CYBER SECURITY ALS MARKTZUGANGS-VORAUSSETZUNG

Was der RED DA fordert und wie die Umsetzung gelingt

ITK Engineering GmbH | www.itk-engineering.de | industry@itk-engineering.de

1. ABSTRACT

Ab August 2025 gilt er verbindlich: Der Radio Equipment Directive Delegated Act für Cybersicherheit (RED DA). Die Richtlinie macht erstmals Sicherheitsvorgaben für Funkanlagen – unter anderem für bestimmte vernetzte Produkte – zur Pflicht. Für Hersteller bedeutet das: wenig Zeit, viele Fragen – und Handlungsdruck. Doch wer RED nur als eine weitere regulatorische Belastung betrachten, übersieht das Wesentliche: Mit RED wird Cyber Security zur Voraussetzung für den Marktzugang – und wer jetzt handelt, ebnet bereits den Weg für den anstehenden Cyber Resilience Act (CRA). In diesem Artikel erklären wir, warum mehr Hersteller als gedacht betroffen sind, wie sich die Einhaltung der RED DA-Richtlinie nachweisen lässt und worauf es bei der Umsetzung der Schlüsselnorm EN 18031 ankommt.

2. DER DELEGATED ACT ZUR FUNKANLAGEN-RICHTLINIE – CYBER SECURITY WIRD ZUR PFLICHT

Ab dem 1. August sollten Hersteller von Geräten mit Funkkomponenten ein besonderes Augenmerk auf den Delegierten Rechtsakt zur Funkanlagenrichtlinie für Cyber Security legen (Radio Equipment Directive Delegated Act, kurz: RED DA). Denn dieser bringt verbindliche Cybersicherheitsanforderungen mit sich, die erfüllt sein müssen, um Produkte auf dem europäischen Markt anbieten zu dürfen.

Was dabei häufig übersehen wird: Der RED DA betrifft nicht nur klassische Funkgeräte. Er könnte auch für Produkte gelten, an die man nicht sofort denkt. Das trifft vor allem auf Kombinationen aus Nicht-Funk- und Funkanlagen zu – also Produkte, die keine Funkanlagen sind, in die aber ein Funkmodul dauerhaft integriert und nicht ohne Weiteres zugänglich ist oder entfernt werden kann. Da heute viele Produkte irgendeine Art von Funkmodul enthalten, reicht der Geltungsbereich der Verordnung weiter als vermutet und gilt für eine Vielzahl von Produkten, die über Geräte mit „Funk" als Kernfunktion hinausgehen. Hersteller müssen sicherstellen, dass die Konformität des Funkmoduls im Endprodukt gewahrt bleibt. Das kann bedeuten: Die RED-Anforderungen müssen auf das gesamte System angewendet werden – selbst dann, wenn das Modul als eigenständige Komponente bereits nachgewiesenermaßen konform ist.

So anspruchsvoll die neuen Pflichten für viele Hersteller auf den ersten Blick wirken mögen: Auf lange Sicht bieten sie eine klare Chance. Entwickeln Hersteller sichere Produkte, verringern sie auch die Risiken für selbst. Dennoch wurde Cyber Security in der Vergangenheit oft als Kostentreiber gesehen, nicht als Wettbewerbsvorteil. Das ändert sich jetzt: Mit dem neuen Rechtsaktsind Investitionen in Cybersicherheit nicht länger optional oder potenziell nachteilig.

Cybersicherheit wird zur Voraussetzung für den Marktzugang: Alle Hersteller, die auf dem europäischen Markt bestehen wollen, müssen dieselben Anforderungen erfüllen. Das schafft gleiche Bedingungen – und belohnt diejenigen, die das Thema Sicherheit ernst nehmen.

Hinzu kommt: Ab Dezember 2027 gilt der EU Cyber Resilience Act (CRA) vollständig. Der RED DA schafft dafür ein starkes Fundament – denn viele der Anforderungen decken zentrale Elemente des CRA bereits ab. Beide Verordnungen beruhen auf mehreren identischen Grundanforderungen. Dazu zählen unter anderem Cyber Security Risikobewertungen, Dokumentationsanforderungen und konzeptionelle Mechanismen für die Cybersicherheit. Wer heute RED-konform entwickelt, ist morgen bereits gut auf den CRA vorbereitet.

Im RED DA sind drei wesentliche Anforderungen an die Cybersicherheit von Funkanlagen definiert [1]:

"Funkanlagen müssen in bestimmten Kategorien oder Klassen so konstruiert sein, dass sie die folgenden grundlegenden Anforderungen erfüllen:

(...)

(d)

Sie haben weder schädliche Auswirkungen auf das Netz oder seinen Betrieb noch bewirken sie eine missbräuchliche Nutzung von Netzressourcen, wodurch eine unannehmbare Beeinträchtigung des Dienstes verursacht würde.

(e)

Sie verfügen über Sicherheitsvorrichtungen, die sicherstellen, dass personenbezogene Daten und die Privatsphäre des Nutzers und des Teilnehmers geschützt werden.

(f)

Sie unterstützen bestimmte Funktionen zum Schutz vor Betrug.

(...)"

Diese grundlegenden Anforderungen des RED DA sind weit gefasst und bieten viel Raum für Interpretation. Genau das macht die Umsetzung oft zur Herausforderung. Es gibt mehrere Wege, damit umzugehen.

3. DER WEG ZUR RED DA-KONFORMITÄT

Wer nachweisen will, dass ein Produkt den Sicherheitsanforderungen des RED DA entspricht, kann dies auf dreierlei Art tun. Dabei werden sogenannte „Konformitätsbewertungsmodule" genutzt:

Modul A: interne Fertigungskontrolle

Bei diesem Ansatz gewährleistet und erklärt der Hersteller auf eigene Verantwortung, dass das Produkt die grundsätzlichen Anforderungen des RED DA erfüllt. Dieser Ansatz kann nur verfolgt werden, wenn der Hersteller sich an eine für den RED DA harmonisierte Norm hält. Gegenwärtig handelt es sich bei der harmonisierten Norm um EN 18031. Zwar ist in diesem Fall keine benannte Stelle an der Produktbewertung beteiligt, der Hersteller ist aber dennoch verpflichtet, die Norm vollumfänglich anzuwenden. Außerdem müssen alle Unterlagen, die zur Beurteilung der ordnungsgemäßen Durchführung erforderlich sind, aufbewahrt und zusammen mit den technischen Unterlagen den nationalen Behörden zur Verfügung gestellt werden. Nationale Behörden können die Unterlagen zu einem beliebigen Zeitpunkt anfordern, um zu überprüfen, ob die interne Bewertung korrekt vorgenommen wurde.

Modul B und C: EU-Baumusterprüfung und Konformität mit dem Baumuster auf der Grundlage einer internen Fertigungskontrolle

Bei diesem Ansatz prüft eine benannte Stelle (Notified Body) die technische Auslegung der Funkanlage sowie verifiziert und attestiert, dass diese die grundsätzlichen Anforderungen erfüllt. Diese Beurteilung kann auf Grundlage der harmonisierten Norm EN 18031 erfolgen, dies ist aber nicht vorgeschrieben. Für diesen Fall wird eine enge Zusammenarbeit mit der benannten Stelle empfohlen, um sich über die spezifischen Kriterien für die Bewertung abzustimmen. Nach einer erfolgreichen Prüfung stellt die benannte Stelle eine EG-Baumusterprüfbescheinigung aus. Nachdem der Hersteller diese Bescheinigung erhalten hat, muss er sicherstellen, dass die hergestellten Produkte der zugelassenen Bauart entsprechen und die Anforderungen des RED DA einhalten.

Modul H: Konformität auf der Grundlage einer umfassende Qualitätssicherung

Bei diesem Ansatz bewertet die benannte Stelle nicht jedes einzelne Produkt, sondern das Qualitätssicherungssystem des Herstellers, das für die Entwicklung und Fertigung der Produkte verwendet wird. Dabei wird insbesondere berücksichtigt, welche Normen während der Entwicklung Anwendung finden und wie deren Einhaltung in der Praxis gewährleistet wird. Die benannte Stelle überprüft, ob das vorgeschlagene Qualitätssicherungssystem zuverlässig gewährleisten kann, dass alle gefertigten Produkte die grundlegenden Anforderungen des RED DA einhalten. Das Qualitätssicherungssystem muss regelmäßigen Re-Auditierungen unterzogen werden. Die benannte Stelle ist berechtigt, unangekündigte Inspektionen durchzuführen, um sicherzustellen, dass es ordnungsgemäß funktioniert. Wie bei Modul A muss der Hersteller die technische Dokumentation sowohl der Produkte als auch des Qualitätssicherungssystems aufbewahren und den nationalen Behörden auf Anforderung zur Verfügung stellen.

Da Bewertungen durch eine benannte Stelle mit erheblichem Aufwand verbunden ist – und da deren Kapazitäten für eine Bewertung begrenzt sind – werden sich die meisten Hersteller voraussichtlich für den Ansatz mit Modul A entscheiden und die harmonisierte Norm EN 18031 anwenden.

Dieses Verfahren erlaubt eine Eigenbewertung und die Ausstellung einer Konformitätserklärung ohne Einbindung Dritter. Wichtig zu beachten: Auch wenn keine benannte Stelle involviert ist, müssen alle relevanten technischen Unterlagen zum Zeitpunkt der Konformitätserklärung vorliegen – und den nationalen Behörden für mindestens zehn Jahre auf Anfrage zur Verfügung gestellt werden.

4. WIE HERSTELLER DIE NORM EN 18031 ERFÜLLEN

Aus unserer Sicht sind mehrere Schritte erforderlich, um die Anforderungen der Norm EN 18031 wirksam umzusetzen. Im Folgenden zeigen wir, worauf es ankommt – inklusive praxisnaher Hinweise.

ERFÜLLUNG DES STANDARDS EN 18031

STEP 1	STEP 2	STEP 3	STEP 4
Bestimmung von Anwendungsbereich und Anwendbarkeit von EN 18031-1 / -2 / -3	Zusammenstellung der technischen Dokumentation als Grundlage für eine Gap-Analyse gegen EN 18031	Cyber Security Risikobewertung	Bewertung für alle Anforderungen von EN 18031 (Bestanden/Nicht bestanden/ Nicht anwendbar)

Schritt 1: Umfang und Anwendbarkeit der EN 18031-1/-2/-3 ermitteln

Zunächst muss geklärt werden, in welchem Umfang ein System unter den RED DA fällt. In diesem Zusammenhang ist auch zu betrachten, ob es sich um ein „kombiniertes Produkt" handelt (siehe oben). [2]. Beispiele für kombinierte Anlagen:

- Leiterplatte ohne eigene Funkfunktion, auf die ein Bluetooth-Modul gelötet wird
- Integrated Administration and Control System (IACS) mit fest verdrahteter Telematikeinheit, die nicht mit wenigen Handgriffen ausgebaut werden kann

Sobald der Systemumfang klar ist, muss festgelegt werden, welche Teile der EN 18031 Anwendung finden. Die EN 18031 umfasst drei Teile, die jeweils eine der wesentlichen Anforderungen d), e) und f) des RED DA abbilden. Das impliziert auch, dass nicht alle drei Normen für jedes Produkt gelten. Entscheidend ist, ob das System …

- … direkt oder indirekt mit dem Internet verbunden ist.

→ Wenn ja, findet die EN 18031-1 wahrscheinlich Anwendung.

Ein Beispiel: Eine Smart-Home-Heizungssteuerung, der über das Internet über eine eigene IP-Adresse erreichbar it, kommuniziert drahtlos mit entfernten Temperatursensoren. Lediglich diese Steuerung ermöglicht es einem Nutzer, die Temperatur im Haus aus der Ferne zeit- und datumsgesteuert anzupassen.

- … ein mit dem Internet verbundenes Funkgerät, Kinderpflegeprodukt, Spielzeug oder Wearable ist und personenbezogene oder datenschutzrelevante Daten verarbeitet.

→ Wenn ja, findet die EN 18031-2 wahrscheinlich Anwendung.

Ein Beispiel: Eine Smartwatch, die Fitnessdaten und gesundheitsbezogene Aktivitätsdaten erfasst. Diese personenbezogenen Daten, wie Herzfrequenz oder Standort, müssen gemäß EN 18031-2 geschützt werden.

- … Nutzern ermöglicht, Geld, Geldwerte oder virtuelle Währungen zu übertragen und potenziell anfällig für Betrug ist.

→ Wenn ja, findet die EN 18031-3 wahrscheinlich Anwendung.

Ein Beispiel: Die in Beispiel 2 genannte Smartwatch unterstützt kontaktloses Bezahlen mit einer digitalen Brieftasche, die wiederum kompatible Zahlungskarten unterstützt. Damit findet nun zusätzlich EN 18031-3 Anwendung.

Die drei Teile der EN 18031 überschneiden sich in vielen Bereichen, enthalten aber jeweils auch spezifische Anforderungen, die sich nach dem Einsatzzweck und Geltungsbereich des jeweiligen Produkts richten.

Schritt 2: Technische Dokumentation erstellen – als Grundlage für die Gap-Analyse nach EN 18031

Die technische Dokumentation ist nicht nur ein zentraler Bestandteil der RED-Konformität, sondern wird auch explizit in EN 18031 gefordert (siehe Abschnitt A.2.5.2). Sie bildet die Grundlage für eine strukturierte Gap-Analyse: Mithilfe der in der Norm enthaltenen Entscheidungsbäume lässt sich prüfen, welche Sicherheitsanforderungen erfüllt sind – und wo ggf. noch Handlungsbedarf besteht. Die Dokumentation sollte mindestens folgende Bestandteile umfassen:

- Angaben zum beabsichtigten Verwendungszweck der Anlage
- Angaben zur voraussichtlichen Einsatzumgebung der Anlage
- technische Daten zur Anlage
- Erklärung zu Stand der Technik und bewährten Vorgehensweisen
- spezifische Details, zum Beispiel eine Liste der externen Anschlüsse
- Risikobewertung der Cyber Security
- Sicherheitskonzept

Schritt 3: Cyber Security Risikobewertung

Obwohl die EN 18031 für jede Anforderung Entscheidungsbäume mit einer strengen Ja/Nein-Logik enthält, muss für jede Entscheidung nachvollziehbar dokumentiert werden, warum ein „Ja" oder „Nein" gewählt wurde. In vielen Fällen sind diese Ja/Nein-Entscheidungen alles andere als trivial, da sie vom beabsichtigten Einsatzzweck und vom betrieblichen Umfeld des Systems abhängen. Um diese individuellen Produktfaktoren angemessen zu berücksichtigen, ist eine Cybersicherheits-Risikobewertung erforderlich. Sie gehört bei den meisten Anforderungen der EN 18031 zum verpflichtend zu dokumentierenden Bestandteil – und ist damit eine zentrale Grundlage für die normkonforme Bewertung.

> „...Ob und wie allgemeine Sicherheitsziele zu erreichen sind, hängt von der vorgesehenen Anlagenfunktionalität und der für die Nutzung vorgesehenen Betriebsumgebung ab. Diese beeinflussen, welche Implementationen von Sicherheitsmaßnahmen tatsächlich bei einer bestimmten Anlage erforderlich sind und wie stark die Kontrollen sein müssen. Eine spezifische Sicherheitsmaßnahme kann für ein Produkt angemessen sein, kann aber für andere Produkte oder das gleiche Produkt beim Einsatz in einer anderen Umgebung zu schwach oder zu stark sein." [3]

Ein Beispiel: [SSM-1] Anwendbarkeit von sicheren Speichermechanismen [4]

- Ziel der Anforderung: „Die Anlage muss immer sichere Speichermechanismen nutzen, um die dauerhaft auf der Anlage gespeicherten Sicherheitswerte und Netzwerkwerte zu schützen..."
- Es gibt mehrere sichere Speichermechanismen mit verschiedenen Sicherheitsmerkmalen: Die Ressourcen können z. B. durch folgendes geschützt werden:
    - durch kryptographische Maßnahmen wie Verschlüsselung, um die Vertraulichkeit sicherzustellen,
    - durch kryptographische Maßnahmen wie digitale Signaturen, um die Integrität und Authentizität sicherzustellen,
    - durch Zugangssteuerung mithilfe von Authentisierung oder Autorisierung
    - durch Hardware-Schutzmaßnahmen
    - durch physische Schutzmaßnahmen."
- Welcher dieser Mechanismen angemessen ist, richtet sich nach der Risikobewertung: „Der angemessene Schutzmechanismus hängt vom Risiko in Verbindung mit den zu speichernden Sicherheitswerten oder Netzwerkwerten ab ..."

Die EN 18031 legt nicht fest, wie die Bewertung der Cybersicherheitsrisiken durchgeführt werden muss. Unternehmen haben daher die Flexibilität, eine Methode zu wählen, die zu ihren individuellen Bedürfnissen passt. Wer viele Produktvarianten betreut, wird vermutlich Teile des Risikomodells wiederverwenden. Unternehmen mit nur einem einzelnen Produkt können dagegen einen gezielteren Ansatz für die Risikobewertung wählen.

Schritt 4: Bewertung aller Anforderungen aus EN 18031 (Erfüllt/Nicht erfüllt/keine Anwendung)

Jede Anforderung der EN 18031 enthält Kriterien zur Anwendbarkeit, durch die eine Anforderung für ein bestimmtes Produkt unter Umständen nicht relevant sein kann. Ist eine Anforderung jedoch anwendbar, muss sichergestellt werden, dass sie durch angemessene Mechanismen erfüllt wird. Diesen Prozess bildet die EN 18031 für jede Anforderung in einem Entscheidungsbaum ab. Der im Entscheidungsbaum eingeschlagene Weg, der zu einem Ergebnis wie „Bestanden"(Pass) oder „Nicht anwendbar" (Not applicable) führt, muss mit den entsprechenden Begründungen dokumentiert werden.

Ein Beispiel: [ACM-1] Anwendbarkeit von Zugangssteuerungsmechanismen [5]

- Die zuvor genannte Smart-Home-Steuerung soll es nur autorisierten Bewohnern ermöglichen, die Temperatur aus der Ferne zu ändern. Ein öffentlicher Zugriff auf die Temperatureinstellungen ist nicht vorgesehen.
- Das Gerät wird an den Endbenutzer mit einer Konfiguration ausgeliefert, die den Zugang über eine öffentliche IP-Adresse ohne Schutz durch eine ordentlich konfigurierte Firewall im lokalen Netz erlaubt.
- Es gibt keine gesetzlichen Einschränkungen, die Zugangssteuerungsmechanismen verbieten. Daher würde das Fehlen eines Zugriffskontrollmechanismus für dieses System die Anwendbarkeitskriterien aus Abschnitt 6.1 der EN 18031-1 **nicht erfüllen.**

5. FAZIT

Der Zeitplan zur RED DA-Konformität stellt viele Hersteller vor große Herausforderungen. Hinzu kommt, dass viele sich noch gar nicht bewusst sind, dass der RED DA für sie gilt – und riskieren, gegen Vorschriften zu verstoßen und die damit einhergehenden Strafen. Gleichzeitig verfügen viele Systeme auch ohne den RED DA bereits über eingebaute Cybersicherheitsmechanismen, die oft nur noch nach EN 18031 dokumentiert werden müssen. Somit ist in vielen Fällen bereits ein großer Schritt in Richtung Compliance getan.

Eine Zertifizierung durch Dritte (benannte Stellen) ist häufig nicht erforderlich, wenn die EN 18031 eingehalten wird, die Marktaufsicht kann dies aber jederzeit überprüfen. Daher ist es ratsam, die notwendigen Maßnahmen so bald wie möglich umzusetzen und zu dokumentieren. Dieser Aufwand ist keine verlorene Zeit – im Gegenteil: Er ist vielmehr einen Schritt auf dem Weg zur Einhaltung des CRA, einer horizontalen Cyber Security Verordnung, für die die Uhr mit Frist Dezember 2027 bereits tickt.

Quellen

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014L0053-20241228
[2] https://ec.europa.eu/docs-room/documents/29121
[3] EN 18031-1
[4] EN 18031-1
[5] EN 18031-1

ITK ENGINEERING

Von Embedded Systems über Cloud Computing bis zu Künstlicher Intelligenz – ITK Engineering bietet als international tätiges Technologieunternehmen plattformunabhängige Software- und Systementwicklung und umfangreiche Methodenexpertise. Das Unternehmen ist Innovationstreiber im Bereich Digital Engineering. ITK hilft namhaften Kunden aus den Branchen Automotive, Industrie, Medizin- und Bahntechnik, Land- und Baumaschinen sowie Motorsport, hochkomplexe Systeme intelligent zu machen. Seit 2017 ist das Unternehmen eine hundertprozentige Tochtergesellschaft der Robert Bosch GmbH.

Breite Methodenkompetenz als Basis für digitale Lösungen

Ausgehend von der modellbasierten Softwareentwicklung setzt ITK Engineering auf Kompetenzen wie Safety, Cyber Security, Künstliche Intelligenz, virtuelle Absicherung sowie Computer Vision. Diese breite Methodenexpertise ist die Basis, um branchenübergreifend digitale und nachhaltige Lösungen für Kunden zu entwickeln – als zuverlässiger Partner von der Idee bis zur Industrialisierung und der normkonformen Zulassung. Das Besondere dabei: Die internationalen Teams arbeiten in teils sehr unterschiedlichen Industriezweigen und können ihre Erfahrungen aus der einen Branche in andere transferieren. Diese Perspektivenvielfalt eröffnet Kunden gänzlich neue Möglichkeiten.

Jens Köhler
Chief Expert Cyber Security
Jens.Koehler@itk-engineering.de

William McCaig
Project Manager
William.Mccaig@itk-engineering.de

ITK. The Art of Digital Engineering.

ITK Engineering GmbH
Hauptsitz Rülzheim
Im Speyerer Tal 6
76761 Rülzheim
Tel.: + 49 (0)7272 7703-0
Fax: + 49 (0)7272 7703-100
info@itk-engineering.de

industry@itk-engineering.de

Folgen Sie uns auch auf: