PICKPLACE
embedded. safe. secure.

CRA-MASSNAHMEN MIT DER TARA ASSESSIEREN

Die Entwicklung sicherer eingebetteter Elektronik erfordert ein umfassendes Verständnis der Bedrohungen und Risiken, die auf das jeweilige System einwirken können. TARA steht für Threat Analysis and Risk Assessment und bildet die notwendige Grundlage für die Implementierung von Sicherheits-maßnahmen. Die TARA ist der zentrale Baustein für die CE-Konformität gemäß des Cyber Resilience Acts, welches ab 2026 verpflichtend wird. Sie ermöglicht es, sowohl die Notwendigkeit als auch die Nichtnotwendigkeit von spezifischen Sicherheitsfunktionen für eingebettete Systeme zu bestimmen. **Die TARA bestimmt letzten Endes , ob und welche konkreten auf das Gerät bezogene Security-Maßnahmen für das Embedded Device notwendig sind.**

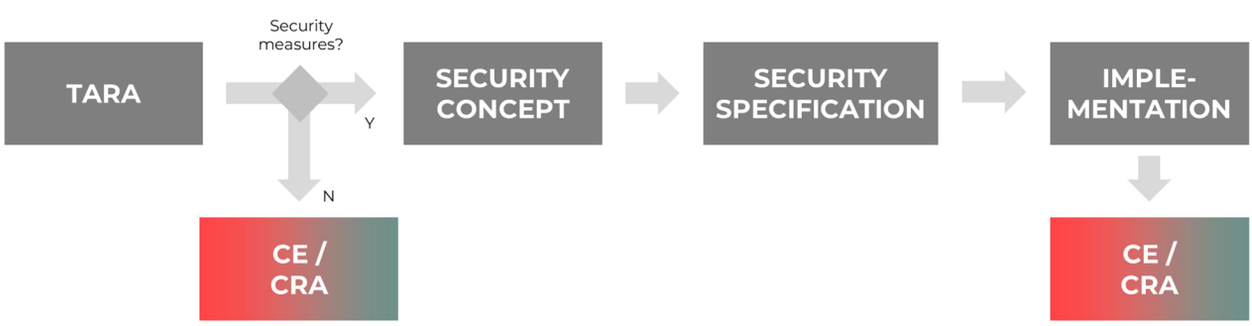

Abbildung 1 Threat and Risk Assessment im Kontext der CE-(CRA-) Zertifizierung

Abbildung 1 zeigt die Entscheidungslogik für die ab 2026 notwendige CE-Zertifizierung gemäß CRA.

Gemäß der Grafik wird ein sequenzieller Ablauf zur Entwicklung sicherer Systeme beschrieben. Entwickler und Entscheider analysieren mit der TARA Bedrohungen und entscheiden gemäß der Kritikalität einzelner Bedrohungen, ob Sicherheitsmaßnahmen notwendig sind. Basierend darauf wird ein Security Concept entwickelt, das in einer detaillierten Spezifikation umgesetzt wird.

Wenn keine Security-Maßnahmen notwendig sind, dient die TARA als Nachweis dafür, dass man innerhalb der Produktentwicklung die Cyber Security in Betracht gezogen hat. Das macht die TARA zum Schlüsselelement für die CE-Zertifizierung im Kontext des Cyber Resilience Acts.

27 MRD. Bis 2025 gibt es schätzungsweise 27 Milliarden IoT-Geräte[1]. Hinzu kommen Geräte, die über Gateways und Routern mittelbar an das Netz angeschlossen sind. 90% aller Rechner weltweit sind Embedded Systems – Steuergeräte, Industriesensoren, Messgeräte, Kameras.

32% Laut dem Microsoft Digital Defense Report 2022 enthalten 32 % aller Firmware-Images mehr als 10 kritische Sicherheitslücken[2]. Darunter fallen vor allem Out-of-Bounds-Reads, Man-in-the-Middle-Exploits und Denial-of-Service-Attacks.

CYBER-SECURITY-PROZESS

Das Umsetzen von Cyber-Security-Maßnahmen auf Produkt- und Embedded-Systems-Ebene ist ein produktstrategischer Prozess und umfasst mehrere Stufen.

THREAT ANALYSIS AND RISK ASSESSMENT (TARA)

Im Rahmen der TARA werden **potenzielle Einfallstore** identifiziert, darunter physische Schnittstellen, Netzwerkschnittstellen wie OTA oder ModBus/CAN, Firmware-Update-Mechanismen und Back-End-Systeme. Angriffsvektoren wie physischer Zugriff auf Geräte, Remote-Angriffe über Netzwerkschnittstellen oder die Manipulation von Firmware-Updates werden detailliert analysiert.

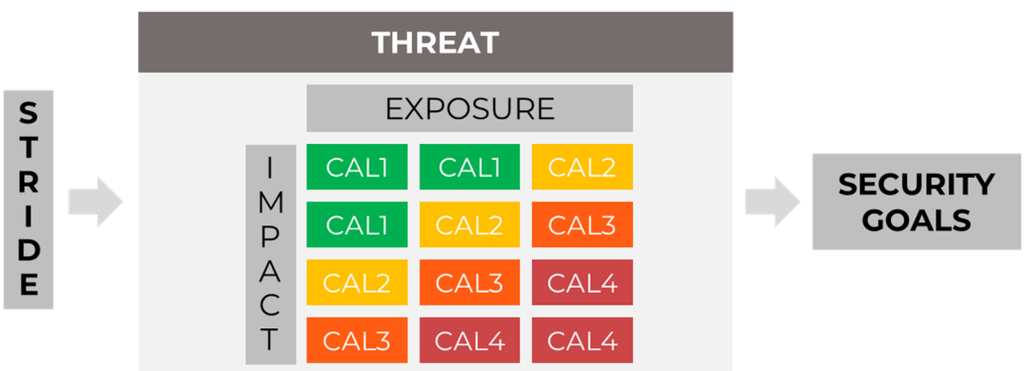

Abbildung 2 Analyse pro Threat hinsichtlich Cybersecurity Assessment Levels

Für jeden Angriffsvektor wird das notwendige Skillset des Angreifers eingeschätzt, von einfachen Tools und Tutorials bis hin zum tiefgreifenden Verständnis von Kryptografie und Systemarchitektur. Die Auswirkungen eines Angriffs werden hinsichtlich der Anzahl betroffener Geräte, der finanziellen Verluste und der Risiken für Leib und Leben bewertet.

SECURITY CONCEPT

Basierend auf der TARA werden konkrete Sicherheitsmaßnahmen definiert. Die Cyber-Sicherheit von Embedded Systems fußt konkret auf **vier Säulen**.

Diese umfassen einerseits systemische Maßnahmen wie Zero-Trust-Kommunikation und Schlüsselmanagement, um die Verwaltung kryptografischer Schlüssel sicherzustellen. Andererseits müssen bestehende Kommunikationsschnittstellen durch Anti-DoS-Maßnahmen sichergestellt werden, um das System durch Traffic-Filter oder Ratenbegrenzungen vor Outages zu schützen. Final sind sicheres Booten und Updates Kernelemente sicherer Embedded Systems.

Zusätzlich werden Empfehlungen zur Verbesserung der Hardware- und Software-Architektur gegeben, beispielsweise der Einsatz moderner Mikrocontroller mit TrustZone oder HSM sowie die Integration sicherer Speicherbereiche für kritische Daten. Der Handlungsplan priorisiert diese Maßnahmen, definiert zeitliche Meilensteine und klärt die Verantwortlichkeiten.

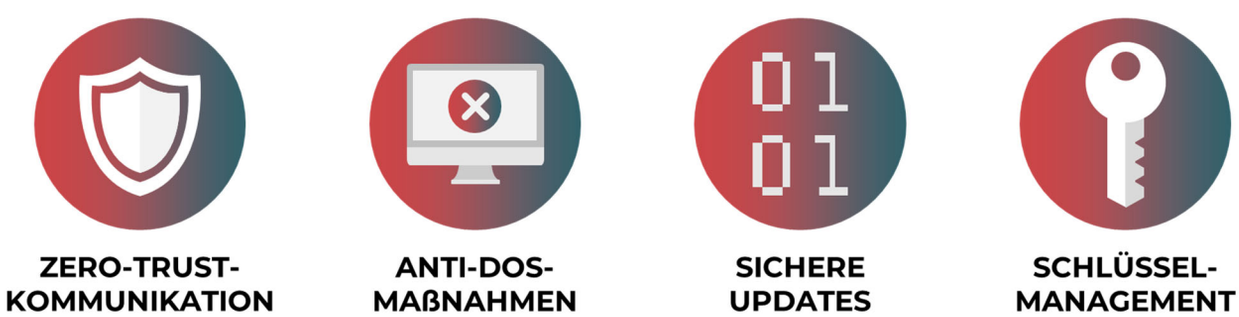

Abbildung 3 Vier Säulen der Cyber-Sicherheit von Embedded Systems

UMSETZUNGSPLANUNG

Die TARA ist als Vorstufe zur CRA-Selbstzertifizierung unverzichtbar für die Sicherheitsarchitektur von Geräten mit eingebetteter Elektronik. Sie stellt eine notwendige Grundlage für die CE-Konformität und die Marktfähigkeit dar. Dieses Projekt bietet eine strukturierte und praxisnahe Lösung, um Geräte effektiv gegen aktuelle und zukünftige Bedrohungen zu schützen und gleichzeitig regulatorische Anforderungen zu erfüllen.

Ab Juni 2026 sind Unternehmen verpflichtet, Schwachstellen innerhalb von 24 Stunden der Europäischen Agentur für Cybersicherheit zu melden. Wichtig sind dabei dedizierte Teams für die Ermöglichung strukturierter Reaktion auf

Sicherheitsvorfälle. Dies ist besonders wichtig, da die Meldepflichten nicht nur für neue Produkte gelten, sondern auch für solche, die bereits auf dem Markt sind.

Der CRA fordert zudem die regelmäßige Analyse von Sicherheitsrisiken. Bedrohungs- und Risikoanalysen müssen daher fester Bestandteil des Entwicklungsprozesses sein. Die TARA gilt allgemein als Ist-Stand-Analyse der Produkte, um den Anforderungen des CRA gerecht zu werden.

TARA-ANALYSEN DURCHFÜHREN

PICKPLACE führt für Sie **unabhängig** TARA-Analysen durch. Unsere Experten untersuchen Ihr System in seiner Gesamtheit anhand von Schaltplänen, Designs und Software. Dabei identifizieren wir potenzielle Angriffsvektoren, bewerten deren Wahrscheinlichkeit und analysieren die Auswirkungen auf Sicherheit, finanzielle Verluste sowie Risiken für Leib und Leben. Das Ergebnis dieser Analyse dient als Grundlage für die Entwicklung effektiver Sicherheitsmaßnahmen und unterstützt Sie dabei, die CE-Konformität zu erreichen. **Vertrauen Sie auf unsere Erfahrung und Kompetenz, um Ihre eingebettete Elektronik zukunftssicher zu gestalten.**

PICKPLACE – PICKPLACE CONSULTING GMBH
BRANDSTÜCKEN 24
22549 HAMBURG
TEL.: +49 (0) 40 3251 6647
GESCHÄFTSFÜHRER: DR.-ING. HENDRIK SCHNACK
E-MAIL: INFO@PICKPLACE.DE
WEB: WWW.PICKPLACE.DE
UST-ID GEMÄSS §27 A UMSATZSTEUERGESETZ: DE317521985
RECHTSFORM: GESELLSCHAFT MIT BESCHRÄNKTER HAFTUNG
VERANTWORTLICH IM SINNE DES PRESSERECHTS: DR.-ING. HENDRIK SCHNACK

[i] *Laut IoT Analytics wird die Anzahl der weltweit verbundenen IoT-Geräte bis 2025 auf 27 Milliarden ansteigen. Quelle: IoT Analytics Bericht*
[ii] *Nach Microsoft Digital Defense Report 2022 enthalten 32 % aller Firmware-Images mehr als 10 kritische Sicherheitslücken. Dazu gehören Out-of-Bounds-Reads, Man-in-the-Middle-Exploits und Denial-of-Service-Angriffe. Quelle: Microsoft Digital Defense Report 2022*