# TÜV Rheinland: Anforderungen an Cybersicherheit wachsen stark

Zunehmend ausgeklügelte Cyberangriffe und wachsende Zahl von Sicherheitslücken / Komplexe Vorschriftenwelt: CRA, NIS-2, RED / Expertise von TÜV Rheinland gibt Orientierung / Interviews mit Fachleuten unter [www.tuv.com/cybersecurity-trends](https://www.tuv.com/landingpage/en/cybersecurity-trends_2024/meta-navigation/expert-interviews/?wt_mc=Mailing.Email.no-interface.CW25_I07_TRENDS.CW25_I07_TRENDS01_NL.textlink.&cpid=CW25_I07_TRENDS01_NL)

**Köln, 20. Mai 2025.** Neue, immer komplexere Vorschriften, zunehmend ausgeklügelte Cyberangriffe und eine wachsende Zahl von Sicherheitslücken – das ThemaCybersicherheit setzt Unternehmen zunehmend unter Druck. Fachleute von TÜV Rheinland geben nun in [Experteninterviews Orientierung zu diesen drei wesentlichen Cybersecurity-Trends](https://www.tuv.com/landingpage/en/cybersecurity-trends_2024/meta-navigation/expert-interviews/?wt_mc=Mailing.Email.no-interface.CW25_I07_TRENDS.CW25_I07_TRENDS01_NL.textlink.&cpid=CW25_I07_TRENDS01_NL) und zeigen Ansätze auf, die zu einer wirksamen Strategie für mehr Cybersicherheit führen.

**CRA, NIS-2, RED: Komplexe Vorschriftenwelt für Unternehmen**

Beispiel regulatorische Anforderungen: Die Funkanlagenrichtlinie (Radio Equipment Directive, RED) der Europäischen Union wird am 1. August 2025 gesetzlich verpflichtend um Anforderungen zur Cybersicherheit erweitert. Ab dann müssen in der EU verkaufte Geräte mit eingebauter Funktechnologie die RED-Vorgaben zur Cybersicherheit einhalten. Hinzu kommen die zweite EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-2) und der Cyber Resilience Act (CRA), die eine immer größere Zahl von Unternehmen und Produkten betreffen. „Global aufgestellte Unternehmen müssen außerdem unterschiedliche Vorschriften harmonisieren. Das ist eine besonders große Herausforderung, da einige Länder wie die USA eher auf risikobasierte Ansätze setzen, während in der EU oft strengere Sicherheitsanforderungen und Meldepflichten gelten“, erklärt Felix Brombach, Practice Leader für OT-Sicherheit bei TÜV Rheinland.

**Grundlegende Fehler immer noch verbreitet**

Auch Cyberangriffe werden zunehmend komplexer. So war 2024 unter Cyberkriminellen die Mehrfacherpressung weit verbreitet: Angreifer beschränken sich nicht mehr nur auf die Verschlüsselung von Daten, sondern drohen auch mit der Freigabe sensibler Informationen, wenn kein Lösegeld gezahlt wird. „Angesichts der Bedrohungen sollten Unternehmen einige grundlegende Fehler unbedingt vermeiden, die wir immer noch beobachten – etwa unzureichende Backups, unzureichende Schulung von Mitarbeitenden, veraltete Systeme, nicht vorhandene Störfallpläne oder die Zahlung von Lösegeld“, berichtet David Allen, Teamleiter für Cybersecurity bei TÜV Rheinland.

**Immer mehr Angriffspunkte**

Neben der Komplexität beschäftigt die IT-Abteilungen von Unternehmen auch die immer weiter steigende Zahl von potenziellen Angriffspunkten für Cyberkriminelle. So erhöhen die zunehmende Vernetzung von Geräten des Internets der Dinge (IoT), Cloud-Dienste, dezentrale Netzwerke und die Nutzung von KI die Sicherheitsrisiken. Branchen wie das Gesundheitswesen, der Finanzsektor und das Bildungswesen sind dabei besonders gefährdet, meint Massimiliano Latini, Experte für Cybersicherheit bei TÜV Rheinland: „Organisationen sind gezwungen, ihre IT-Sicherheitsstrategien entsprechend anzupassen – etwa durch proaktive Sicherheitsmaßnahmen und die Automation von Sicherheitsprozessen.“

Weitere Informationen in den unter [www.tuv.com/cybersecurity-trends](https://www.tuv.com/landingpage/en/cybersecurity-trends_2024/meta-navigation/expert-interviews/?wt_mc=Mailing.Email.no-interface.CW25_I07_TRENDS.CW25_I07_TRENDS01_NL.textlink.&cpid=CW25_I07_TRENDS01_NL) veröffentlichten Interviews.

*Die Welt zu einem sicheren Ort machen – und das seit mehr als 150 Jahren: Dafür steht TÜV Rheinland als einer der weltweit führenden Prüfdienstleister mit einem Jahresumsatz von mehr als 2,7 Milliarden Euro und rund 26.000 Mitarbeitenden in gut 50 Ländern. Die hoch qualifizierten Expertinnen und Experten prüfen technische Anlagen und Produkte, begleiten Innovationen und gestalten den Wandel zu mehr Nachhaltigkeit mit. Sie trainieren Menschen in zahlreichen Berufen und zertifizieren Managementsysteme nach internationalen Standards. Mit besonderer Expertise in Mobilität, Energieversorgung, Infrastruktur und vielen weiteren Bereichen sichert TÜV Rheinland unabhängig Qualität, insbesondere bei innovativen Technologien wie grünem Wasserstoff, künstlicher Intelligenz oder automatisiertem Fahren – und ermöglicht so eine sichere und lebenswerte Zukunft. Seit 2006 ist TÜV Rheinland Mitglied im Global Compact der Vereinten Nationen für mehr Nachhaltigkeit und gegen Korruption. Hauptsitz des Unternehmens ist Köln, Deutschland. Website:* [*www.tuv.com*](http://www.tuv.com)

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

Ihr Ansprechpartner für redaktionelle Fragen:

Pressestelle TÜV Rheinland, Tel.: +49 2 21/8 06-21 48

Die aktuellen Presseinformationen sowie themenbezogene Fotos und Videos erhalten Sie auch per E-Mail über contact@press.tuv.com sowie im Internet: [www.tuv.com/presse](http://www.tuv.com/presse).