Pressemitteilung

Mehr Wert.
Mehr Vertrauen.

Cyber Resilience Act

20. November 2024

TÜV SÜD macht digitale Produkte cyberfit

München. Mit seiner Verkündung im Amtsblatt der EU am 20. November 2024 hat der Cyber Resilience Act (CRA) die Anforderungen an digitale Produkte in der EU verschärft. Hersteller, Importeure und Vertreiber müssen ihre Cybersicherheitsrichtlinien und -praktiken dahingehend anpassen. Im Fokus stehen ein umfassendes Schwachstellen-Management, die verpflichtende CE-Kennzeichnung, die Cybersicherheit von digitalen Produkten und strenge Meldepflichten von Sicherheitsvorfällen.

Der CRA stellt neue verbindliche und umfangreiche Anforderungen an die Cybersecurity von vernetzten Hardware- und Software-Produkten in der Europäischen Union. „Ziel ist, sogenannte 'Produkte mit digitalen Elementen' sicherer zu machen. Darüber hinaus sollen Hersteller zum Schutz von Unternehmen und Verbrauchern während des gesamten Produktlebenszyklus für die Cybersicherheit der Produkte verantwortlich sein“, sagt Maxime Hernandez, IoT Cybersecurity Program Manager bei TÜV SÜD. Die neue Verordnung gilt für Produkte wie Smart TVs, Firmware, Sensoren zur Überwachung von Maschinen oder sogar für Produkte, die in Industrieanlagen eingesetzt werden. Ausgenommen sind unter anderem Medizinprodukte und Sicherheitssysteme für Kraftfahrzeuge und die zivile Luftfahrt, für die eigene branchenspezifische Anforderungen gelten. Wer nicht CRA-konforme digitale Produkte herstellt, vertreibt oder importiert, riskiert hohe Geldstrafen und verliert die Zulassung für den europäischen Markt. „Um sich gegen immer komplexere Cyberbedrohungen zu wappnen, muss nicht nur der Betrieb des digitalen Produkts, sondern sein gesamter Lebenszyklus, vom Entwurf über die Entwicklung und Herstellung etc. berücksichtigt werden“, so Maxime Hernandez weiter.

- Wie die CRA-Konformität nachgewiesen werden muss, hängt ab von der Risikoklasse des Produkts. Für digitale Produkte, die nicht als kritisch oder hochkritisch eingestuft sind, genügt zum Beispiel die Selbsterklärung durch die Hersteller gemäß Modul A einschließlich der Technischen Dokumentation als Nachweis für die Konformität mit den grundlegenden Anforderungen. Kritische Produkte müssen Hersteller und Händler jedoch durch eine Benannte Stelle wie TÜV SÜD bewerten lassen und sich dabei auf

harmonisierte Normen stützen, sobald diese zur Verfügung stehen. Darunter fallen in der so genannten Klasse I etwa Netzwerk-Managementsysteme, Passwort-Manager oder Smart-Home-Produkte mit Sicherheitsfunktionalitäten. Klasse II umfasst digitale Produkte mit einem höheren Cyberrisiko wie Firewalls, manipulationssichere Mikroprozessoren und Microcontroller. Maxime Hernandez: „Dafür bieten wir Audits, Tests und Risikobewertungen basierend auf unserer langjährigen Erfahrung mit den für diese Produktkategorie maßgeblichen Normen an."

Secure by Design

Vernetzte Produkte müssen nach CRA z. B. über Möglichkeiten zur Datenverschlüsselung und Zugangsverwaltung verfügen und eine sichere Standardkonfiguration bieten. Es reicht nicht mehr aus, dass Hersteller beim Inverkehrbringen nachweisen, dass sie cybersicher sind. Vielmehr muss über den gesamten Lebenszyklus der Produkte eine Risikobewertung erfolgen. „Wenn zum Beispiel Hersteller Komponenten zukaufen, müssen sie eine Due Diligence vornehmen, um Sicherheitslücken beim Endprodukt auszuschließen, die sich durch den Zukauf ergeben könnten", sagt Maxime Hernandez. Der Umgang mit Sicherheitslücken ist eine zentrale Pflicht der Hersteller. „Nur wer Sicherheitslücken früh entdeckt und bewertet, kann angemessen darauf reagieren." Hersteller müssen während der gesamten Lebensdauer ihrer Produkte für Sicherheits-Updates sorgen. Tritt in dieser Zeit eine Sicherheitslücke auf, müssen die Hersteller Security Advisories herausgeben und kostenlose Updates bereitstellen.

Hersteller haben zudem eine Meldepflicht von Sicherheitsvorfällen – gegenüber der ENISA (Agentur der Europäischen Union für Cybersicherheit), dem Produktnutzer und gegebenenfalls dem Beauftragten für Wartung und Instandhaltung. Insbesondere bei digitalen Produkten mit Schwachstellen müssen Produktnutzer schnell reagieren und Sicherheits-Patches installieren, sobald diese Updates verfügbar sind, oder das Produkt in der Zwischenzeit, während sie auf den Sicherheits-Patch warten, isolieren. TÜV SÜD unterstützt Hersteller dabei, Prozesse zur Meldung solcher Vorfälle zu implementieren und die CRA-Vorgaben zur technischen Dokumentation einzuhalten.

Transparent kommunizieren und dokumentieren

Der CRA schreibt zudem eine umfassende Produktdokumentation vor, die alle wichtigen Eigenschaften und Sicherheitsfunktionen aufführt. Sie muss enthalten, welche Cyberrisiken unter welchen Umständen eintreten können sowie einen Kontakt, an den man sich im Fall einer Cybersicherheitslücke wenden kann. Sie muss auch deutlich machen, wo das CE-Kennzeichen und die Software-Stücklisten zu finden sind. Letztere listen detailliert alle Bestandteile einer Software auf und erleichtern das Sicherheitsmanagement.

Nach einer Übergangsfrist von 36 Monaten treten alle Anforderungen der CRA in Kraft. „Hersteller, Händler und Importeure sollten das Thema CRA trotzdem frühzeitig angehen, um die Sicherheit für die Nutzer zu gewährleisten und später keine Wettbewerbsnachteile zu haben. Die Hersteller müssen beginnen, ihre Produkte zu verbessern und dies geht nicht von heute auf morgen“, sagt Maxime Hernandez. Vor diesem Hintergrund hat TÜV SÜD bereits damit begonnen, ein umfassendes Schulungs- und Testprogramm zur Cyber Resilience anzubieten.

Weitere Informationen:

- tuvsud.com/en/resource-centre/stories/cyber-resilience-act-a-new-era-in-product-cybersecurity
- tuvsud.com/de-de/dienstleistungen/cyber-security/europaeische-cybersecurity-regulierung
- Regulation - 2024/2847 - EN - EUR-Lex

Pressekontakt:

TÜV SÜD AG Unternehmenskommunikation Westendstraße 199 80686 München	Dirk Moser-Delarami Telefon +49 89 5791-1592 E-Mail dirk.moser-delarami@tuvsud.com Internet tuvsud.com/presse