

Pressemitteilung



Mehr Wert.
Mehr Vertrauen.

Cyber-Resilienz stärken

13. Februar 2025

Mit TÜV SÜD NIS 2- und DORA-Konformität erreichen

München. Verlust sensibler Daten, enormer finanzieller Schaden oder die Störung der öffentlichen Ordnung – Cyberangriffe auf Kritische Infrastrukturen und Finanzinstitute können erhebliche gesellschaftliche Auswirkungen haben. Die Europäische Union hat deshalb die NIS2-Richtlinie und den Digital Operational Resilience Act (DORA) eingeführt, um diese zu minimieren. Beide Regulierungen zielen darauf ab, Cyber-Sicherheitsstandards zu harmonisieren, die Widerstandsfähigkeit zu verbessern und die Einhaltung in allen Mitgliedstaaten durchzusetzen. TÜV SÜD veranstaltet dazu am 25. Februar ein [Webinar](#).

„Schätzungen gehen davon aus, dass EU-weit mehr als 100.000 Organisationen allein von NIS-2 betroffen sind“, meint Richard Skalt, Advocacy Manager Cybersecurity Office bei TÜV SÜD. „Selbst auf Organisationen mit Firmensitz außerhalb der EU können diese Regulierungen Auswirkungen haben. Auch wenn sich in vielen Mitgliedsstaaten die Umsetzung verzögert, stellen sich viele Unternehmen die Frage, wie sie sicherstellen können, dass sie die gesetzlichen Vorgaben erfüllen und mithilfe welcher Maßnahmen sie ihre Cyber-Resilienz nachhaltig verbessern können.“

Was ist DORA?

Der Digital Operational Resilience Act kommt seit dem 17. Januar dieses Jahres voll zur Anwendung. Er betrifft alle Finanzinstitute in der EU und deren kritische IT-Service-Provider. DORA fordert bestimmte Risikomanagementmaßnahmen, wie beispielsweise ein Risk Assessment durch Dritte. Auch IT-Service-Provider mit Sitz außerhalb der EU können durch die nationalen Aufsichtsbehörden aufgefordert werden, eine Niederlassung in der EU zu eröffnen. Organisationen, die die Vorgaben nicht erfüllen, müssen mit hohen Geldstrafen rechnen.

Was ist NIS2?

Die europäische Richtlinie zur Sicherheit von Netz- und Informationssystemen, kurz NIS-2, verlangt, dass Organisationen in kritischen Sektoren geeignete Sicherheitsmaßnahmen

ergreifen, um die Risiken für ihre Systeme zu minimieren. Eine Nichteinhaltung kann verschiedene negative Folgen – wie finanzielle Strafen, Cybersecurity-Risiken oder Probleme bei Geschäftsbeziehungen – mit sich ziehen. Betroffen sind Unternehmen in kritischen Bereichen wie der Energieversorgung, im Gesundheitswesen oder Transport.

Die Rolle von ISO-Standards

Viele der von NIS 2 und DORA betroffenen Organisationen sind bereits nach den international weit verbreiteten Cybersicherheits-Standards ISO 27001 und IEC 62443 zertifiziert. ISO 27001 hilft bei der Einrichtung und Aufrechterhaltung eines effektiven Informationssicherheits-Managementsystems (ISMS). In Unternehmen, in denen OT-Sicherheit eine wichtige Rolle spielt, ist auch die internationale Normenreihe IEC 62443 relevant.

„ISO-Standards helfen Unternehmen bei der Erfüllung der Vorgaben von NIS2 und DORA“, meint Skalt. „ISO 27001-zertifizierte Unternehmen müssen beispielsweise ein effektives Risikomanagement von Lieferanten und Dienstleistern nachweisen, wie es in NIS-2 gefordert wird.“

Das TÜV SÜD Webinar „Ensuring Cyber Resilience – Navigating NIS2 and DORA Compliance Across Critical Sectors“ findet am 25. Februar um 10 Uhr statt. Eine Anmeldung ist unter tuvsud.com/en-in/resource-centre/webinar/nis2 möglich.

Pressekontakt:

TÜV SÜD AG Unternehmenskommunikation Westendstraße 199 80686 München	Laura Albrecht Telefon +49 89 5791-2935 E-Mail laura.albrecht@tuvsud.com Internet tuvsud.com/presse
---	---

Im Jahr 1866 als Dampfkesselrevisionsverein gegründet, ist TÜV SÜD heute ein weltweit tätiges Unternehmen. Mehr als 28.000 Mitarbeitende sorgen an über 1.000 Standorten in rund 50 Ländern für die Optimierung von Technik, Systemen und Know-how. Sie leisten einen wesentlichen Beitrag dazu, technische Innovationen wie Industrie 4.0, autonomes Fahren oder Erneuerbare Energien sicher und zuverlässig zu machen. tuvsud.com/de