Cyber Resilience Act

Zeit für ein Rendez-vous mit TARA

Bild: Sidney vd Boogaard/stock.adobe.com

Im September tritt die erste konkrete Maßnahme im Zusammenhang mit dem Cyber Resilience Act (CRA) in Kraft: die Meldepflicht aktiv ausgenutzter Schwachstellen. Und ab Dezember 2027 dürfen nur noch Produkte mit nachgewiesener CRA-Konformität in Verkehr gebracht werden. Höchste Zeit, den ersten konkreten Schritt hin zu »Security by Design« zu tun – die Bedrohungsanalyse TARA (Threat and Risk Assessment). Von Jonas Schuster

Mit dem CRA schafft die EU erstmals einen verbindlichen Rechtsrahmen, der alle Hersteller von Produkten mit digitalen Elementen dazu verpflichtet, Cybersicherheit systematisch über den gesamten Produktlebenszyklus umzusetzen und nachzuweisen. Das schließt Embedded-Systeme ausdrücklich mit ein und betrifft somit auch Maschinenbauer und Industrieausrüster. Der CRA verlangt von ihnen eine angemessene Risikoanalyse und -bewertung, um Bedrohungen zu identifizieren, Schutzmaßnahmen abzuleiten, »Security by Design« nachzuweisen und Compliance zu belegen. Eine strukturierte Bedrohungsanalyse gemäß TARA-Standards, die technische, organisatorische und betriebliche Aspekte gleichermaßen berücksichtigt, ist zwar nicht zwingend erforderlich, als auditsichere Methode aber dringend empfehlenswert. Zudem setzt die geforderte »Security by Design« eine strukturierte Bedrohungsanalyse voraus. Aus Sicht von Grossenbacher Systeme wird TARA daher zum Schlüssel für die Entwicklung CRA-konformer Produkte. Mit anderen Worten: TARA weist einen besonders sicheren und ebenen Weg zur CE-Kennzeichnung.

Durchgesetzt hat sich diese Erkenntnis unter Maschinenbauern und Industrieausrüstern jedoch noch nicht. Für Grossenbacher war dies ein Grund, anlässlich der letzten SPS in Nürnberg einen TARA-Workshop zu verlosen. Der Gewinner war die Maico Elektroapparate-Fabrik GmbH – sie hat den Workshop bereits absolviert. Für den baden-württembergischen Spezialisten für Ventilatoren und Lüftungslösungen hat Michael Vosseler in seiner Funktion als Abteilungsleiter Technologie & Entwicklung teilgenommen. Sein Fazit: »Wir bei Maico hatten uns bereits ein-

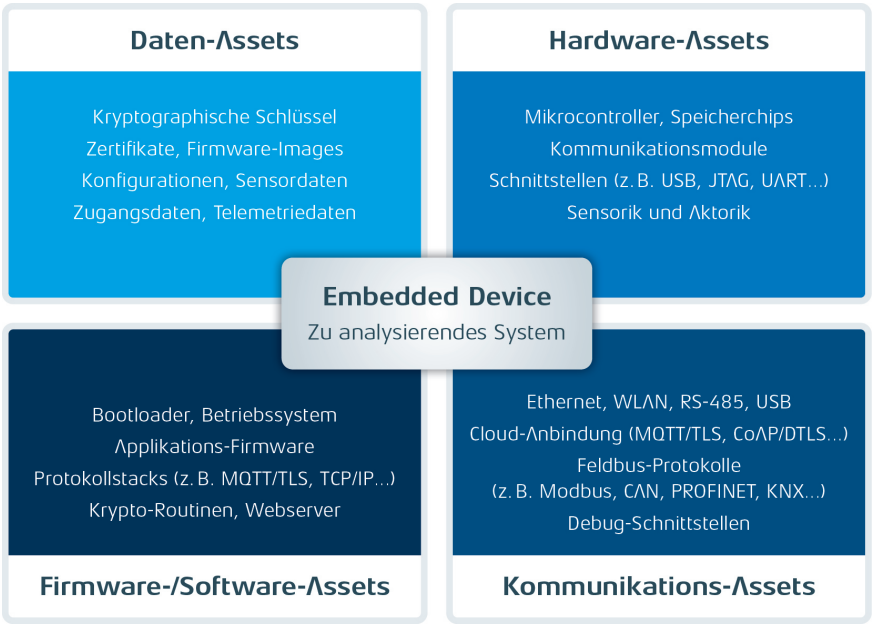
gehend mit dem Thema CRA beschäftigt und können sagen, dass uns der Workshop eine Vielzahl neuer Einsichten und Erkenntnisse gebracht hat. Das bringt uns im Hinblick auf das vollständige Inkrafttreten des CRA definitiv einen wichtigen Schritt weiter.«

Gemeinsames Systemverständnis als Grundlage

Doch was genau verbirgt sich hinter dem Begriff »Threat and Risk Assessment«? TARA ist ein systematisches Vorgehen, eine Methode, um Bedrohungen zu identifizieren, Risiken zu bewerten und daraus Sicherheitsmaßnahmen abzuleiten. Dabei startet TARA auf organisatorischer Ebene: Unternehmen, die eine Bedrohungsanalyse durchführen, müssen alle relevanten produktbezogenen Rollen einbinden, um ein vollständiges Systemverständnis zu schaffen. Neben Projektleitung und Produkt-Verantwortlichen gehören dazu auch Systemarchitekten, Security-Experten sowie Hardware- und Softwareentwickler als technische Experten.
Ebenso wichtig sind jedoch Rollen mit Blick auf den realen Einsatz: Lieferanten liefern Informationen zu integrierten Komponenten, während Servicetechniker und Support typische Wartungsszenarien und Fehlbedienungen kennen. Auch kundennahe Funktionen wie Vertrieb und Customer Success können wertvolle Hinweise geben, etwa zur Akzeptanz von Sicherheitsmaßnahmen oder zu realen Nutzungsmustern. Gerade bei Embedded-Systemen, die häufig über viele Jahre in unterschiedlichsten Umgebungen betrieben werden, ist diese ganzheitliche Sicht von entscheidender Bedeutung.

Systemabgrenzung: Was gehört zum Betrachtungsumfang?

Im ersten inhaltlichen Analyseschritt wird das betrachtete System eindeutig definiert. Ziel ist ein für alle Beteiligten verbindliches, dokumentiertes Verständnis darüber, welche Komponenten, Schnittstellen und Funktionen analysiert werden. Typische Embed-



TARA bringt es an den Tag: Ein einziges beispielhaftes Embedded-System in der Industrie kann eine Vielzahl schutzwürdiger Assets enthalten. (Bild: Grossenbacher Systeme)

ded-Systeme haben eine Vielzahl potenzieller Angriffspunkte: lokale Schnittstellen wie USB oder SD-Karte, Debug-Interfaces wie JTAG, Netzwerkverbindungen über WLAN oder Ethernet sowie drahtlose Kommunikationsschnittstellen wie Bluetooth. Doch selbst Displays können sicherheitsrelevant sein, etwa im Hinblick auf Datenschutz oder physische Manipulation. Eine visuelle Darstellung in Form von Blockdiagrammen oder Netzplänen hat sich als besonders hilfreich erwiesen. Sie schafft Transparenz über Kommunikationspfade, Systemgrenzen und Vertrauenszonen und bildet die Grundlage für alle weiteren Analyseschritte.

Security Context: Annahmen zur Nutzung und Betriebsumgebung

Anschließend folgt die Beschreibung des sogenannten Security Contexts. Dabei werden Annahmen über Einsatzumgebung, Nutzungsverhalten und Betriebsanforderungen dokumentiert. Diese Annahmen sind entscheidend, weil sie definieren, unter welchen Bedingungen ein Produkt als sicher gilt. Beispiele hierfür sind physische Zugangsbeschränkungen, Netzwerkarchitekturen oder Anforderungen an die Passwortsicherheit. Der CRA verlangt ausdrücklich eine solche Kontextdefinition, da sie die Grundlage für eine realistische Risikobewertung und die Abgrenzung zwischen Herstellerverantwortung und Betreiberpflicht bildet.

Schnittstellen und Assets systematisch erfassen

Im nächsten Schritt werden schutzwürdige Assets und sämtliche Schnittstellen identifiziert und hinsichtlich der Protokolle, Zugriffsmöglichkeiten und übertragenen Daten analysiert. Typische Beispiele sind Fernwartungszugänge über SSH, Datenschnittstellen wie MQTT oder lokale Konfigurationsschnittstellen. Zu den schutzwürdigen Assets gehören neben sensiblen Daten wie Zugangsdaten oder personenbezogenen Informationen auch Firmware, Konfigurationsdateien und proprietäre Algorithmen. Selbst Hardwarekomponenten können kritische Assets darstellen, wenn ihr Ausfall oder ihre Manipulation den Systembetrieb beeinträchtigt. Durch diese strukturierte Erfassung entsteht Transparenz darüber, was geschützt werden muss. Somit bildet sie die Grundlage für die eigentliche Risikobewertung.

Auswirkungen und Eintrittswahrscheinlichkeit bewerten

Die Risikobewertung beruht auf zwei zentralen Dimensionen: der möglichen Schadensauswirkung und der Eintrittswahrscheinlichkeit. Die Auswirkungsanalyse befasst sich mit den Folgen eines erfolgreichen Angriffs, beispielsweise mit Systemausfällen, Datenverlusten, Sicherheitsrisiken für Personen, regulatorischen Konsequenzen sowie wirtschaftlichen Schäden und Reputationsverlusten. Hinsichtlich der Eintrittswahrscheinlichkeit empfiehlt sich eine differenzierte Betrachtung, die zwischen Ausgesetztheit und Ausnutzbarkeit unterscheidet. Während die Ausgesetztheit beschreibt, wie zugänglich eine Schnittstelle ist, bewertet die Ausnutzbarkeit den technischen Aufwand eines Angriffs. So erhöht ein zugänglicher USB-Port die Ausgesetztheit, während eine Authentifizierung die Ausnutzbarkeit verringert.

Bedrohungen identifizieren und strukturiert analysieren

Auf Basis dieser Vorarbeiten werden konkrete Bedrohungsszenarien identifiziert. Methoden wie Angriffsbäume helfen dabei, mögliche Angriffspfade systematisch zu analysieren. Dafür ist ein breites Expertenwissen entscheidend, weil viele Risiken aus der spezifischen Kombination von Hardware, Firmware und Einsatzumgebung entstehen.

Risiken bewerten und Maßnahmen ableiten

Aus den Bewertungen ergibt sich ein Risikoniveau, typischerweise anhand einer mehrstufigen Matrix: von »akzeptabel« über »grundsätzlich« und »eingeschränkt akzeptabel« bis hin zu »nicht akzeptabel«. Risiken der letzten Kategorie erfordern zwingend Gegenmaßnahmen, die auf unterschiedlichen Ebenen ansetzen können: Eine stärkere Authentifizierung verringert die Ausnutzbarkeit, deaktivierte Schnittstellen reduzieren die Ausgesetztheit, und Fail-Safe-Konzepte begrenzen potenzielle Schäden. Wichtig ist, dass alle Maßnahmen systematisch dokumentiert und in die Produktanforderungen integriert werden. Dabei sollte man die grundlegende Zielsetzung des CRA im Auge behalten. Im Fokus steht nicht die vollständige Eliminierung aller Risiken, sondern eine nachverfolgbare und angemessene Beherrschung der Sicherheitsrisiken während des gesamten Produktlebenszyklus.

Kontinuierlicher Prozess, dauerhafte Partnerschaft

TARA ist also eine dauerhafte Aufgabe, denn neue Funktionen, Software-Updates oder veränderte Einsatzbedingungen können die Risikolage jederzeit verändern und zum Handeln zwingen. Die strukturierte Bedrohungsanalyse entwickelt sich somit zu einem Kernelement moderner Embedded-Entwicklung. Aus Sicht der Grossenbacher Systeme AG sind OEMs in der Industrie daher gut beraten, sich zügig und sorgfältig einen kompetenten TARA-Partner zu suchen. Denn dieser sollte die Entwicklung, Fertigung und Pflege der Embedded-Systeme beherrschen, um die Einhaltung der regulatorischen Anforderungen und die Wettbewerbsfähigkeit der Lösungen während des gesamten Produktlebenszyklus zu gewährleisten. ak

Jonas Schuster

ist Geschäftsleiter Marketing & Vertrieb bei Grossenbacher Systeme.