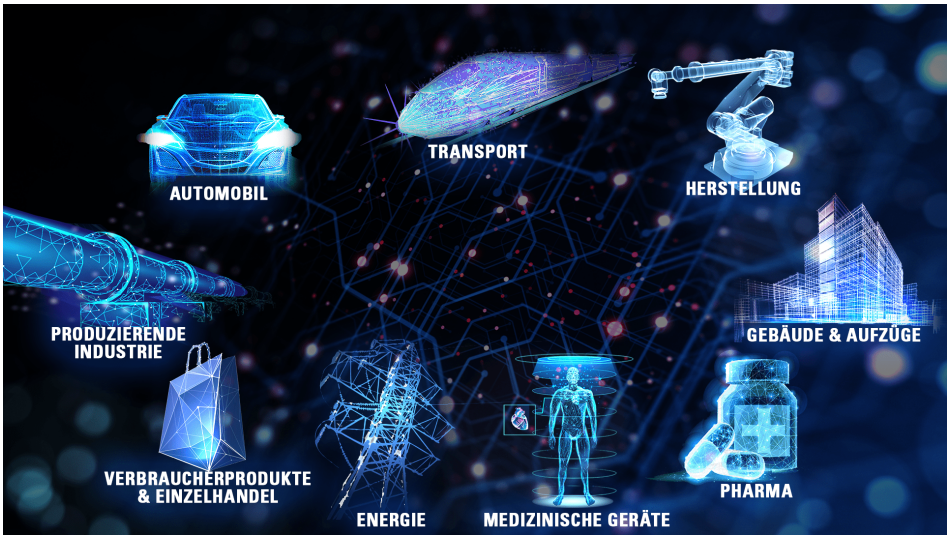
Zur Stärkung der Cybersicherheit

Artikel vom **4. März 2025**
Sonstige Dienstleistungen

Das erweiterte Dienstleistungsportfolio mit besonderem Schwerpunkt auf den aktuellen EU-Regulierungen im Bereich Cybersecurity präsentiert Tüv Süd vom 11. bis 13. März während der »Embedded World«. Als Prüfdienstleister unterstützt das Unternehmen Hersteller, Zulieferer und Betreiber dabei, die Anforderungen des »Cyber Resilience Act« (CRA), der »NIS-2«-Richtlinie sowie der »Radio Equipment Directive« (RED) zu erfüllen.



Tüv Süd präsentiert auf der Embedded World 2025 erweiterte Dienstleistungen zur Cybersicherheit. Bild: Tüv Süd

Mit der Einführung des »CRA« setzt die EU Maßstäbe für die Sicherheit digitaler Produkte und deren Software. Der »CRA« legt verbindliche Cybersicherheitsanforderungen für alle Produkte mit digitalen Elementen fest, die in der EU hergestellt, importiert oder vertrieben werden. Ziel ist es, Sicherheitslücken frühzeitig zu erkennen, Risiken zu minimieren und eine durchgehende Cybersicherheit über den gesamten Lebenszyklus eines Produkts hinweg sicherzustellen. Tüv Süd unterstützt Unternehmen dabei, die regulatorischen Anforderungen zu erfüllen, indem das Unternehmen umfassende Dienstleistungen zur Sicherheitsbewertung,

Penetrationstests, Software-Analysen und Zertifizierungen anbietet.

- Risikobewertung und Schwachstellenanalyse: Identifikation potenzieller Sicherheitslücken und Erarbeitung von Maßnahmen zur Risikominimierung.
- »Secure Software Development Lifecycle«-Bewertungen: Unterstützung bei der Implementierung sicherer Entwicklungsprozesse zur Einhaltung der »CRA«-Vorgaben.
- Zertifizierung und Konformitätsbewertung: Prüfung, ob Produkte den neuen Sicherheitsanforderungen entsprechen, einschließlich der Vergabe entsprechender Zertifikate.

Tüv Süd unterstützt Unternehmen bei der Einhaltung von EU-Regulierungen wie CRA, NIS-2 und RED. Bild: Tüv Süd

»Der Cyber Resilience Act stellt Unternehmen vor neue Herausforderungen, bietet aber auch eine große Chance, die Sicherheit digitaler Produkte nachhaltig zu verbessern«, erklärt Stefan Würth, Senior Manager Automotive & Industrie Security bei Tüv Süd. »Wir helfen Herstellern dabei, die gesetzlichen Vorgaben zu erfüllen und ihre Produkte auf ein höheres Sicherheitsniveau zu bringen.« **Schutz Kritischer Infrastrukturen** Die neue EU-Richtlinie zur Netz- und Informationssicherheit (»NIS-2«) trat 2024 in Kraft und erweitert die Anforderungen für Unternehmen in kritischen und essenziellen Sektoren. Unternehmen müssen strengere Cybersicherheitsmaßnahmen umsetzen, eine verbesserte Risikoanalyse durchführen und sich auf umfangreiche Berichtspflichten einstellen. Tüv Süd bietet Unternehmen gezielte Unterstützung bei der Umsetzung der »NIS-2«-Anforderungen.

- Gap-Analysen zur Einhaltung der »NIS-2«-Richtlinie: Bewertung bestehender Sicherheitsmaßnahmen und Identifikation von Optimierungspotenzial.
- Erstellung und Implementierung von Sicherheitsrichtlinien: Entwicklung maßgeschneiderter Sicherheitsstrategien für Organisationen.
- Penetrationstests und Angriffssimulationen: Testen der Resilienz gegenüber Cyberangriffen und Schwachstellenanalysen.
- Awareness-Schulungen für Mitarbeiter: Sensibilisierung für Cyberbedrohungen und Schulung zu sicherem Verhalten im Unternehmensumfeld.

„Die Richtlinie hat eine weitreichende Wirkung auf Unternehmen vieler Branchen. Tüv

Süd hilft dabei, frühzeitig notwendige Maßnahmen umzusetzen und langfristig die Cybersicherheit zu erhöhen“, erläutert Würth. **Vernetzte Geräte** Ab 1. August 2025 treten neue regulatorische Anforderungen an die Cybersicherheit von Funkanlagen gemäß der »Radio Equipment Directive« (RED) in Kraft. Diese betreffen insbesondere die Netzwerksicherheit, den Schutz der Privatsphäre der Nutzer sowie die Vermeidung von finanziellen Betrugsrisiken bei funktionsfähigen, vernetzten Geräten. Tüv Süd bietet Herstellern umfassende Prüf- und Zertifizierungsdienstleistungen um sicherzustellen, dass ihre Produkte mit den neuen Anforderungen der Richtlinie konform sind.

- Sicherheitsprüfungen für vernetzte Geräte: Überprüfung von IoT-Produkten hinsichtlich Datenschutz und Manipulationssicherheit.
- Evaluierung der Netzwerksicherheit: Prüfung von Schwachstellen in der drahtlosen Kommunikation und Schutzmaßnahmen gegen Angriffe.
- Konformitätsbewertung nach den neuen »RED«-Vorgaben: Sicherstellung, dass Produkte den neuen Sicherheitsstandards entsprechen und marktfähig bleiben.

»Die neuen Anforderungen der Richtlinie stellen sicher, dass vernetzte Geräte nicht nur zuverlässig, sondern auch sicher gegenüber Cyberbedrohungen sind«, erläutert Würth. »Mit unseren umfassenden Prüfverfahren sorgen wir dafür, dass Hersteller und Zulieferer den steigenden Anforderungen gerecht werden.«

Die »Embedded World Exhibition&Conference« bietet während der »Embedded World 2025« einen Einblick in die Welt der eingebetteten Systeme, von Bauelementen und Modulen über Betriebssysteme bis hin zu Hard- und Software-Design sowie M2M-Kommunikation. Bild: Tüv Süd

Während der Fachmesse Embedded World 2025 stehen die Experten von Tüv Süd für Fachgespräche zur Verfügung und informieren Unternehmen zu den Herausforderungen der neuen Cybersicherheitsrichtlinien. Besucherinnen und Besucher haben die Möglichkeit, sich über Best Practices und konkrete Lösungsansätze für die Einhaltung des »Cyber Resilience Acts«, der »NIS-2«-Richtlinie und der »Radio Equipment Directive« zu informieren. Die Embedded World Exhibition&Conference ist ein internationaler Branchentreffpunkt für die Embedded-Community. Sie bietet einen umfassenden Einblick in die Welt der eingebetteten Systeme, von Bauelementen und Modulen über Betriebssysteme bis hin zu Hard- und Software-Design sowie M2M-Kommunikation. Die Veranstaltung fokussiert auf Technologien, Prozesse und zukunftsweisende Produkte.

Hersteller aus dieser Kategorie