NIS-2 GAP-Analyse und Planung der Umsetzung mit GAP View Audit Management Software

03.03.2026, 09:00 | IT, New Media & Software

Pressemitteilung von: *GAP View GmbH*

GAP View GmbH - Audit Management Software

Mit der **NIS2-Richtlinie** (Network and Information Security Directive 2) verfolgt die Europäische Union das Ziel, das gemeinsame Sicherheitsniveau im Bereich der Netz- und Informationssysteme deutlich zu verbessern. Ursachen dafür sind unter anderem die zunehmende Digitalisierung und die veränderte geopolitische Lage, durch die Angriffe auf kritische Infrastrukturen massiv zugenommen haben, sowie die Unzulänglichkeiten der Vorgängerrichtlinie NIS-1. Sie dient insbesondere dazu, zunehmende Cyberangriffe abzuwehren, kritische Dienstleistungen zu stabilisieren und das Sicherheitsniveau innerhalb der EU zu harmonisieren.

Die Umsetzung der NIS2-Richtlinie in deutsches Recht erfolgte mit der Verkündung des ***NIS2UmsuCG*** (Gesetz zur Umsetzung der Richtlinie (EU) 2022/2555 über Maßnahmen zur Gewährleistung der Netz- und Informationssicherheit) im Bundesgesetzblatt am 5. Dezember 2025 und dessen Inkrafttreten am 6. Dezember 2025. Das NIS2UmsuCG erlässt, ändert oder hebt mehrere Einzelgesetze gleichzeitig auf. Neben der ***Novellierung des BSIG*** (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) sind davon auch weitere Fachgesetze betroffen, beispielsweise aus den Bereichen Telekommunikation, Energie oder Sozialversicherung. Mit dem Inkrafttreten des NIS2UmsuCG und der vollständigen Neufassung des BSI-Gesetzes gelten die neuen materiellen Anforderungen an die Informationssicherheit unmittelbar und ohne Übergangsfrist. Einige Pflichten sind jedoch fristgebunden, darunter insbesondere die Registrierung nach § 33 BSIG, die spätestens drei Monate nach Eintritt der Registrierungspflicht erfolgen muss. Für Einrichtungen, die bereits seit Inkrafttreten betroffen sind, läuft diese **Frist** regelmäßig bis zum **6. März 2026**.

Wer ist betroffen?

Der Geltungsbereich des NIS-2-Umsetzungsgesetzes geht weit über den bisher bekannten Kreis der KRITIS-Unternehmen hinaus. Direkt betroffen sind sogenannte „besonders wichtige Einrichtungen" und „wichtige Einrichtungen". Neben der Zugehörigkeit zu einem Wirtschaftssektor oder einer Branche sind die Anzahl der beschäftigten Mitarbeiter, der Jahresumsatz und die Bilanz von Bedeutung. Die Betroffenheit legt das § 28 BSIG Abs. 1 und 2 in zwei Kategorien fest:

- Besonders wichtige Einrichtungen (bwE): Große Unternehmen ab 250 Mitarbeiter oder ab € 50 Mio. Jahresumsatz und € 43 Mio. Bilanzsumme. Betreiber kritischer Anlagen (KRITIS) gelten kraft Gesetzes als besonders wichtig in Sektoren: Energie, Transport und Verkehr, Finanzwesen, Gesundheit, Wasser, Digitale Infrastruktur und Weltraum.
- Wichtige Einrichtungen (wE): Mittlere Unternehmen ab 50 Mitarbeiter und ab € 10 Mio. Jahresumsatz oder Bilanzsumme in Sektoren: Transport und Verkehr, Abfallwirtschaft, Produktion, Herstellung und Handel mit chemischen Stoffen, Produktion, Verarbeitung und Vertrieb von Lebensmitteln, Verarbeitendes Gewerbe/Herstellung von Waren, Anbieter digitaler Dienste und Forschung.

Die Betroffenheit der Einrichtungen der Bundesverwaltung ist in § 29 BSIG geregelt. Demnach sind die Bundesbehörden, die öffentlich-rechtlich organisierten IT-Dienstleister der Bundesverwaltung sowie weitere Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts auf Bundesebene betroffen.

Gesetzliche Pflichten der betroffenen Unternehmen

Ein besonderes Augenmerk im BSIG gilt den Pflichten und Verantwortlichkeiten der Geschäftsleitung. Neben der Verpflichtung zur Umsetzung der vorgegebenen Sicherheitsmaßnahmen und deren Überwachung sind auch die Haftungsregeln bei schuldhaft verursachten Schäden festgelegt, die entstehen, wenn die Vorgaben nicht beachtet werden. Zu den technischen und organisatorischen Sicherheitsmaßnahmen gehören u. a.:

- **[§ 33]** Die betroffenen Unternehmen müssen sich spätestens bis zum 6. März 2026 über ein zentrales Portal bei dem Bundesamt für Sicherheit in der Informationstechnik (BSI) registrieren.
- **[§ 32]** Bei festgestellten erheblichen Sicherheitsvorfällen besteht eine Meldepflicht innerhalb vorgegebener Fristen.
- **[§ 30]** Es müssen geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen umgesetzt werden, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die für die Erbringung der Dienste genutzt werden, zu vermeiden und die Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Darunter:
  - Risikoanalyse und Sicherheitskonzept
  - Bewältigung von Sicherheitsvorfällen
  - Betriebliches Kontinuitäts- und Krisenmanagement
  - Sicherheit von Lieferketten
  - Sicherheit in der Beschaffungs-, Entwicklungs- und Wartungsphase
  - Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik
  - Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik
  - Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren
  - Personalsicherheit, Zugriffskontrolle und Verwaltung von IKT- Systemen, -Produkten und -Prozessen
  - Multi-Faktor-Authentifizierung, kontinuierliche Authentifizierung, gesicherte Kommunikation
- **[§ 38]** Gemäß § 38 Abs. 1 BSIG sind Geschäftsleiter persönlich verpflichtet, die Risikomanagementmaßnahmen nach § 30 BSIG umzusetzen und deren Umsetzung zu überwachen. Zudem müssen sie regelmäßig an Schulungen zur Cybersicherheit teilnehmen (§ 38 Abs. 3 BSIG). Ein Verzicht auf Schadensersatzansprüche der Einrichtung gegen die Geschäftsleitung ist bei Pflichtverletzungen nicht zulässig.

NSI-2 Roadmap (nach BSI)

Die vom BSI veröffentlichte NIS-2-Roadmap zeigt eine systematische Vorgehensweise in Phasen für die Umsetzung der Richtlinie auf. In zwei dieser Phasen kommt die Audit-Management-Software GAP View zum Einsatz. Einerseits bei der Feststellung des aktuellen Standes der Cybersicherheit (Gap-Analyse) und der sich daraus ergebenden Maßnahmen für die Umsetzung der Richtlinie, andererseits bei der kontinuierlichen Überwachung und Verbesserung der umgesetzten Sicherheitsmaßnahmen (kontinuierliches Monitoring).

NIS-2 GAP-Analyse mi GAP View Software

Mithilfe der GAP View Software und des bereitgestellten Fragenkatalogs kann der **aktuelle technische, organisatorische und prozessuale IST-Zustand der Cybersicherheit** in einem Unternehmen ermittelt werden. Der speziell dafür entwickelte, detaillierte **Fragenkatalog** basiert auf dem Mapping der ISO/IEC 27001 Controls auf die Sicherheitsanforderungen des BSIG. Für KRITIS-Organisationen gibt es zusätzlich einen Fragenkatalog zur Überprüfung der Vollständigkeit und Wirksamkeit des eingesetzten **Systems zur Angriffserkennung**, der auf der BSI-Orientierungshilfe und den IT-Grundschutz-Bausteinen basiert. Die auf diese Art und Weise ermittelten Abweichungen (GAPs) zwischen den BSIG-Sicherheitsanforderungen und dem vorgefundenen IST-Zustand werden in einem automatisch erstellten Maßnahmenkatalog zusammengefasst. Dieser stellt eine **Grundlage für die Planung und Überwachung** der Umsetzung gesetzlicher Sicherheitsanforderungen dar. In ihm können Verantwortlichkeiten,

Umsetzungshinweise, Prioritäten, Zeitaufwand und Fristen für die Umsetzung festgelegt werden. Bei der Konzeption der Umsetzungshinweise kann über eine integrierte Schnittstelle direkt auf **OpenAI ChatGPT** zugegriffen werden. Durch die regelmäßige Aktualisierung des Umsetzungsstatus einzelner Sicherheitsmaßnahmen (Dashboard und Bewertung) und die Generierung entsprechender **Berichte** können die Geschäftsleitung und die beteiligten Mitarbeiter über den Projektfortschritt informiert werden.

NIS-2 Kontinuierliche Überwachung mit GAP View Software

In der Regel erfolgt die Überwachung der umgesetzten Sicherheitsanforderungen im Rahmen interner und externer Audits. Die GAP View Software wurde speziell für die effiziente, kontinuierliche Überprüfung der Wirksamkeit, Vollständigkeit und Angemessenheit von Managementsystemen für Informationssicherheit entwickelt. Somit ist sie sehr gut für die Erfüllung der Anforderungen gemäß § 38 BSIG geeignet. Sie unterstützt die Planung und Durchführung interner und externer Audits gemäß **ISO 19011** und **ISO/IEC 17021** sowie IS-Revisionen gemäß dem BSI-Leitfaden „**IS-Revision auf Basis von IT-Grundschutz**" und dem Baustein DER.3.1 „Audits und Revisionen".

GAP View Software - Weiterführende Informationen und Webinare

Weiterführende Informationen über NIS-2 Gap-Analyse, Planung und Umsetzung sowie kontinuierlichen Überwachung nach § 38 BSIG" finden Sie unter
https://www.gap-view.de/
und
https://www.gap-view.de/Webinare.html

GAP View GmbH

Schauenburgerstrasse 116 Schauenburgerstrasse 116
24118 Kiel
Deutschland

KrzysztofPaschke (Geschäftsführer und Berater)

+49 1608826100

kpaschke@gap-view.de

www.gap-view.de/

Portrait

Die GAP View GmbH ist ein Beratungsunternehmen, das am 1. März 2021 von dem Wirtschaftsinformatiker Krzysztof Paschke gegründet wurde. Der Schwerpunkt der Tätigkeit liegt auf der Entwicklung und Vermarktung der Audit-Management-Software „Gap View" sowie der Beratung im Bereich Managementsysteme für Informationssicherheit, Business Continuity und Internes Kontrollsystem sowie deren Auditierung. Darüber hinaus unterstützt die Unternehmensberatung ihre Kunden bei der Implementierung der genannten Managementsysteme.

News-ID: 1305399 • Views: 329 (Stand: 03.06.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/1305399/NIS-2-GAP-Analyse-und-Planung-der-Umsetzung-mit-GAP-View-Audit-Management-Software.html