Kosten verursacht, ohne einen funktionalen Mehrwert zu bieten. Dabei ist sie eine der wichtigsten nichtfunktionalen Eigenschaften eines Systems, frei nach dem Motto: Sicherheit ist nicht alles, aber ohne Sicherheit ist alles nichts.

Gefragt ist deshalb die projekt- und anwendungsbezogen richtige Abwägung zwischen der Sicherheit und funktionalen Eigenschaften wie Schnelligkeit und komfortable Bedienbarkeit: Die Sicherheit sollte so hoch wie möglich sein, ohne diese Eigenschaften zu beeinträchtigen.

Entwicklungs- und Produktionsdienstleister wie Grossenbacher Systeme müssen deshalb als Partner von OEMs in der Lage sein, gemeinsam mit den Projektverantwortlichen auf Kundenseite individuelle und sinnvoll ausbalancierte Security-Konzepte zu erarbeiten und konsequent umzusetzen. Wichtig ist dabei auch Offenheit im Umgang miteinander. Schließlich ist Sicherheit nie absolut, und die letzte Verantwortung für das Gesamtsystem muss der OEM übernehmen. Auf Basis eines konsequent umgesetzten Security-Konzepts fällt das entschieden leichter. (ak)