NIS-2 und DORA: Cybersecurity-Lehren für Verkehrsunternehmen

Artikel vom **27. Juli 2026**
Glatteisfrühwarnsysteme

Die Fabasoft Contracts GmbH zeigt, welche Erfahrungen aus DORA für Verkehrsunternehmen relevant sind: Lieferketten, IKT-Drittdienstleister, kritische Abhängigkeiten und revisionssichere Prozesse rücken bei NIS-2 in den Fokus. So wird Cyberresilienz zur Governance-Aufgabe.

NIS-2 verschärft Anforderungen an Cybersecurity und Lieferkettensicherheit. Verkehrsunternehmen können aus DORA lernen, wie IKT-Drittdienstleister, Risiken und Nachweise strukturiert gesteuert werden (Bild: Fabasoft).

Mit NIS-2 verschärft die Europäische Union die Anforderungen an Cybersicherheit,

Risikomanagement und Lieferkettensicherheit. Für Verkehrsunternehmen stellen sich damit neue Fragen: Welche Dienstleister und Systeme sind für den sicheren Betrieb unverzichtbar? Wo entstehen kritische Abhängigkeiten? Und lassen sich Risiken, Maßnahmen und Verantwortlichkeiten im Prüfungsfall nachvollziehbar belegen? Der Blick auf den »Digital Operational Resilience Act« kann dabei Orientierung geben. Die EU-Verordnung verpflichtet Finanzunternehmen seit Anfang 2025 zu umfangreichen Maßnahmen für digitale Widerstandsfähigkeit. Während DORA auf den Finanzsektor begrenzt ist, betrifft NIS-2 deutlich mehr Branchen. Aus den Erfahrungen der Finanzwirtschaft lassen sich mehrere Lehren für Verkehrsunternehmen ableiten.

Sicherheit endet nicht an der Unternehmensgrenze Cybersecurity konzentrierte sich lange vor allem auf eigene Systeme und Prozesse. Die Erfahrungen aus der DORA-Umsetzung zeigen jedoch, dass Risiken häufig bei externen IKT-Drittdienstleistern entstehen. Nach Angaben der österreichischen Finanzmarktaufsicht hatten mehr als 50 Prozent der seit Inkrafttreten von DORA gemeldeten Sicherheitsvorfälle ihren Ursprung bei einem solchen Dienstleister. Für Verkehrsunternehmen bedeutet das: Die eigene Sicherheitsstrategie sollte die digitale Verkehrsinfrastruktur entlang der gesamten Lieferkette berücksichtigen. Dazu zählen Leit- und Dispositionssysteme ebenso wie Cloud-, Software- und IT-Dienstleister. Wer nur interne Systeme betrachtet, blendet einen Teil des tatsächlichen Risikos aus. **Kritische Abhängigkeiten früh erkennen** Finanzunternehmen mussten im Zuge von DORA prüfen, wie stark Geschäftsprozesse von einzelnen IT-Dienstleistern abhängen. Dabei wurde deutlich, dass für zentrale Anbieter häufig keine belastbaren Ausstiegsstrategien oder Alternativen vorlagen. NIS-2 fordert solche Exit-Pläne nicht ausdrücklich, dennoch ist die Erkenntnis relevant: Organisationen sollten wissen, welche Folgen der Ausfall eines Dienstleisters hätte, wie schnell Alternativen aktiviert werden könnten und welche vertraglichen oder technischen Hürden einem Wechsel entgegenstehen. Das gilt besonders für Verkehrsunternehmen, die mit vielen externen IT-, Software- und Infrastrukturdienstleistern arbeiten. Eine zentrale Erfassung relevanter Dienstleisterinformationen und strukturierte Prozesse für das Drittparteienmanagement können helfen, spätere Hürden zu vermeiden.

Drittparteienmanagement und Nachweise strukturieren Die DORA-Erfahrungen zeigen, dass Drittparteienrisikomanagement mehr ist als klassische Lieferantenverwaltung. Gefordert sind Dokumentation, Berichtspflichten, Risikobewertungen, Due Diligence, aktuelle Lieferanteninformationen und angepasste Verträge. Prüfungen zeigten unter anderem lückenhafte Inventare, unklare Verantwortlichkeiten, unvollständige Prozesse und mangelnde Datenqualität. Für NIS-2-betroffene Unternehmen ist deshalb entscheidend, Governance-, Risiko- und Kontrollprozesse von Beginn an transparent aufzubauen. Digitale Workflows können Prozessschritte steuern, Verantwortlichkeiten zuordnen und Tätigkeiten revisionssicher dokumentieren. Audit-Trails und elektronische Workflow-Unterschriften ermöglichen den Nachweis, wer wann Bewertungen durchgeführt, Entscheidungen getroffen oder Freigaben erteilt hat. KI-gestütztes Vertragsmanagement kann zusätzlich unterstützen, Verträge auf regulatorische Risiken zu prüfen und notwendige Anpassungen schneller umzusetzen. Die cloudbasierte Software ermöglicht laut Anbieter unter anderem das Erstellen, Digitalisieren, Signieren und Verwalten von Verträgen sowie das Management von Vertragspartnern über den gesamten Lifecycle. Für den Finanzsektor wird zudem ein Produkt für regulatorikkonformes Auslagerungsmanagement angeboten. NIS-2 ist damit kein reines IT-Projekt. Die Vorgaben adressieren die Verantwortung der Unternehmensleitung und verlangen einen organisationsweiten Umgang mit Cyberrisiken. IT, Lieferantenmanagement, Risikomanagement, Compliance, Einkauf, Fachbereiche und Geschäftsführung sollten eng zusammenarbeiten. Wer relevante Stakeholder früh einbindet, Verantwortlichkeiten klar verteilt und Entscheidungen nachvollziehbar dokumentiert, kann regulatorische Anforderungen besser im Unternehmen verankern und zugleich die Resilienz kritischer Verkehrs- und Mobilitätsinfrastrukturen stärken.

Hersteller aus dieser Kategorie