Der blinde Fleck vieler Geschäftsführer: Sie haften – aber Ihre Organisation arbeitet dagegen

Viele Geschäftsführer im Mittelstand investieren derzeit in **KI-Agenten für Kundenservice**, prüfen **Automatisierung statt Neueinstellung**, beschäftigen sich mit **Retention Management, Liquiditätssicherung** oder lassen eine Unternehmensbewertung per **KMU-Rechner** durchführen. All das ist sinnvoll.

Was jedoch oft übersehen wird:

Die größte Haftung entsteht nicht durch fehlende Innovation – sondern durch scheinbar harmlose Alltagsprozesse.

„Wir nutzen doch HTTPS“ – warum dieses Argument unter NIS-2 nicht mehr trägt

Ein Klassiker aus der Praxis:

- Passwörter werden per E-Mail versendet

- Zugangsdaten stehen im GET-Parameter einer URL
- Der Einwand lautet: „Der Transport ist doch verschlüsselt (HTTPS).“

Technisch ist das korrekt.
Rechtlich und organisatorisch ist es unter NIS-2 eine Katastrophe.

Warum?

- GET-Parameter landen im Klartext:
  - in Server-Logs (access.log)
  - im Browser-Verlauf
  - in Proxy- und Firewall-Logs
    → Verstoß gegen Security by Design
- E-Mails:
  - liegen jahrelang unverschlüsselt im Postfach
  - im „Gesendet“-Ordner des Kunden
  - im Support-Postfach Ihres Unternehmens

Das Entscheidende:
Das ist kein Hackerangriff.
Das ist eine **grob fahrlässige Schwachstelle im Standardprozess.**

Unter **NIS-2** ist genau das der Punkt, an dem die **persönliche Haftung des Geschäftsführers** beginnt:

Sie hätten organisatorisch und technisch sicherstellen müssen,
dass sensible Daten nicht so verarbeitet werden.

Die „Passwort-Richtlinie“ und die TXT-Datei in der Schublade

Ein zweites, ebenso typisches Szenario:

- Der Geschäftsführer unterschreibt eine Passwort-Richtlinie
  (12 Zeichen, Sonderzeichen, Wechsel alle 90 Tage)
- Der Administrator denkt sich:
  „Das kann sich kein Mensch merken.“
- Ergebnis:

- passwords.txt
  oder der berühmte **Zettel in der Schublade**

Das eigentliche Haftungsproblem liegt **nicht beim Admin**, sondern beim Geschäftsführer.

Unter NIS-2 reicht es **nicht mehr**, Regeln zu erlassen.
Sie haben eine **Überwachungspflicht**.

Die kritische Frage des Auditors lautet dann:

„Herr Geschäftsführer, wie haben Sie technisch sichergestellt,
dass Mitarbeiter keine Passwort-TXT-Dateien anlegen können?“

Die Antwort

„Ich habe ihnen vertraut.“

ist keine Entlastung, sondern der **Beweis eines Organisationsverschuldens**.

Das eigentliche Dilemma: Unpraktische Regeln erzeugen Regelverstöße

Die Realität im Mittelstand ist klar:

- Ihre Mitarbeiter umgehen Regeln **nicht aus Böswilligkeit**,
- sondern weil sie **unpraktisch** sind.
- Gleichzeitig **haften Sie persönlich**, wenn genau diese Umgehungen zum Vorfall führen.

Das ist der Kernkonflikt moderner Geschäftsführung:
Sie tragen die Haftung – aber die operative Realität entzieht sich Ihrer Kontrolle.

Die Lösung liegt nicht in mehr Papier, sondern in Technik

Genau hier greifen **moderne, haftungsrelevante Schutzmechanismen:**

- **Identity & Access Management (IAM)**
- **Single Sign-On (SSO)**

- **Privileged Access Management (PAM)**
- **Sichere Datentransfer-Verfahren (z. B. One-Time-Secret statt E-Mail)**

Diese Systeme lösen zwei Probleme gleichzeitig:

- **Ihre Mitarbeiter können die Regeln einhalten, ohne Umwege zu suchen**
- **Sie erfüllen Ihre Überwachungs- und Organisationspflicht nachweisbar**

Das ist der eigentliche NIS-2-Schutzschild für Geschäftsführer.

KI, Automatisierung und Cyber-Haftung gehören zusammen

Ob Sie:

- **KI im Vertrieb automatisieren**
- **KI-Use-Cases in der Produktion einführen**
- **KI-Agenten im Kundenservice integrieren**
- **über Stiftungslösungen, Unternehmensbörsen, einen Unternehmensbroker oder sogar einen Notfallplan bei Geschäftsführer-Ausfall nachdenken**

entscheidend ist immer dieselbe Frage:

Ist Ihre Organisation so gebaut,
dass sie auch unter Stress, Wachstum und Automatisierung rechtssicher funktioniert?

Wenn nicht, entsteht kein technisches Risiko –
sondern ein persönliches Haftungsrisiko.

Fazit für Geschäftsführer

- NIS-2 ist kein IT-Thema, sondern Unternehmensführung
- Vertrauen ersetzt keine technischen Kontrollen
- Unpraktische Regeln erzeugen Haftung
- Gute Technik schützt Menschen, nicht nur Daten
- Cyber-Sicherheit ist heute Teil der Liquiditäts- und Existenzsicherung

Nicht, weil Hacker gefährlich sind –

sondern weil Organisationen es oft selbst sind.

Rechtlicher Hintergrund: Warum NIS-2 die Rolle des Geschäftsführers verändert

Die NIS-2-Richtlinie der EU ist kein IT-Projekt und kein Spezialgesetz für Konzerne.
Sie ist eine Governance- und Haftungsrichtlinie, die die Verantwortung ausdrücklich auf die Geschäftsführungsebene verlagert.

Für welche Unternehmen gilt NIS-2?

Hier ist eine wichtige Einordnung notwendig, um unnötige Verunsicherung zu vermeiden:

- Unternehmen, die **keine**
  - Vertrauensdiensteanbieter (Trust Service Provider),
  - öffentlichen Telekommunikationsanbieter
  - oder Anbieter strategisch kritischer Leistungen
    sind, fallen nicht automatisch unter NIS-2.
- Für diese Unternehmen greift NIS-2 **grundsätzlich erst ab der Schwelle „mittleres Unternehmen“**:
  - **ab 50 Mitarbeitenden** oder
  - **ab 10 Mio. Euro Jahresumsatz**

Kleine Unternehmen unterhalb dieser Schwelle sind in der Regel **nicht unmittelbar betroffen**.

Aber:
Sobald diese Größenordnung erreicht ist – oder absehbar erreicht wird –
stellt sich nicht mehr die Frage *ob*, sondern *wie* Sie vorbereitet sind.

Ab wann gilt NIS-2?

- Die EU-Richtlinie ist seit **2023 beschlossen**
- Die nationale Umsetzung in den Mitgliedsstaaten läuft

- Für Unternehmen bedeutet das:
  ab 2025/2026 gelten die Pflichten faktisch verbindlich, Prüfungen und Sanktionen folgen zeitversetzt

Entscheidend für Sie als Geschäftsführer ist nicht das exakte Inkrafttretensdatum, sondern:

Ab jetzt wird geprüft, ob Sie sich vorbereitet haben.

Was NIS-2 konkret vom Geschäftsführer verlangt – in Klartext

NIS-2 verlangt **keine technische Detailkenntnis** vom CEO.
Aber sie verlangt **nachweisbare organisatorische Verantwortung.**
Konkret heißt das:

- Sie dürfen sich auf IT-Spezialisten stützen
- Sie dürfen Verantwortung delegieren
- Sie dürfen Haftung nicht delegieren

Die Richtlinie spricht ausdrücklich von:

- angemessenen technischen UND organisatorischen Maßnahmen
- Überwachungspflichten der Geschäftsleitung
- persönlicher Verantwortlichkeit bei vorhersehbaren Schwachstellen

Der zentrale Punkt ist neu und für viele ungewohnt:

„Ich habe meinem IT-Team vertraut“ gilt nicht mehr als Entlastung.

Warum Vertrauen in diesem Kontext leichtsinnig wäre

Das klingt hart, ist aber realistisch:

- Ihre Mitarbeiter handeln nicht falsch,
- sie handeln **pragmatisch**.

Aus der Praxis wissen wir:

- Mitarbeiter **kennen Datenschutzregeln**
- sie wissen, was *„richtig“* wäre

- **sie bekommen aber oft weder Prozesse noch Werkzeuge**, um es richtig zu tun

Der typische Zielkonflikt:

- Prozesse senken kurzfristig Produktivität
- Sicherheits-Tools kosten Lizenzen
- Budgets werden nicht freigegeben
- Leistung wird trotzdem erwartet

Die logische Folge:

Der Mitarbeiter wählt den **Weg des geringsten Widerstands**.

Nicht aus Bequemlichkeit, sondern aus **Systemdruck**.

Seit dem **1.1.2026** wird genau dieses Verhalten für die Geschäftsführung gefährlich:
Nicht das Wissen der Mitarbeiter zählt, sondern die organisatorische Ermöglichung durch das Unternehmen.

Warum interne Kontrollen nicht ausreichen

Ein CEO steht hier in einem strukturellen Dilemma:

- Interne IT prüft sich faktisch selbst
- Interne Audits sind Teil der Hierarchie
- Kritische Punkte werden oft „mitgedacht“ oder relativiert

NIS-2 setzt deshalb implizit auf ein bekanntes Prinzip aus anderen Hochrisikobereichen:

Unabhängige, externe Prüfung

Nicht aus Misstrauen gegenüber Mitarbeitern, sondern:

- zur **Entlastung der Geschäftsführung**
- zur objektiven Bewertung realer Prozesse
- zur Dokumentation, dass Organisationspflichten erfüllt wurden

Ein externes Audit ist damit **kein Kontrollinstrument**, sondern:
ein Haftungsschutz für den Geschäftsführer.

Der Denkfehler vieler CEOs

Viele Geschäftsführer denken:

„Wenn ich Prozesse verschärfe und Tools einführe, verliere ich Produktivität."

Kurzfristig ist das oft richtig.
Langfristig ist es gefährlich.

Denn NIS-2 bewertet **nicht**, ob Ihre Mitarbeiter schnell arbeiten,
sondern ob Ihr Unternehmen **vorhersehbare Risiken organisatorisch beherrscht.**

Oder anders gesagt:

Produktivität ohne Struktur ist seit 2026 kein Wettbewerbsvorteil mehr,
sondern ein Haftungsrisiko.

Einordnung zum Schluss

NIS-2 will keine Angst erzeugen.
Die Richtlinie folgt einer einfachen Logik:

- Komplexe, digitalisierte Organisationen
- können nicht mehr allein auf Vertrauen basieren
- Verantwortung muss **systemisch abgesichert** werden

Für Geschäftsführer bedeutet das:

Nicht mehr selbst alles wissen zu müssen –
aber sicherzustellen, dass Wissen, Prozesse und Technik zusammenpassen.

Genau hier beginnt professionelle Unternehmensführung im digitalen Zeitalter.

Um Sie als CEO/Geschäftsführer zu unterstützen, kann 4WT eine unabhängige **Backbox-Analyse** Ihrer geschäftskritischen Altsysteme durchführen. Auf dieser Grundlage erhalten Sie eine fundierte Entscheidungshilfe.

Die Ingenieure von 4WT werden meist für Unternehmen aus dem DACH-Raum hinzugezogen wenn:

- Sie planen, den südostasiatischen Markt zu erschließen (Expansion, Markteintritt, Diversifizierung von Lieferketten);
- Sie deutsche Ingenieure mit technischem Sachverstand (juristische thailändische Person mit deutscher DNA), lokaler Präsenz und deutscher Management, jedoch keine Folienberatung suchen;
- Sie einen juristischen deutschen Partner vor Ort in Südostasien zur Unterstützung Ihrer Aktivitäten und als verlängerten Arm benötigen (operativ/technisch-exekutiv Betreuung vor Ort);
- Sie den Eindruck haben, dass in Ihrer Niederlassung ein Shadow-Management etabliert werden muss, welches die asiatische Arbeitskultur schon seit Jahrzehnten kennt, aber eine 100-prozentige deutsche DNA besitzt - Cultural Broker.
- Sie eine kulturell angepasste Unterstützung Ihrer thailändischen Geschäftsführung entsprechend deutscher Qualitäts- und Prozessanforderungen suchen.
- Sie die enormen Kosten ihres entsendeten Expat mit Sorge erfüllen und Sie eine deutlich günstigere skalierbare Alternative suchen.
- Sie eine Repräsentation bzw. bevollmächtigte Unternehmensvertretung als Liaison Office, Business Proxy oder Corporate Service Provider benötigen.
- Sie rechtssichere pragmatische FBA-konforme Inkubation suchen.

oder

- die Kosten für Ihre IT nicht mehr kalkulierbar sind und Sie keinen echten Mehrwert spüren,
- operativer Betrieb und IT nicht mehr sauber zusammenpassen und dadurch wirtschaftliche Entscheidungen ins Leere laufen,
- Sie das Gefühl haben, ihre Unternehmen arbeiten für die IT und nicht umgekehrt
- trotz gleicher Sprache es zu Verständnisschwierigkeiten zwischen Ihnen und Ihrer IT-Abteilung kommt und Sie einen Sparringspartner benötigen,
- Sie suchen eine Person, die ihnen in Augenhöhe ehrliche Antworten gibt und nicht aufgrund von Befürchtungen bezüglich seiner nächsten Beförderung oder seines Arbeitsvertrags handelt.

- sich keiner Ihrer Mitarbeiter mehr mit den Legacy-(Alt-)Systemen im Keller auskennt,

Lassen Sie uns konkret über Ihr Vorhaben sprechen.

Kein Pitch.
Keine Verpflichtung.
Keine Vertriebsrhetorik
Austausch zwischen zwei Unternehmer, die Klartext reden.
Nur 15 Minuten zur Einordnung Ihres Themas.

+49 30 8687094010 (6:00 bis 16:00 Uhr MEZ)
✉ uwe.richter@it-e-com.de
4WT Kontaktseite
4WT Firmenseite

Manchmal reicht ein einziges Gespräch, um teure Fehler zu vermeiden.

Zufällige Auswahl von Artikeln zum Thema: Unternehmensführung

- KI im Mittelstand beginnt nicht bei der IT (Serie, Teil 13 von 14)
- KI im Mittelstand beginnt nicht bei der IT (Serie, Teil 14 von 14)
- KI im Mittelstand beginnt nicht bei der IT (Serie, Teil 8 von 14)
- KI im Mittelstand beginnt nicht bei der IT (Serie, Teil 7 von 14)
- KI im Mittelstand beginnt nicht bei der IT (Serie, Teil 2 von 14)
- Das „trojanische Profil“: Warum Ihr bester Problemlöser niemals Ihren Schreibtisch erreicht
- IT-Sanierung statt Milliardengrab: Warum Inhaber-Strategie im Maschinenraum beginnt
- Enterprise-Architect im Unternehmen: Aufgaben, Nutzen und Mehrwert für Unternehmer
- Unternehmensberatung Mittelstand mit Umsetzungsverantwortung
- Das Erbe von Horst Kuchling – Warum Fachwissen ohne Methode wertlos ist

---

Weiterführende Links

- Eine unabhängige Blackbox-Analyse für Geschäftsführer, die für ein geschäftskritisches Altsystem persönlich Verantwortung tragen und vor einer teuren Fehlentscheidung stehen.