SecuCheck-IQ

Cyber Health Report

Compliance-Status-Bewertung nach NIS2 und ISO 27001 (Best Practices)

Meines

Erstellt am 10. Juni 2026

Executive Summary

Cyber Health Score

38 / 100

Ihr Unternehmen hat grundlegende Sicherheitsmaßnahmen, aber mehrere kritische Lücken gefährden den Geschäftsbetrieb — besonders vor dem Hintergrund, dass Sie selbst Kreditkartendaten verarbeiten und Gesundheitsdaten speichern. Am dringendsten: veraltete Systeme ohne Updates, fehlender Schutz gegen Schadsoftware, unregelmäßige Backups ohne offline-Kopie und die Selbstverarbeitung von Kartendaten. Da Sie als Zulieferer für größere Unternehmen agieren, sollten diese Punkte priorisiert werden, um Geschäftsbeziehungen nicht zu gefährden.

NIS2-Betroffenheit

Voraussichtlich mittelbar betroffen (Lieferkette)

Nach Ihren Angaben (Finanzen/Versicherung, 50–249 Mitarbeitende, 2–10 Mio € Umsatz) fällt Ihr Unternehmen nicht direkt unter NIS2, da Finanzunternehmen überwiegend über DORA reguliert werden. Als Zulieferer für größere Unternehmen sind Sie jedoch voraussichtlich mittelbar betroffen, da Ihre Auftraggeber zunehmend Sicherheitsnachweise verlangen.

Status pro Kategorie

Kategorie	Score	Status
Organisation & Verantwortung	60 / 100	Warnung
Mitarbeitende & Awareness	50 / 100	Warnung
Zugänge & Identität	65 / 100	Warnung
Daten & Verschlüsselung	30 / 100	Kritisch
Geräte, Updates & Schadsoftware	20 / 100	Kritisch
Netzwerk & Fernzugriff	75 / 100	Gut
Datensicherung & Notfall	30 / 100	Kritisch
Sicherheitsvorfälle & Meldepflicht	25 / 100	Kritisch
Dienstleister & Lieferkette	50 / 100	Warnung
Online-Shop & Zahlungsdaten	20 / 100	Kritisch

Findings

KRITISCH Geräte, Updates & Schadsoftware

Veraltete Systeme ohne Sicherheitsupdates und fehlender Schadsoftware-Schutz

Einige Geräte oder Programme erhalten keine Sicherheitsupdates mehr, und auf nicht allen Geräten ist ein aktueller Schutz gegen Schadsoftware aktiv. Dies macht Ihr Unternehmen besonders anfällig für Angriffe, die gezielt bekannte Schwachstellen ausnutzen. Bei Verarbeitung von Gesundheits- und Kartendaten kann ein erfolgreicher Angriff zu Datenverlust, Bußgeldern und einem Vertrauensverlust bei Kunden führen.

EMPFEHLUNG

Ersetzen Sie sofort alle Geräte und Programme, die keine Updates mehr erhalten (z. B. Windows 7). Installieren Sie auf allen Geräten einen aktuellen Virenschutz (z. B. Microsoft Defender, ESET, Bitdefender GravityZone). Geben Sie diesen Schritt an Ihre IT-Betreuung weiter. Aufwand: einmalig, mittel bis hoch.

KRITISCH Online-Shop & Zahlungsdaten

Selbstverarbeitung von Kartendaten im Online-Shop

Sie verarbeiten und speichern Kartendaten selbst. Dies erhöht das Risiko für Datenpannen und Compliance-Verstöße (z. B. gegen PCI-DSS) massiv. Bei einem Angriff könnten Kundendaten gestohlen werden, was zu hohen Bußgeldern und einem Verlust des Zahlungsabwicklungsrechts führen kann.

EMPFEHLUNG

Wechseln Sie umgehend zur Zahlungsabwicklung über einen spezialisierten Dienstleister (z. B. Stripe, PayPal, Mollie). Diese übernehmen die Compliance und reduzieren Ihr Risiko. Aufwand: einmalig, mittel. Beauftragen Sie Ihre IT-Betreuung mit der Umstellung.

KRITISCH Datensicherung & Notfall

Keine offline-Sicherung gegen Erpressungstrojaner

Ihre Backups werden unregelmäßig erstellt und es gibt keine Kopie, die getrennt vom Netzwerk aufbewahrt wird. Im Fall eines Erpressungstrojaners (Ransomware) könnten alle Daten — inklusive Backups — verschlüsselt werden. Ohne wiederherstellbare Daten droht ein vollständiger Geschäftsstillstand.

EMPFEHLUNG

Richten Sie sofort eine automatisierte, regelmäßige Datensicherung ein und bewahren Sie mindestens eine Kopie offline oder unveränderbar auf (3-2-1-Regel). Nutzen Sie z. B. Veeam, Acronis oder NAS-eigene Tools (Synology/QNAP). Aufwand: einmalig, mittel.

KRITISCH Daten & Verschlüsselung

Unvollständige Geräteverschlüsselung bei Gesundheitsdaten

Nur teilweise sind die Festplatten Ihrer Laptops und Rechner verschlüsselt. Bei Verlust oder Diebstahl eines unverschlüsselten Geräts könnten Gesundheitsdaten in falsche Hände geraten. Dies kann zu Bußgeldern nach DSGVO und einem Vertrauensverlust bei Kunden führen.

EMPFEHLUNG

Verschlüsseln Sie alle Geräte sofort: Windows → BitLocker (in Windows Pro enthalten), Mac → FileVault (in macOS enthalten). Geben Sie diesen Schritt an Ihre IT-Betreuung weiter. Aufwand: einmalig, niedrig.

KRITISCH Sicherheitsvorfälle & Meldepflicht

Kein klarer Plan für Sicherheitsvorfälle und fehlende Meldepflicht-Kenntnis

Es gibt nur eine grobe Vorstellung, was im Fall eines Cyberangriffs zu tun ist, und die Meldepflichten nach NIS2 sind unbekannt. Im Ernstfall könnte dies zu Verzögerungen bei der Reaktion und zu Compliance-Verstößen führen, besonders als Zulieferer für größere Unternehmen.

EMPFEHLUNG

Erstellen Sie einen einfachen Notfallplan mit klaren Verantwortlichkeiten und Meldewegen. Klären Sie, ob und wie Sie als Zulieferer von Meldepflichten betroffen sind. Nutzen Sie Mustervorlagen (z. B. von Aufsichtsbehörden). Aufwand: einmalig, niedrig.

WARNUNG Dienstleister & Lieferkette

Unvollständige Sicherheitsvereinbarungen mit IT-Dienstleistern

Nicht alle wichtigen IT-Dienstleister haben vertraglich geregelte Verantwortlichkeiten für Datenschutz und Sicherheit. Dies kann zu Lücken in der Compliance führen, besonders bei der Verarbeitung von Gesundheits- und Kartendaten.

EMPFEHLUNG

Fordern Sie von allen IT-Dienstleistern einen Auftragsverarbeitungs-Vertrag (AVV) an, der Sicherheit und Datenschutz regelt. Für lokale Dienstleister gibt es kostenlose Mustervorlagen (z. B. GDD, Aufsichtsbehörden). Aufwand: einmalig, mittel.

WARNUNG Mitarbeitende & Awareness

Unregelmäßige Schulungen zu IT-Sicherheit

Mitarbeitende werden nur einmalig oder selten geschult. Der Mensch ist das häufigste Einfallstor für Angriffe wie Phishing. Bei Verarbeitung sensibler Daten steigt das Risiko für erfolgreiche Angriffe.

EMPFEHLUNG

Führen Sie eine jährliche Online-Awareness-Schulung ein, als fertiges Paket buchbar (z. B. SoSafe, Hornetsecurity, G DATA academy). Erster Schritt: ein Angebot einholen und einen jährlichen Termin setzen. Aufwand: einmalig, niedrig.

WARNUNG Zugänge & Identität

Einige Mitarbeitende haben Administrator-Rechte auf ihren Geräten

Administrator-Rechte erhöhen das Risiko für versehentliche oder böswillige Änderungen an Systemen. Dies kann zu Sicherheitslücken oder Datenverlust führen, besonders bei gemischter Geräte-Welt.

EMPFEHLUNG

Entziehen Sie allen Mitarbeitenden, die keine Administrator-Aufgaben haben, diese Rechte. Nutzen Sie separate Konten für administrative Aufgaben. Geben Sie diesen Schritt an Ihre IT-Betreuung weiter. Aufwand: einmalig, niedrig.

Maßnahmen-Roadmap

Sortiert nach Priorität. Die Top-3 sollten zuerst angegangen werden.

#	Maßnahme	Aufwand	Wirkung	Zeitrahmen
1	Veraltete Systeme ersetzen und Schadsoftware-Schutz auf allen Geräten aktivieren	hoch	hoch	Sofort
1	Zahlungsabwicklung auf externen Dienstleister umstellen (z. B. Stripe, PayPal)	mittel	hoch	Sofort
1	Alle Geräte verschlüsseln (BitLocker/FileVault)	gering	hoch	Sofort
1	Automatisierte Backups mit offline-Kopie einrichten	mittel	hoch	1–2 Wochen
2	Einfachen Notfallplan mit Meldewegen erstellen	gering	hoch	1 Monat
2	Auftragsverarbeitungsverträge mit allen IT-Dienstleistern abschließen	mittel	mittel	1–3 Monate
3	Jährliche Awareness-Schulung für Mitarbeitende einführen	gering	mittel	3–6 Monate
3	Administrator-Rechte auf Geräten auf notwendige Personen beschränken	gering	mittel	1 Monat