NIS-2 und sichere Lieferkette - Lieferantenaudit mit der GAP View Software

12.05.2026, 09:00 | IT, New Media & Software

Pressemitteilung von: *GAP View GmbH*

GAP View GmbH

In der heutigen digitalen Wirtschaft sind Unternehmen und Behörden stark von IT-Lieferanten und -Dienstleistern abhängig. Je nach Umfang und Art der gelieferten Leistungen kann diese Abhängigkeit gravierende operative und rechtliche Risiken mit sich bringen. Die Behandlung dieser Risiken ist regulatorisch festgelegt und in nationalen sowie internationalen Informationssicherheitsstandards fest verankert. Durch gezielte organisatorische und technische Sicherheitsmaßnahmen können die Risiken auf ein Minimum reduziert werden. Ihre Aktualität und Wirksamkeit müssen jedoch regelmäßig überprüft werden. Im Rahmen des Lieferantenmanagements werden geeignete Lieferanten und Dienstleister anhand festgelegter Kriterien identifiziert und ausgewählt. Neben den betriebswirtschaftlichen Aspekten müssen auch die Sicherheitskriterien berücksichtigt werden. Aufgrund der Dynamik des Marktes und der sich stetig verändernden Sicherheitslage müssen diese Kriterien sowie die Eignung eines Lieferanten regelmäßig überprüft und neu bewertet werden. Dies geschieht in sorgfältig geplanten Lieferantenaudits.

NIS-2/BSIG und sichere Lieferkette

Das novellierte BSI-Gesetz verpflichtet daher besonders wichtige Einrichtungen (bwE) und wichtige Einrichtungen (wE), die Sicherheit ihrer Lieferketten zu gewährleisten. Eine der zehn Risikomanagementmaßnahmen gemäß § 30 Abs. 2 ist die Gewährleistung der „**Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern**“ unter Einhaltung des „Stands der Technik“ und unter Berücksichtigung „einschlägiger europäischer und internationaler Normen.“ Das Ziel ist die Stärkung der Widerstandsfähigkeit gegenüber Cyberangriffen, die von Lieferanten und Dienstleistern ausgehen können.

Standards und Vorgaben

Die etablierten nationalen und internationalen Informationssicherheitsstandards dienen als „Best Practice“ und werden bei der Planung und Umsetzung von Anforderungen an eine sichere Lieferkette herangezogen und tragen somit zur Erfüllung von gesetzlichen Pflichten der NIS-2 betroffenen Organisationen bei. Die folgenden Beispiele verdeutlichen die Anforderungen an die kontinuierliche Überprüfung der Einhaltung vertraglich festgelegter Sicherheitsmaßnahmen durch Dienstleister und Lieferanten.

ISO/IEC 27001:2022: Im Anhang A der internationalen Norm sind zahlreiche Sicherheitsmaßnahmen für das Lieferantenmanagement festgelegt (vgl. A.5.19, A.5.20, A.5.21, A.5.23). Bei der Zusammenarbeit mit Dienstleistern und Lieferanten muss der dort geforderte Mindeststandard zwingend gewähr-leistet werden. Die verbindlich festgelegten Vorgaben müssen regelmäßig kontrolliert, bewertet und ggf. angepasst werden. Dies erfolgt unter anderem durch Audits (vgl. **A.5.22 „Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen”**).

BSI: In dem Beitrag **"#nis2know, Sichere Lieferkette"** stellt das BSI eine pragmatische Vorgehensweise zur Etablierung von Sicherheitsaspekten bei Dienstleistern und Lieferanten im Kontext des novellierten BSIG vor. In den "Grundlagen des Cyber-Supply-Chain-Risk-Managements (C-SCRM)" wird in fünf Schritten eine effektive Methodik vorgestellt, mit der eine NIS-2 betroffene Organisation angemessen auf die Gefahren in der Lieferkette vorbeugen und reagieren kann. Der fünfte Punkt widmet sich der Überprüfung der umgesetzten Maßnahmen. Ein wichtiger Bestandteil der Überprüfung sind die Lieferantenaudits.

UP-KRITIS: Im Rahmen der „Unabhängigen Partnerschaft KRITIS“ (UP KRITIS) wurden „Best-Practice-Empfehlungen für Anforderungen an Lieferanten zur Gewährleistung der Informationssicherheit in kritischen Infrastrukturen“ veröffentlicht. Demnach soll der Dienstleister/Lieferant dem Auftraggeber Informationen zu seiner Sicherheitsorganisation offenlegen. Darüber hinaus ist der Auftraggeber oder von ihm beauftragte Dritte befugt die Informationssicherheitsmaßnahmen zu auditieren.

RUN: Mittels des Dokuments "Reife- und Umsetzungsgradbewertung im Rahmen der Nachweisprüfung (RUN)“ wurde seitens des BSI eine einheitliche Bewertungsgrundlage für Betreiber von KRITIS und prüfende Stellen geschaffen, um den Reife- und Umsetzungsgrad im Kontext des § 8a BSIG zu ermitteln. Im Bereich "Organisatorische Maßnahmen (OrgM)" findet sich die Maßnahme **KdA 99 "Kontrolle der Leistungserbringung und der Sicherheitsanforderungen an Dienstleister und Lieferanten des KRITIS-Betreibers"**, welche die regelmäßige Überwachung und Überprüfung der vereinbarten Leistungen und Sicherheitsanforderungen von Dritten vorsieht. Die Maßnahme beinhaltet die regelmäßigen, unregelmäßigen Audits sowie die Überprüfung von sicherheitsrelevanten Vorfällen.

Lieferantenaudit mit der GAP View Software

Die Nutzung der Audit Management Software GAP View in Kombination mit den bereitgestellten Fragenkatalogen ermöglicht es NIS-2 betroffenen Organisationen, ihre Dienstleister und Lieferanten gemäß den Anforderungen des BSIG zu planen, durchzuführen und zu bewerten. Damit wird die gesetzliche Vorgabe hinsichtlich einer sicheren Lieferkette erfüllt. GAP View wurde speziell für die effiziente, kontinuierliche Überprüfung der Wirksamkeit, Vollständigkeit und Angemessenheit der implementierten Informationssicherheitsmaßnahmen im Rahmen von internen und externen Audits sowie Lieferantenaudits mit folgenden Eigenschaften entwickelt:

- Stammdatenmanagement aller im Auditprogramm beteiligten sicherheits-relevanten Dienstleister und Lieferanten
- Bereitstellung der Audit-Fragenkatalogen (Content) für Lieferantenaudits und NIS-2 GAP Analyse
- Management aller geplanten und durchgeführten Audits mit genauer Zeitplanung (Kalender), Ressourcenzuteilung, Fragenkatalogen, Nachweisen und Ergebnissen
- Management aller für ein Audit erforderlichen Dokumentationen und Auditnachweisen (Dateien unterschiedlicher Formate sowie im Audit generierte Fotos)
- Ganzheitliche Unterstützung der internen und externen Auditoren bei der Organisation von Audits und Lieferantenaudits nach ISO 19011 und ISO/IEC 17021
- Unterstützung von Remote-, Vor-Ort-Audits und Self-Assessments
- Unterstützung verschiedener Audit- und Bewertungsmethoden nach ISO und BSI
- Unterstützung aller erforderlichen Prüfmethoden (u.a. Befragung, Begehung, Beobachtung, Aktenanalyse, technische Prüfung, Datenanalyse)
- Management der Korrekturmaßnahmenkataloge mit Zuordnung der zuständigen Personen, geschätztem Zeitaufwand, Umsetzungsdatum, Prioritäten und Umsetzungsstatus
- Umsetzungsdokumentation der durchgeführten Korrekturmaßnahmen
- Dashboard (Stand der Umsetzung eines Audits, verbleibende Zeit bis zum Abschluss des Audits, Bewertung, Stand der Umsetzung von Korrekturmaßnahmen)
- Umfassendes Berichtswesen für die Planung, Durchführung und Bewertung von Audits sowie Korrekturmaßnahme

Weiterführende Informationen und Webinare

über Lieferantenaudits sowie NIS-2-Gap-Analyse und Umsetzung der kontinuierlichen Überwachung nach § 38 BSIG

finden Sie unter https://www.gap-view.de/Webinare.html

GAP View GmbH

Schauenburgerstrasse 116 Schauenburgerstrasse 116
24118 Kiel
Deutschland

KrzysztofPaschke (Geschäftsführer)

+49 160 88 26100

kpaschke@gap-view.de

www.gap-view.de/

Portrait

Die GAP View GmbH ist ein Beratungs- und Softwareentwicklungsunternehmen, das sich auf die Entwicklung und Einführung der gleichnamigen Software bei Behörden, Unternehmen und sonstigen öffentlichen oder privaten Organisationen spezialisiert hat. GAP View ist eine Audit- und Revisions-Management-Software, die eine effiziente und effektive kontinuierliche Überprüfung von Informationssicherheitsmanagementsystemen nach unterschiedlichen Sicherheitsstandards und Normen ermöglicht und das Management von Korrekturmaßnahmen unterstützt.

News-ID: 1311528 • Views: 213 (Stand: 26.07.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/1311528/NIS-2-und-sichere-Lieferkette-Lieferantenaudit-mit-der-GAP-View-Software.html