RED-DA-Cybersicherheit für Hersteller funkbasierter IoT-Geräte

Wenn Sie funkbasierte oder intelligente/smarte Produkte herstellen, die sich über WiFi, Bluetooth oder andere Funktechniken vernetzen, sind Sie wahrscheinlich mit der CE-Kennzeichnung auf Elektronikgeräten vertraut. Das CE-Logo ist mehr als nur ein Label – es ist die Voraussetzung für das legale Inverkehrbringen von Produkten auf dem Markt der Europäischen Union (EU) und bestätigt, dass Geräte die grundlegenden Anforderungen an Gesundheit und Sicherheit erfüllen.

Überarbeitete Richtlinie

Bis vor kurzem konzentrierten sich die EU-Vorschriften für Elektronikgeräte vor allem darauf, körperliche Schäden, Gerätefehlfunktionen und Funkstörungen zu vermeiden. Mit der zunehmenden Verbreitung intelligenter und vernetzter Produkte – von alltäglichen Consumer-Geräten bis hin zu komplexen industriellen Systemen – nehmen jedoch auch die Cyberrisiken zu. Geräte sind zunehmend mit Netzwerken verbunden, verarbeiten personenbezogene Daten und sind Teil kritischer Infrastrukturen, was sie zu bevorzugten Zielen für Cyberangriffe macht.

Um diesen wachsenden Bedenken zu begegnen, hat die EU die Funkanlagenrichtlinie RED (Radio Equipment Directive) durch den RED Delegated Act (RED-DA) überarbeitet, der im August 2025 in Kraft getreten ist. Die neue Verordnung stellt sicher, dass alle funkfähigen und IoT-Produkte, die auf den EU-Markt in Verkehr gebracht werden, die verbindlichen Cybersicherheitsanforderungen erfüllen.

Wo gilt RED-DA?

Der Anwendungsbereich der RED-DA ist breit gefächert und erweitert sich mit dem Wachstum des digitalen Ökosystems. Die Richtlinie gilt für alle Produkte, die eine Funkschnittstelle enthalten. Dazu gehören Geräte wie Unterhaltungselektronik (Smart Speaker, vernetzte Lichtschalter und Fernseher), Wearables (Smartwatches und Fitness-Tracker), Gesundheits-/Medizintechnik und medizinische Sensoren, vernetztes Spielzeug und Ortungsgeräte sowie IoT-Systeme, die Smart Homes, industrielle Umgebungen und kritische Infrastrukturen unterstützen.

RED-DA im Kontext des Cyber Resilience Act (CRA)

RED-DA konzentriert sich zwar speziell auf funkbasierte Geräte, ist jedoch keine isolierte Initiative. Sie ist Teil einer umfassenderen Regulierungsinitiative der EU zum Aufbau eines stärkeren und sichereren digitalen Ökosystems. CRA ist eine separate, aber ergänzende Verordnung, die sich auf eine breitere Kategorie digitaler Produkte mit Embedded-Software bezieht, unabhängig davon, ob diese über eine Funkschnittstelle verfügen.

Zusammen bilden RED-DA und CRA wichtige Säulen des sich weiterentwickelnden Cybersicherheits-Regulierungsrahmens der EU. Während RED-DA sicherstellt, dass Geräte, die Funktechnik verwenden, sicher, vertrauenswürdig und konform sind, bevor sie das CE-Zeichen tragen dürfen, erweitert CRA diesen Anwendungsbereich auf den gesamten Lebenszyklus digitaler Produkte. Dazu gehören die Entwicklung nach dem Prinzip „Secure by Design“, die laufende Softwarewartung, die Meldung von Schwachstellen und der langfristige Support, um einen stärkeren Schutz und eine höhere Widerstandsfähigkeit im gesamten digitalen Ökosystem zu gewährleisten. Kurz gesagt, RED-DA ist ein Baustein im mehrschichtigen Ansatz der EU zur Sicherheit digitaler Produkte. Für Hersteller hilft das Verständnis von RED-DA nicht nur dabei, unmittelbare Compliance-Anforderungen zu erfüllen, sondern auch, sich auf die umfassenderen, systemischen Verpflichtungen vorzubereiten, die durch die CRA eingeführt werden.

Autor:
Abhinay Venuturumilli
Senior Manager Worldwide Marketing der Wireless Solutions Group
Microchip Technology
www.microchip.com

EN 18031 als harmonisierte Norm

In diesem Sinne hat Europa die Norm EN 18031 als harmonisierte Norm eingeführt, um die Cybersicherheitsanforderungen der RED zu erfüllen. Sie umfasst Netzwerkschutz, Datenschutz und Betrugsprävention und bietet Herstellern einen praktischen Rahmen für den Nachweis der Konformität. Für die meisten funkbasierten und IoT-Produkte steht die Norm EN 18031 im Mittelpunkt, die Anforderungen an den Schutz von Netzwerken vor Missbrauch, Störungen und Angriffen festlegt. Sie betont sichere Designpraktiken wie Authentifizierung, Zugriffskontrolle, verschlüsselte Kommunikation, geschützte Updates und Widerstandsfähigkeit gegen gängige Bedrohungen, um sicherzustellen, dass vernetzte Geräte sowohl konform als auch vertrauenswürdig sind. Die Norm enthält maßgeschneiderte Leitlinien für verschiedene Gerätetypen und stellt sicher, dass die Sicherheitsmaßnahmen dem Risiko angemessen sind.

Da Europa seine digitale Widerstandsfähigkeit (Resilienz) stärkt, werden diese Normen und Vorschriften die Art und Weise prägen, wie Produkte entworfen, getestet, dokumentiert und gewartet werden, und gleichzeitig die Messlatte für die Sicherheit höher legen.

Warum Konformität für Entwickler funkbasierter Produkte wichtig ist

- **Risko und Ruf**

  Für Lösungsanbieter, die funkbasierte Technik integrieren, ist robuste Netzwerksicherheit nicht nur für die Einhaltung von Vorschriften unerlässlich, sondern auch zum Schutz des Kundennutzens und zur Wahrung des Vertrauens im Markt. Die Nichteinhaltung der RED-DA-Anforderungen kann Produkte anfällig für Sicherheitslücken, Rückrufe oder Verkaufsbeschränkungen machen. Dies stört den Geschäftsbetrieb und schädigt den Ruf der Marke sowie die langfristige Glaubwürdigkeit bei Partnern, Regulierungsbehörden und Endnutzern. Seit dem 1. August 2025 ist die Einhaltung der Vorschriften für alle neuen funkbasierten Geräte, die in der EU verkauft werden, obligatorisch. Jedes Produkt, das keine gültige Konformitätserklärung (DoC; Declaration of Conformity) gemäß EN 18031 vorweisen kann, riskiert nun ein Verkaufsverbot in Europa.

- **Komplexität in der Lieferkette**

  Hersteller integrieren häufig Funkmodule oder System-on-Chip-Bausteine (SoCs) als Rückgrat ihrer Funkanbindung. Wenn sichergestellt ist, dass diese Komponenten selbst die Norm EN 18031 erfüllen und über eine vorgelagerte DoC verfügen, vereinfacht sich die nachgelagerte Konformitätsprüfung erheblich, was die Kosten und den technischen Aufwand reduziert.

RED-DA

Die Rolle der Konformitätserklärung (DoC)

Eine DoC ist eine offizielle Erklärung, die bestätigt, dass ein Produkt alle geltenden Richtlinien und Normen erfüllt, einschließlich der RED-DA-festgelegten Cybersicherheitsanforderungen. Für Unternehmen, die Funkmodule oder SoCs integrieren, bietet der Erhalt einer DoC von Technologieanbietern erhebliche Vorteile: Erstens vereinfacht sie die Dokumentation, da die DoC des Lieferanten in die Konformitätsunterlagen des Produkts aufgenommen werden kann. Zweitens beschleunigt sich die CE-Kennzeichnung durch den Einsatz vorzertifizierter Module und drittens reduziert sich der Gesamtaufwand für die Konformität, da umfangreiche zusätzliche Tests auf ein Minimum reduziert werden.

Über die Effizienz hinaus stärkt es auch das Vertrauen, indem es ein starkes Bekenntnis zur regulatorischen Verantwortung gegenüber Partnern und Endnutzern signalisiert. Anbieter von Funk-SoCs und -modulen, die der RED-DA-Konformität Priorität einräumen, ermöglichen ihren Kunden schnellere, sicherere und zuverlässigere Neuerungen.

Praktische Schritte für Hersteller funkbasierter Geräte

Für Hersteller funkbasierter Geräte umfassen die RED-DA-Anforderungen praktische Schritte, die mit dem Verständnis der Verordnung und den für das jeweilige Produkt geltenden harmonisierten Normen beginnen. Es ist faktisch notwendig, nur Funkmodule oder Chipsätze RED-DA-konformer Lieferanten mit gültigen DoCs für EN 18031 auszuwählen. Da die Verantwortung für das Endprodukt letztlich beim Hersteller liegt, stellt eine gründliche Lückenanalyse sicher, dass alle zusätzlichen Anforderungen, die über die vom ausgewählten Modul oder SoC abgedeckten Anforderungen hinausgehen, ordnungsgemäß berücksichtigt werden. Sicherheit muss ebenfalls von Anfang an integriert werden, wobei Security-by-Design-Praktiken in den Hardware- und Software-Lebenszyklus einfließen müssen. Um die Konformität zu gewährleisten, sollten Hersteller eine vollständige und überprüfbare Dokumentation, einschließlich technischer Unterlagen, Testberichte und Konformitätserklärungen von Lieferanten, mindestens zehn Jahre nach Markteinführung aufbewahren. Schließlich sollten Unternehmen eine kontinuierliche Konformität planen, indem sie sich über neue Vorschriften wie den CRA auf dem Laufenden halten und Prozesse für zeitnahe Sicherheitsupdates und Schwachstellenmanagement implementieren.

Sicherheit ist eine gemeinsame Verantwortung

Die RED-DA-Cybersicherheitsanforderungen, mit der Norm EN 18031 als Kernstück, stellen einen Wandel im Umgang von Herstellern mit der Sicherheit funkbasierter und IoT-Produkte dar. Die Verantwortung für die Einhaltung der Vorschriften liegt nicht bei einem einzelnen Akteur, sondern ist eine gemeinsame Verpflichtung des gesamten Entwicklungs- und Lieferökosystems.

Die Wahl des richtigen Anbieters für Funkmodule oder SoCs, der RED-DA proaktiv unterstützt und eine Konformitätserklärung ausstellt, ist von entscheidender Bedeutung. Genauso wichtig ist auch, dass Hersteller selbst Verantwortung dafür übernehmen, wie diese Technologien in ihre Endprodukte integriert und implementiert werden. Sicherheit muss von Anfang an in den Entwicklungsprozess integriert sein und darf nicht erst in einer späten Phase als Patch hinzugefügt werden.

Dazu zählt auch das Prinzip der gestaffelten Verteidigung, die gewährleistet, dass die Sicherheit über mehrere Ebenen des Systems hinweg implementiert wird, anstatt sich auf einen einzigen Schutzpunkt zu verlassen. Kunden werden dazu angehalten, TLS (Transport Layer Security) für verschlüsselte Kommunikation zu aktivieren – auch wenn ihre Geräte bereits WiFi-Sicherheitsprotokolle nutzen. Durch solche mehrschichtigen Schutzmaßnahmen lassen sich Risiken mindern, wenn eine Ebene versagt. Angreifer werden daran gehindert, über eine einzige Schwachstelle Zugriff auf sensible Daten oder Systemsteuerungen zu erlangen.

Durch die enge Zusammenarbeit mit erfahrenen, compliance-fähigen Lieferanten und die Ausrichtung interner Entwicklungsprozesse an anerkannte Standards können Unternehmen die gesetzlichen Anforderungen erfüllen und somit widerstandsfähigere, vertrauenswürdige Lösungen für die vernetzte Welt bereitstellen.

Fazit

Jetzt ist es an der Zeit, zu handeln, um sich vorzubereiten, zusammenzuarbeiten und sichere funkbasierte Produkte zu entwickeln, die den Erwartungen von heute und den Herausforderungen von morgen gerecht werden. ◄