Pressemitteilung

Mehr Wert.
Mehr Vertrauen.

Mit TÜV SÜD NIS-2-Konformität erreichen 22. Oktober 2024

Vier Komponenten für ein strategisches, maßgeschneidertes und kontinuierliches Cybersecurity-Programm

München. Die neue 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. TÜV SÜD hilft Organisationen, ihre NIS-2-Compliance sicherzustellen und ein strategisches, maßgeschneidertes und kontinuierliches Cybersecurity-Programm zu entwickeln. Auch Unternehmen, die nicht von NIS-2 betroffen sind, können so ihre Widerstandsfähigkeit stärken.

„NIS-2 ist das Cybersecurity-Thema des Jahres. Doch die Frage, ob ein Unternehmen die Vorgaben erfüllt, ist nicht immer leicht zu beantworten“, meint Sudhir Ethiraj, Global Head of Cybersecurity Office (CSO) und CEO Business Unit Cybersecurity Services bei TÜV SÜD. „TÜV SÜD hilft als neutraler Partner dabei, die Anforderungen der Richtlinie zu verstehen und sie umzusetzen. Organisationen, die nicht nur NIS-Konformität erreichen, sondern auch ihre allgemeine Cyber-Resilienz stärken wollen, bieten wir in vier Bereichen Unterstützung.“

Risk Assessments und Gap Analysen zur Erfassung des Status-Quos

Risk Assessments und Gap Analysen decken Schwachstellen in bereits etablierten Cybersecurity-Maßnahmen auf. Besonderes Augenmerk liegt dabei auf den Bereichen Incident Response, allgemeines Risikomanagement und Sicherheit der Lieferkette, die gemäß NIS-2 besonders relevant sind. Organisationen können mithilfe dieser Maßnahmen ihr Cyber-Risiko bewerten.

Entwicklung von Richtlinien und Prozessen

Die Definition relevanter, unternehmensspezifischer Richtlinien ist die Grundlage für alle weiteren Maßnahmen. Dazu zählt auch die Entwicklung von Notfallplänen und Maßnahmen zur Absicherung der Lieferkette, um im Ernstfall schnell und effektiv reagieren zu können. Die nötigen finanziellen, personellen und technischen Ressourcen bleiben dabei stets im Blick.

Interne Audits

Mittels interner Audits können die bislang ergriffenen Maßnahmen – auch im Hinblick auf die Supply Chain – regelmäßig überprüft werden. Lücken und Schwachstellen, die bei Audits und Vorfallüberprüfungen gefunden werden, müssen umgehend behoben und die unternehmensspezifischen Richtlinien und Prozesse anhand dieses Feedbacks und im Hinblick auf die sich wandelnde Bedrohungslandschaft kontinuierlich verbessert werden.

Schulungen

Der Mensch gilt als das Haupteinfallstor für Cyberkriminelle. Deshalb ist es wichtig, die Mitarbeitenden kontinuierlich zu schulen. Dabei sollte auch auf die unternehmenseigenen Richtlinien eingegangen werden, die im Hinblick auf NIS-2-Compliance entwickelt wurden. Auch Partner in der Lieferkette können durch regelmäßige Schulungsangebote mit ins Boot geholt werden. Daneben sind laut NIS-2 auch Managementverantwortliche verpflichtet, sich mit dem Risikomanagement im Bereich der Sicherheit in der Informationstechnik vertraut zu machen.

Weiterführende Informationen:

- NIS-2-Assessments von TÜV SÜD
- Schulungsangebot der TÜV SÜD Akademie zur IT-Sicherheit
- Weiterbildung für Managementverantwortliche

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