Südtiroler Wirtschaftszeitung — Nr. 27 | 25 — Freitag, 11. Juli 2025

Chefsache Cybersicherheit

CYBERSICHERHEIT (3) – Wer nicht sichert, der haftet. Die neue EU-Richtlinie NIS2 verpflichtet Unternehmen dazu, Cybersicherheit strategisch zu verankern. Was Südtiroler Betriebe jetzt tun müssen – und warum Führungskräfte dabei eine Schlüsselrolle spielen.

Bozen – Vom IT-Keller ins Vorstandsbüro. Cybersicherheit ist nicht mehr nur ein IT-Thema – mit NIS2 rückt sie direkt auf den Schreibtisch der Chefetage.

Die EU-Richtlinie NIS2 (Network and Information Security Directive) zielt auf den Schutz kritischer Geschäftsprozesse vor Cyberangriffen und die Prävention von Sicherheitsvorfällen ab. Sie definiert die Anforderungen und Verantwortlichkeiten neu und umfassend: Nicht nur die IT-Abteilung ist gefragt, sondern die gesamte Organisationsstruktur des Unternehmens – von internen Abläufen bis hin zum Umgang mit Lieferanten.

Seit April 2025 wissen registrierte Südtiroler Unternehmen, ob sie unter die NIS2 fallen. Bereits ab Januar 2026 müssen erste Anforderungen umgesetzt sein, insbesondere die Meldung von Sicherheitsvorfällen. Bis Oktober 2026 ist die vollständige Umsetzung Pflicht.

Foto: Shutterstock AI

Was ist konkret für NIS2 zu tun?

Unternehmen müssen ein strukturiertes Risikomanagement etablieren, Abläufe zur Bewältigung von Sicherheitsvorfällen inklusive Meldepflichten einrichten, diverse technische und organisatorische Vorkehrungen treffen sowie Verantwortlichkeiten definieren.

Drei zentrale Handlungsfelder für Entscheider:innen:

1. Strategische Steuerung und Integration: NIS2 verlangt die Integration der Cybersicherheit in die Unternehmensstrategie und -kultur sowie in alle internen Abläufe. Die Steuerung und Entscheidungsgrundlage erfolgt durch Nachweise, Kennzahlen, Berichterstattung sowie letztendlich durch die Übernahme der unternehmerischen Risiken.
2. Risikomanagement verankern: Die Geschäftsführung ist verpflichtet, ein System zur Erkennung und Bewertung von Cyber-Risiken einzuführen und regelmäßig auf Wirksamkeit zu prüfen. Zentral ist der Schutz wichtiger Vermögenswerte (Assets) u.a. Gebäude, Maschinen, Mitarbeiter, Know-how, Geschäftsprozesse, primäre Lieferanten und deren Daten.
3. Vorfallmanagement organisieren: Unternehmen müssen definieren, was im Ernstfall zu tun ist – also bei einem Cyberangriff, Systemausfall oder Datenabfluss. Dazu gehört die Einrichtung eines Meldesystems mit klaren Reaktionszeiten, Zuständigkeiten und Kommunikationswegen inkl. Meldepflichten an Behörden, Kundinnen und Kunden.

Delegieren ist erlaubt, die Verantwortung bleibt bei der Führung

Die wohl gravierendste Änderung: Verwaltungs- und Leitungsorgane sind persönlich verantwortlich. Sie müssen künftig aktiv und nachweisbar die geforderten Maßnahmen steuern, kontrollieren und die Verantwortung für die Umsetzung übernehmen.

Verstöße können zivil- und strafrechtliche Konsequenzen nach sich ziehen – inklusive Geldstrafen bis zu zehn Million Euro oder zwei Prozent des Jahresumsatzes (Art. 34 NIS2).

Die Umsetzung der NIS2 erfolgt idealerweise in fünf Phasen:

1. Bestandsaufnahme (Gap-Analyse): Wo steht das Unternehmen aktuell? Welche Anforderungen sind erfüllt? Wo gibt es Lücken? Eine strukturierte Analyse bildet die Grundlage für alle weiteren Schritte.
2. Governance und Verantwortlichkeiten festlegen: Wer übernimmt welche Rolle? Wer steuert und wer setzt um? Die Ernennung eines NIS2-Koordinators hilft, Zuständigkeiten zu bündeln, effizient umzusetzen und permanent zu verankern.
3. Maßnahmen umsetzen (technisch und organisatorisch): Dazu zählen technische Maßnahmen – u.a. Backup, Patching, Netz- und Zugangskontrollen – bei IT, sowie OT (Industrie 4.0) und IoT (u.a. Haustechnik) ebenso wie organisatorische Aspekte wie Schulungen, Lieferantensteuerung, Erstellung von Richtlinien, physische Zugangskontrollen und Notfallpläne.
4. Vorfallmanagement und Meldewege vorbereiten: Unternehmen müssen in der Lage sein, Sicherheitsvorfälle innerhalb von 24 Stunden zu melden. Ein funktionierender Ablaufplan ist daher Pflicht – samt Reaktionsplan und Ansprechpartnern. Analog zur Feuerwehr gilt: Regelmäßig üben!
5. Kontrollmechanismen und Nachweise etablieren: NIS2 verlangt regelmäßige Kontrollen und die Nachweisbarkeit aller Maßnahmen – nicht nur gegenüber Behörden, sondern zunehmend auch gegenüber Kundschaft, Partnerinnen und Partnern oder Versicherungen.

Integration in bestehende Systeme spart Aufwand

NIS2 lässt sich effizient in bestehende Managementsysteme wie ISO 9001 oder Food Standard integrieren. Gemeinsame Prozesse wie Risikomanagement, Audits und Schulungen bieten klare Synergien und reduzieren den Aufwand beträchtlich.

Die ISO 27001 ist eine praxisbewährte Alternative zur Umsetzung von NIS2 – sie erfüllt alle wesentlichen Anforderungen der Richtlinie und bietet darüber hinaus klare Strukturen für kontinuierliche Verbesserung und regelmäßige Kontrolle. Durch die Zertifizierung schaffen Unternehmen Vertrauen bei Kundinnen und Kunden, reduzieren Anfragen als Lieferant und bieten Wettbewerbsvorteile etwa bei Ausschreibungen.

Fünf Aufgaben für die Geschäftsführung

Cybersicherheit ist nicht nur eine technische, sondern eine strategische Aufgabe. Sie gehört auf die Agenda der Geschäftsleitung – und das verbindlich und überprüfbar.

Die wichtigsten Handlungsfelder für CEOs und Vorstände lassen sich in fünf Kernthemen bündeln:

1. Verantwortlichkeiten definieren: Die Geschäftsleitung muss klare Zuständigkeiten für Informationssicherheit schaffen – intern oder mithilfe externer Spezialisten. Elementar ist die Benennung eines NIS2-Beauftragten, der als zentrale Schnittstelle agiert.
2. Assets ermitteln und Risiken bewerten: Ohne eine fundierte Analyse der bestehenden IT- und Prozessrisiken bleibt jedes Sicherheitskonzept lückenhaft. Eine strukturierte Risikoanalyse ist daher der erste operative Schritt.
3. Ressourcen freigeben: Cybersicherheit braucht nicht nur Strategie, sondern auch Budget. Ob für technische Schutzmaßnahmen, für Schulungen oder für die Integration in bestehende Managementsysteme – ohne gezielte Investitionen bleibt NIS2 ein Papiertiger.
4. Maßnahmen initiieren: Sicherheitskonzepte, Vorfallmanagement, Schulungen, interne Prozesse – sie alle müssen nicht nur geplant, sondern zügig angestoßen werden. Entscheidend ist die Balance zwischen Pragmatismus und Sorgfalt.
5. Fortschritt regelmäßig prüfen: NIS2 verlangt laufende Kontrolle, Nachweise und ggf. Nachbesserung. Geschäftsleitungen sollten sich daher regelmäßig berichten lassen, ob die Sicherheitsstrategie funktioniert und ob sie neuen Bedrohungen standhält.

Umsetzung NIS2-Maßnahmen bis Januar 2026

Die ersten gesetzlichen Verpflichtungen treten bereits in einem halben Jahr in Kraft. Eine solide Basis für Cybersicherheit muss bis dahin etabliert sein; Vorfälle müssen aufgezeichnet und gemeldet werden. Im Fall von Versäumnissen drohen Sanktionen bis hin zur persönlichen Haftung der Geschäftsleitung.

Wer vorbereitet ist, schützt seine essenziellen Unternehmenswerte und Produktionsabläufe, gewinnt an Vertrauen und steigert seine Widerstandskraft und Wettbewerbsfähigkeit.

Fazit: Unternehmen jetzt cybersicher machen

Der Appell an alle Entscheider:innen lautet daher klar: Jetzt ist die Zeit zu handeln und das Thema Cybersicherheit selbst in die Hand zu nehmen. Wer die Herausforderung annimmt, schützt nicht nur das eigene Unternehmen, sondern positioniert es für die Zukunft.

Der Projektplan für NIS2

Ein strukturiertes Vorgehen in Form eines Projektplans hilft den Überblick bei NIS2 zu behalten und die geforderten Maßnahmen termingerecht umzusetzen

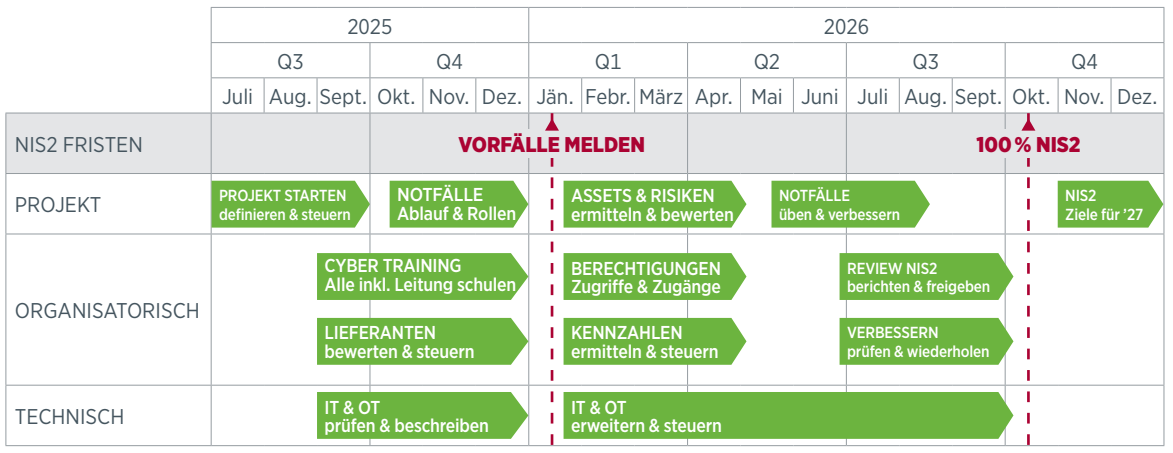

Foto: Silbersalz.photo

Foto: Alfred Tschager

Christian Feichter und Stefan Laimer

DIE AUTOREN Christian Feichter ist Senior Berater für IT und Cybersicherheit und Zertifizierter Auditor ISO 27001 und TISAX. **Stefan Laimer** ist Head of Security Operations und Security Manager bei Konverto.