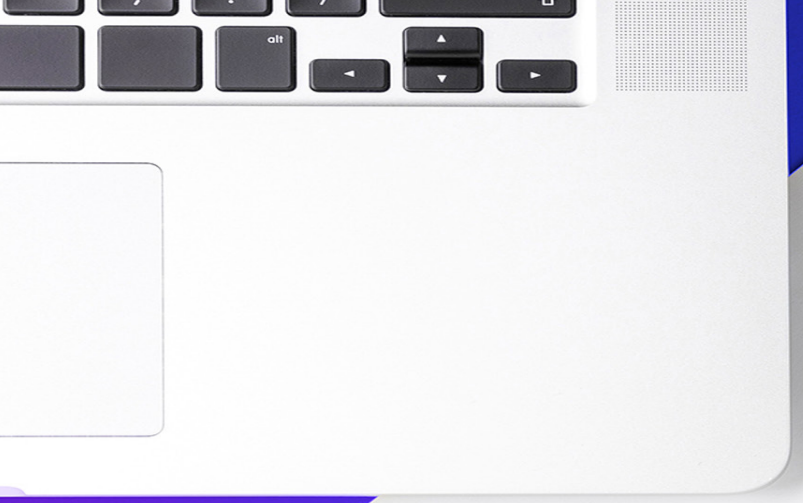
NIS 2: Warum alle Händler die neue Cyber-sicherheitsrichtlinie kennen sollten

Expertenartikel

Cybersecurity



Technologie ist im Handel mittlerweile maßgeblich bestimmend in der Kundenbeziehung und in den Betriebsabläufen. Daher wird der Handel zunehmend zu einem Ziel von Cyberangriffen und Cyberkriminellen. Laut einer KPMG-Studie aus dem Jahr 2023 haben 78 Prozent der Einzelhändler einen Anstieg von Cyberangriffen verzeichnet, was das hohe Risiko deutlich macht.

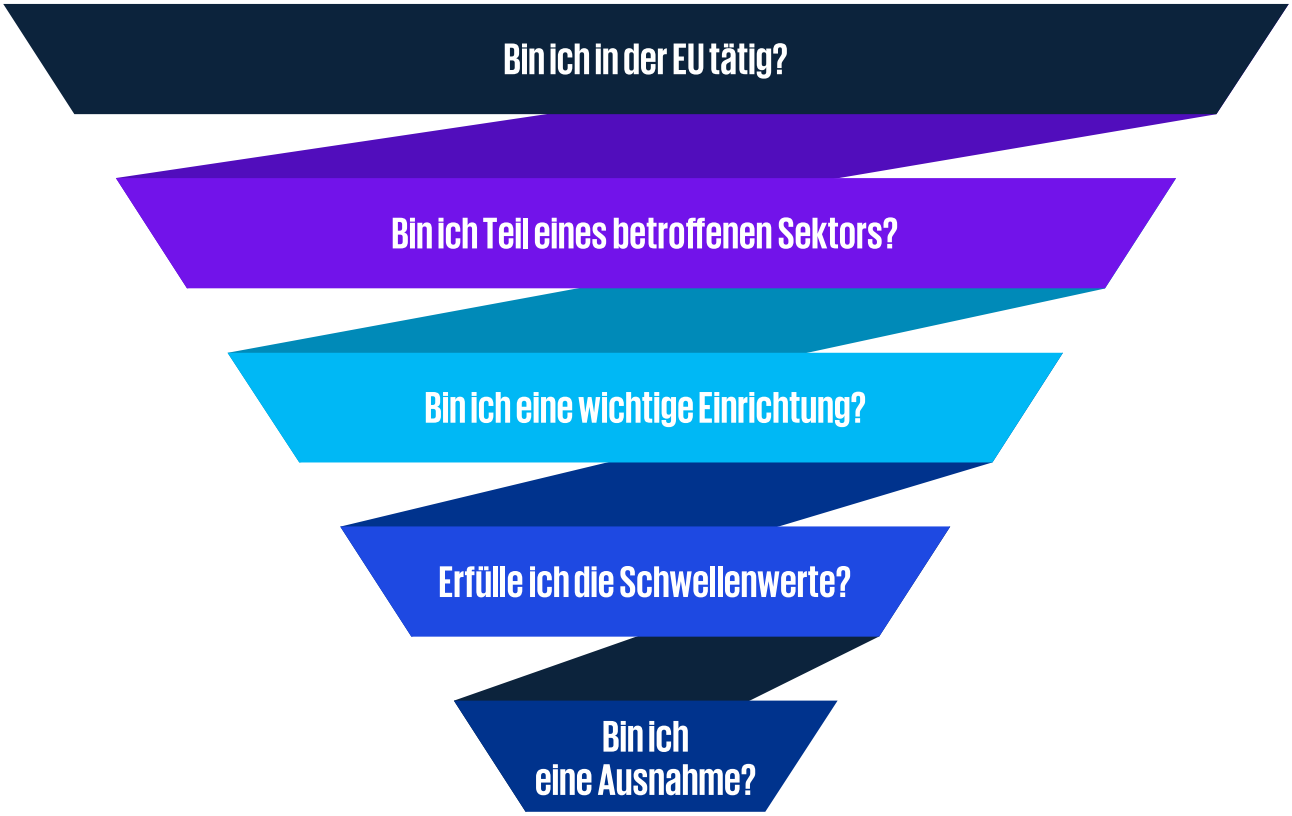
Quelle: KPMG Newsletter Retail Sales Monitor, Ausgabe 2 | 2023

Die gute Nachricht: Viele Händler reagieren darauf und beginnen mit einer der effektivsten Maßnahmen, der Sensibilisierung der Mitarbeitenden und der Durchführung von IT-Sicherheitsschulungen.

Kein Händler, unabhängig von Größe und Branche, sollte das Thema Cybersicherheit ignorieren. Ob es darum geht, Zahlungsdaten an einem Selbstbedienungskiosk zu schützen, die Integrität von Online-Transaktionen zu sichern oder Kundendaten über die gesamte Handelskette hinweg zu schützen – der Bedarf an umfassenden Cybersicherheitsmaßnahmen war noch nie so dringend. Händler müssen ihr Sicherheitskonzept weiterentwickeln und kontinuierlich verbessern, indem sie in Strategien und Technologien investieren, die diesen digitalen Bedrohungen effektiv entgegenwirken können.

Die NIS 2-Richtlinie hebt die Cybersicherheit in der Europäischen Union (EU) auf ein neues Level. Ihr Ziel ist es, ein einheitliches Schutzniveau für Netzwerk- und Informationssicherheit zu schaffen. Im Vergleich zur bereits 2016 verabschiedeten NIS-Richtlinie, welche sich auf die Cybersicherheit von kritischen Infrastrukturen (KRITIS) konzentrierte, hat die NIS 2-Richtlinie ihren Anwendungsbereich erweitert. Sie umfasst nun nicht nur Betreiber kritischer Anlagen, sondern „besonders wichtige Einrichtungen“ (Großunternehmen bestimmter Sektoren, einige Unternehmen unabhängig ihrer Größe und Betreiber kritischer Anlagen) und „wichtige Einrichtungen“ (Großunternehmen und mittlere Unternehmen in vielen Sektoren). Seit dem 16. Januar 2023 ist die NIS 2-Richtlinie in Kraft und soll bis März 2025 in deutsches nationales Recht umgesetzt werden. Einrichtungen, welche die Anforderungen nicht erfüllen, drohen Geldstrafen von bis zu 10 Millionen Euro oder zwei Prozent des weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist. Für Führungskräfte im Handel ist dies nicht nur eine Frage der Compliance – es geht darum, finanzielle und rechtliche Konsequenzen zu vermeiden. Die zentrale Frage lautet nun: Wie können Sie als Händler herausfinden, ob die NIS 2-Richtlinie für Sie relevant ist?

Beantworten Sie diese fünf Fragen, um herauszufinden, ob NIS 2 Ihr Unternehmen betrifft:



Quelle: KPMG in Deutschland, 2025

Überlegen Sie zunächst, ob Ihr Unternehmen in der EU tätig ist und zu welchem Sektor es gehört. Für Händler könnten Sektoren wie z.B. „Anbieter digitaler Dienste", „Produktion, Verarbeitung und Vertrieb von Lebensmitteln", „Digitale Infrastruktur", „Finanzwesen" relevant sein. Bewerten Sie, ob Ihr Unternehmen als „besonders wichtig" oder „wichtig" eingestuft wird, basierend auf seiner Rolle in der kritischen Infrastruktur und den potenziellen Auswirkungen eines Ausfalls. Überprüfen Sie, ob Ihr Unternehmen die Größenkriterien hinsichtlich Mitarbeiterzahl und Umsatz für diese Einstufungen erfüllt. Berücksichtigen Sie schließlich etwaige Ausnahmen, wie z. B. die Einstufung als kleines oder mittleres Unternehmen, die Ihr Unternehmen von den NIS 2-Anforderungen befreien könnten.

NIS 2-Ready: Wie Ihr Unternehmen sich jetzt vorbereiten kann

Warten Sie nicht, bis das nationale Gesetze in Kraft tritt – beginnen Sie noch heute mit der Umsetzung der NIS 2-Anforderungen. Die Implementierung geeigneter Maßnahmen auf der Grundlage einer umfassenden Risikobewertung ist entscheidend. Setzen Sie auf eine ganzheitliche, bedrohungsorientierte Strategie, um Sicherheitsvorfälle zu verhindern oder deren Auswirkungen zu minimieren.

So könnten Sie beginnen:

Bewerten Sie Ihre aktuellen IT-Sicherheitsmaßnahmen und identifizieren Sie Schwachstellen, um die NIS 2-Compliance zu gewährleisten. Basierend auf dem entsprechenden Geschäftsmodell sollten Sie sich auf diese Schlüsselbereiche konzentrieren:

Führen Sie umfassende Risikoanalysen durch, implementieren Sie Backups, testen Sie Ihre Systeme regelmäßig und nutzen Sie moderne Verschlüsselungstechnologien, um Kundendaten und Transaktionsinformationen effektiv zu schützen. Etablieren Sie Protokolle zur Meldung von Sicherheitsvorfällen an eine zuständige Stelle und informieren Sie Partner und Stakeholder bei gravierenden Ausfällen umgehend. Achten Sie zudem darauf, alle Registrierungspflichten einzuhalten, um potenzielle Strafen zu vermeiden.

Das Management muss die Umsetzung dieser Maßnahmen aktiv überwachen. Schulen Sie Ihr Management und Ihre Mitarbeitenden in den Bereichen Datenschutz, Cybersicherheit und Technologie.

Die Umsetzung dieser Maßnahmen wird nicht nur die Compliance sicherstellen, sondern auch Ihre Abwehr gegen sich entwickelnde

Cyberbedrohungen stärken. Mit dem Trend der Digitalisierung, insbesondere in Zahlungssystemen, sind starke Cybersicherheitsmaßnahmen von entscheidender Bedeutung. Für den Handel sind insbesondere die folgenden Cyber-Trends wichtig:

- Schutz von Zahlungsdaten
- Sicherung von Online-Marktplätzen und -Transaktionen
- Schutz von Kundendaten über die gesamte Handelskette hinweg

Die NIS-2-Richtlinie verlangt ein hohes Maß an Cybersicherheit in der EU. Prüfen Sie Ihre Relevanz im Rahmen von NIS-2, indem Sie Ihren operativen Tätigkeitsbereich, die sektorspezifische Einstufung sowie mögliche Auswirkungen auf die kritische Infrastruktur analysieren. Ein proaktiver Umgang mit den Anforderungen der NIS-2-Richtlinie ermöglicht es Ihnen, Cyberrisiken effektiv zu minimieren, sensible Kundendaten zu schützen und das Vertrauen Ihrer Kunden in einer zunehmend digitalen Marktlandschaft zu stärken. Handeln Sie jetzt, um sicherzustellen, dass Ihr Unternehmen NIS-2-konform ist und in der digitalen Ära die Nase vorn behält.

Letztlich kann es sich kein Händler leisten, das Thema Cybersicherheit zu vernachlässigen. Indem Sie die NIS-2-Anforderungen frühzeitig umsetzen, sichern Sie nicht nur Ihre Systeme, sondern vor allem das Fundament Ihres Erfolgs: Das Vertrauen Ihrer Kunden und Geschäftspartner.

Kontakt

KPMG AG
Wirtschaftsprüfungsgesellschaft

Barbarossaplatz 1a
50674 Köln

Markus Limbach
Partner
T +49 221 2073-5833
mlimbach@kpmg.com

Markus Limbach ist Partner im Bereich Cyber Security & Resilience bei der KPMG AG und berät nationale und internationale Organisationen in den Bereichen Cyber Security, Informationssicherheit und Business Continuity & Resilience Management. Mit umfassender Expertise unterstützt er seine Kunden dabei, sich vor Cyberbedrohungen zu schützen und eine hohe Resilienz gegenüber digitalen Angriffen aufzubauen.

www.kpmg.de

www.kpmg.de/socialmedia