München, 18. Juni 2026
Presseinformation

Claudia Grzelke
PR Manager
Tel. +49 89 949-21498
claudia.grzelke@
messe-muenchen.de

electronica 2026
Sichere Komponenten: Cyber-Resilienz rückt in den Fokus der Elektronikentwicklung

- **Unternehmen müssen vernetzte Elektronik gegen Attacken von außen schützen**
- **Studien zeigen: Cyberangriffe nehmen zu, allerdings bleiben Investitionen in Sicherheit oft aus**
- **Die electronica 2026 zeigt Technologien für resiliente Elektronik**

Vernetzte und digitalisierte Fahrzeuge, Maschinen und Energiesysteme stellen neue Anforderungen an die Elektronik. Sie muss ab sofort nicht nur leistungsfähig sein, sondern auch Angriffe erkennen, Störungen begrenzen und sichere Updates ermöglichen. Cyber-Resilienz trägt daher wesentlich zu Vertrauen, Verfügbarkeit und Erfolg im Markt bei. Welche Technologien dafür entscheidend sind, zeigt die electronica 2026 vom 10. bis 13. November in München.

Industrielle Anlagen, Fahrzeuge und Energiesysteme entwickeln sich zunehmend zu vernetzten Elektroniksystemen, die über Software gesteuert, aktualisiert und abgesichert werden. Sicherheitsmechanismen lassen sich daher nicht nachträglich ergänzen, sondern müssen von Beginn an im Systemdesign verankert sein, insbesondere für Schnittstellen, Updates und softwaredefinierte Funktionen.

Gleichzeitig erwarten Kunden, Regulierer und Betreiber belastbare Nachweise für die Sicherheit und Updatefähigkeit elektronischer Systeme. „Die electronica 2026 in München bringt als Weltleitmesse der Elektronik zentrale Akteure der gesamten Wertschöpfungskette zusammen. Damit schafft sie den Rahmen, um Cybersicherheit nicht isoliert zu betrachten, sondern als gemeinsame

Architekturaufgabe der Elektronikbranche zu lösen“, erklärt Caroline Pannier, Projektleiterin der electronica.

Studien zeigen steigenden Handlungsdruck

Die wachsende Bedeutung des Themas zeigt sich in aktuellen Studien. So nennt zum Beispiel der *ENISA Threat Landscape 2025* Bericht Cyber-Angriffe auf öffentliche Einrichtungen sowie den Transportsektor als meist gewählte Ziele. Die dabei am häufigsten eingesetzte Methode ist Phishing. Vielfach ist dabei die Betriebstechnik (OT) von Unternehmen das Ziel der Angreifer.

Trotz der steigenden Bedrohungslage investieren laut einer *PwC-Studie* bisher lediglich etwa 15 Prozent der deutschen Unternehmen gezielt in proaktive Sicherheits- und Resilienz-Maßnahmen. Der überwiegende Teil bleibe reaktiv: Investitionen werden überwiegend erst nach Vorfällen oder im Zuge regulärer Updates vorgenommen, ein umfassendes, präventiv ausgerichtetes Transformationskonzept ist oft nicht vorhanden.

Zunehmende Regulierung von Cybersicherheit

Um Unternehmen ins Handeln zu bringen und Sicherheit von Beginn an in Produkte zu integrieren, hat die Europäische Union die Verordnung zum Cyber Resilience Act (CRA) erlassen. Er reguliert gezielt Produkte, die Unternehmen auf dem europäischen Markt in Umlauf bringen. So verlangt der CRA unter anderem, dass Produkte mit digitalen Elementen während ihrer erwarteten Nutzungsdauer sicher sind und Schwachstellen über den gesamten Lebenszyklus behandeln. Der CRA betrifft dabei eine breite Palette elektronischer Produkte, und zwar nicht nur internetfähige Geräte, sondern grundsätzlich alle Produkte mit direkter oder indirekter logischer oder physischer Verbindung zu einem Gerät oder Netzwerk.

Cyberangriffen wirkungsvoll begegnen

Damit macht der CRA Sicherheit zu einer wichtigen Entwicklungsanforderung. Zugleich entstehen neue Risiken durch KI-basierte Systeme: Data Poisoning, Model Poisoning oder Adversarial Attacks können KI-Modelle manipulieren

und Fehlentscheidungen auslösen. Entwickler reagieren darauf mit „Security-by-Design“ – also mit Sicherheitsmechanismen, die von Beginn an in Architektur, geschützter Firmware sowie überprüfbaren Updates integriert sind.

Auf Komponentenebene zählen hierzu unter anderem eine Hardware Root of Trust, Secure Boot und Trusted Platform Modules (TPMs). Sichere Mikrocontroller (MCUs) implementieren Sicherheitsfunktionen direkt im Bauteil und ermöglichen beispielsweise, dass beim Systemstart nur authentifizierte Firmware oder signierter Code ausgeführt wird.

Aussteller zeigen relevante Technologien

Auf der electronica präsentieren zahlreiche Aussteller ihre Innovationen und Lösungen für resiliente Elektronik. Infineon beispielsweise adressiert das Thema der Cyber-Resilienz unter anderem mit seinen „Optiga“-Sicherheitsbausteinen für Embedded Security. Renesas bietet im Kontext sicherer, vernetzter Geräte vor allem seine sicheren „RA“-Mikrocontroller an, einschließlich isolierter kryptografischer Operationen, sicherer Schlüsselspeicherung, Arm TrustZone®-Technologie und Schutzmaßnahmen gegen Seitenkanalangriffe. Texas Instruments ergänzt das Produktspektrum mit seinen AM263x-Sitara-MCUs und implementiert unter anderem Secure Boot, kryptografische Schlüssel sowie ein Hardware-Security-Modul.

electronica als Plattform für resiliente Elektronik

Auch das Rahmenprogramm der electronica widmet sich dem Thema der Cyber-Resilienz, unter anderem im Cyber Security Forum sowie in einer Vortrags- und Workshop-Reihe zum Cyber Resilience Act. Branchenexperten geben dort Einblicke in aktuelle Technologien sowie praktische Ansätze und Strategien für resiliente Elektronikprodukte. Mit diesem Rahmen bietet die electronica 2026 Entwicklern, technischen Entscheidern und CEOs eine konkrete Orientierung, um ihr Unternehmen resilienter gegen Cyberangriffe aufzustellen.

Diese Pressemitteilung inklusive Bildmaterial steht auch zum Download im electronica Newsroom bereit.

Über die electronica
Die electronica ist der wichtigste internationale Branchentreffpunkt der Elektronikindustrie. Als Weltleitmesse präsentiert sie die ganze Bandbreite an Technologien, Produkten und Lösungen der Elektronik und bringt Experten und Anwender aus aller Welt zusammen. Das umfangreiche Rahmenprogramm mit hochkarätig besetzten Konferenzen und praxisorientierten Foren vermittelt tiefe Einblicke in neueste Trends von der Forschung bis zur Anwendung und behandelt aktuelle gesellschaftliche Themen. Die nächste electronica findet vom 10. bis 13. November 2026 auf dem Gelände der Messe München statt.

electronica weltweit
Neben der electronica organisiert die Messe München die electronica China, die electronica India North and South, die SmartTech Asia und die electronicAsia. Zum Netzwerk an Elektronikmessen zählen zudem die productronica in München, die productronica China, die productronica India North and South sowie die LOPEC.

Messe München
Als einer der bedeutendsten Messeveranstalter zeigt die Messe München auf ihren weltweit rund 90 Fachmessen die Welt von morgen. Das Portfolio umfasst Fachmessen für Investitions- und Konsumgüter ebenso wie für neue Technologien. Darunter 14 Weltleitmessen wie bauma, BAU, IFAT oder electronica, Kooperationsveranstaltungen wie die IAA MOBILITY und zahlreiche Gastveranstaltungen. Mit einem internationalen Netzwerk von Beteiligungsgesellschaften und Auslandsvertretungen ist die Messe München weltweit aktiv. Zusammen mit ihren rund 1.200 Mitarbeitenden im Konzern organisiert sie Fachmessen in China, Indien, Brasilien, Südafrika, Türkei, Singapur, Vietnam, Hongkong, Thailand, den USA und in Saudi-Arabien. Rund 150 Veranstaltungen jährlich, ziehen im In- und Ausland über 50.000 Aussteller und rund drei Millionen Besucher an. Damit ist die Messe München ein wichtiger Wirtschaftsmotor, der Kaufkrafteffekte in Milliardenhöhe auslöst.