MYRA

NIS-2-Anforderungen mit Myra umsetzen

Mit NIS-2 erfährt die europäische Cybersicherheitsstrategie die nächste Evolutionsstufe. Die Richtlinie erweitert den Anwendungsbereich erheblich und setzt strengere Anforderungen an Unternehmen und Organisationen in kritischen Sektoren. Der Fokus liegt dabei auf dem Risikomanagement, der Meldung von Sicherheitsvorfällen und der Informationssicherheit entlang der Lieferkette. Die Umsetzung der Anforderungen sind eine enorme Herausforderung für viele betroffene Organisationen.

Myra ist selbst KRITIS-Unternehmen und erfüllt als solches alle Anforderungen, die mit NIS-2 einhergehen. Zudem verfügt Myra über mehr als 10 Jahre Erfahrung in der Absicherung digitaler Geschäftsprozesse vor Cyberangriffen auf der Infrastruktur- und Anwendungsebene im Bereich hochregulierter Sektoren und KRITIS. Auf diese Expertise können Unternehmen vertrauen. Unsere Kunden profitieren von umfassend zertifizierten und auditierten Lösungen und Prozessen – diese tragen maßgeblich zur Erfüllung der Compliance-Anforderungen von NIS-2 bei.

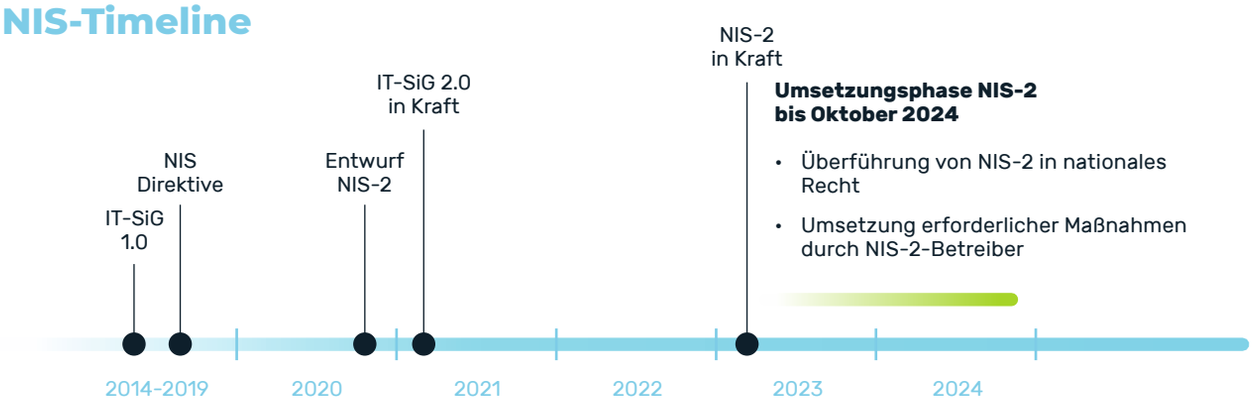
In diesem Compliance Fact Sheet erfahren Sie, in welchen Bereichen Myra Ihr Unternehmen bei der Umsetzung der NIS-2-Anforderungen unterstützen kann. Zusätzliche Informationen zu NIS-2, etwa zum Geltungsbereich und zu drohenden Bußgeldern bei Nichteinhaltung der regulatorischen Vorgaben in Deutschland, finden Sie in unserem Fact Sheet „NIS-2: Plötzlich KRITIS und was nun?“

Disclaimer:

Bitte beachten Sie, dass die bereitgestellten Informationen nach bestem Wissen und Gewissen und mit juristischer Unterstützung erstellt wurden. Dennoch dienen Sie rein informativen Zwecken und sind nicht als rechtliche Beratung zu verstehen. Eine pauschale Beurteilung regulatorischer Vorgaben ist aufgrund der individuellen Anforderungen eines jeden Instituts nicht möglich.

Wir übernehmen keine Gewähr für Richtigkeit, Vollständigkeit oder Aktualität der folgenden Informationen. Jegliche Haftung oder Verantwortung für Handlungen, die auf der Grundlage der bereitgestellten Informationen getätigt werden, wird hiermit ausgeschlossen. Als Grundlage für das Fact Sheet dient der Referentenentwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) vom 24.06.2024.

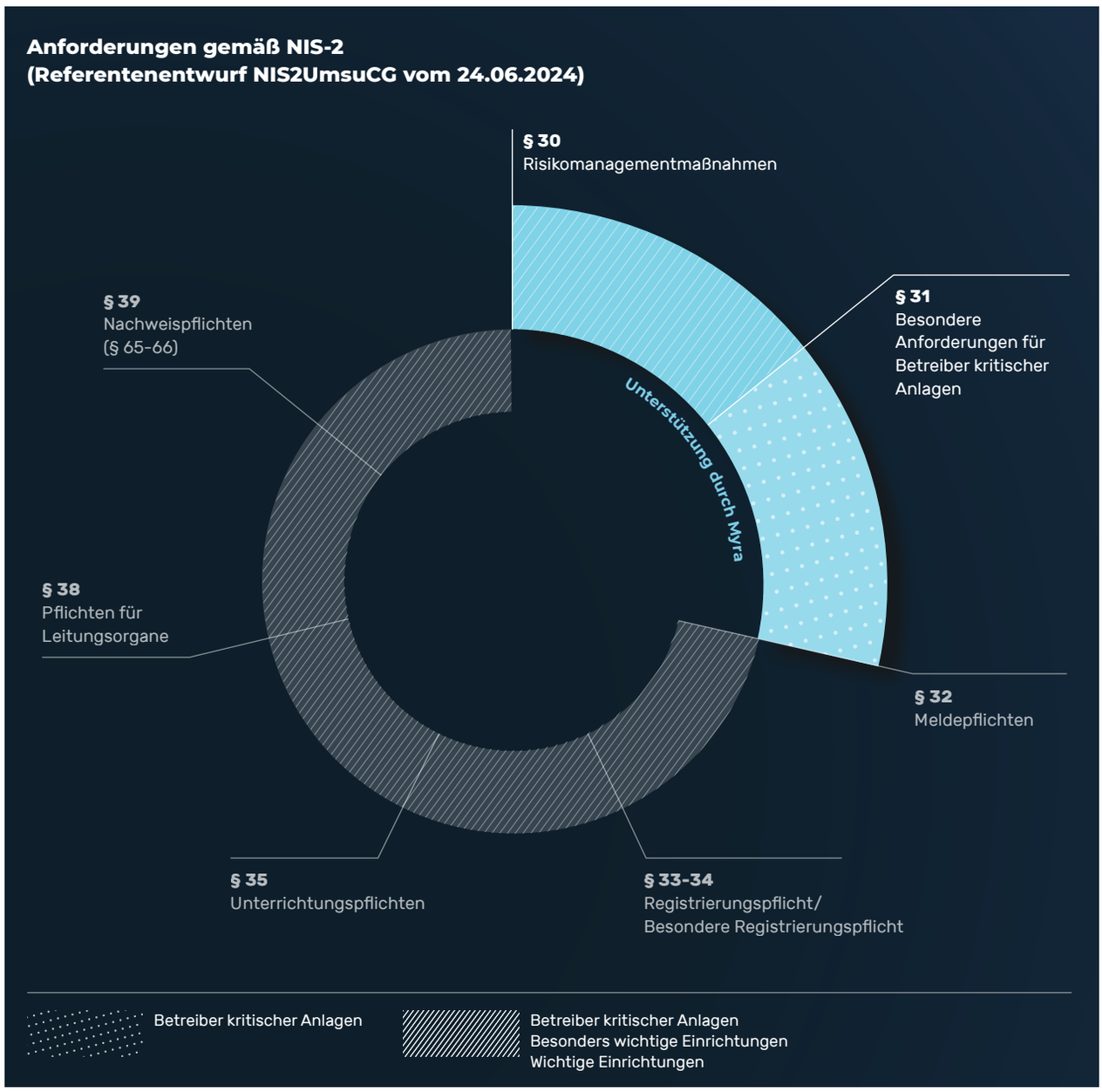
NIS-Timeline



Cybersecurity-Anforderungen in NIS-2

NIS-2 konzentriert die Anforderungen an die Cybersicherheit in sieben wesentliche Bereiche, um die Resilienz von Betreibern und Einrichtungen zu stärken. Wobei das Risikomanagement als zentrale Komponente der Anforderungen hervorzuheben ist. Die konkreten Vorgaben der einzelnen Bereiche werden in den Paragrafen 30 bis 35, 38 und 39 definiert, wie der folgenden Grafik zu entnehmen ist.

Myra kann mit seinen Lösungen zum Schutz vor Cyberangriffen auf der Infrastruktur- und Anwendungsebene maßgeblich zur Erfüllung der Compliance-Anforderungen beitragen, insbesondere in den Bereichen Risikomanagement (§ 30) und besondere Anforderungen für Betreiber kritischer Anlagen (§ 31).



Anforderungen an das Risikomanagement durch NIS-2

Besonders wichtige und wichtige Einrichtungen müssen technische und organisatorische Maßnahmen ergreifen, um angemessen IT-Störungen zu vermeiden und Auswirkungen von Sicherheitsvorfällen zu minimieren. Die Einhaltung der Maßnahmen ist zu dokumentieren. Diese sollen dem Stand der Technik entsprechen, einschlägige Normen berücksichtigen und auf einem gefahrenübergreifenden Ansatz beruhen.

Angesichts der knappen Zeit bis zur Umsetzungsfrist und der Komplexität bei der Erfüllung aller Anforderungen empfiehlt es sich, einzelne Schutzmaßnahmen an qualifizierte Dienstleister auszulagern. Folgende Tabelle zeigt im Detail, wie Sie zentrale Anforderungen von NIS-2 mit den Lösungen und Prozessen von Myra umsetzen können.

NIS-2-Anforderung nach § 30 (2)	Umsetzungsansatz von Myra
1. Risikoanalyse und Sicherheit für Informationssysteme	Mittels **individueller Risikoanalysen und laufender Sicherheitsoptimierungen** in Zusammenarbeit mit Kunden, externen Prüfern, Aufsichtsbehörden und unseren Partnern unterstützt Myra bei **Aufbau und Pflege effizienter Sicherheitskonzepte.** ✓
2. Bewältigung von Sicherheitsvorfällen	Webseiten, Online-Plattformen, Web-APIs und Web-Infrastrukturen sichert Myra mit seinen **Schutzlösungen für die Infrastruktur- und Anwendungsebene** umfassend und automatisch vor Cyberrisiken wie DDoS-Attacken, Bot-Netzwerken und Angriffen auf Datenbanken. (Eine Übersicht des Schutzumfangs der Myra-Lösungen auf Basis der Gartner-Taxonomie für DDoS-Mitigationslösungen finden Sie auf Seite 5) ✓
3. Aufrechterhaltung des Betriebs, Wiederherstellung, Backup-Management, Krisen-Management	Die Lösungen von Myra sorgen für einen fehlerfreien Betrieb von Geschäftsprozessen und sichern damit die Business Continuity – selbst im akuten Angriffsfall. Die **mehrfach georedundante Server-Infrastruktur** sorgt für ausfallsichere Hochverfügbarkeit mittels **policy-based Routing und IP Anycast.** Darüber hinaus erlaubt Myra eine **Absicherung von Redundanzen über mehrere Rechenzentren und Cloud-Instanzen hinweg**, um eine gleichbleibende Schutzfunktionalität und Qualität sicherzustellen. ✓
4. Sicherheit in der Lieferkette, Sicherheit zwischen Einrichtungen, Dienstleister-Sicherheit	Die **KI-basierte Bot- und Threat Detection mit automatisierter Abwehr von Angriffen** verhindert den Zugriff von Angreifern auf Webprozesse in Echtzeit und schützt damit vor einer Kompromittierung von Systemen und der Ausbreitung von Schadsoftware auf angeschlossene Organisationen. ✓
5. Sicherheit bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen	Die Technologie von Myra sowie die darauf betriebenen Schutzdienstleistungen sind **umfassend geprüft, auditiert und zertifiziert,** um für unsere Kunden ein Höchstmaß an Integrität, Vertraulichkeit und Verfügbarkeit sicherzustellen. • BSI ISO 27001 auf Basis von IT-Grundschutz • KRITIS-Nachweis gemäß § 8a Abs. 3 BSIG • BSI C5 Typ 2 • PCI DSS • IDW PS 951 Typ 2 (ISAE 3402) • Trusted Cloud • VS-NfD ✓
6. Bewertung der Wirksamkeit von Risikomanagementmaßnahmen	Das **Echtzeit-Monitoring** von Myra erlaubt die **granulare Identifikation, Klassifizierung und Protokollierung von Anomalien und Sicherheitsvorfällen auf Traffic-Ebene.** Alle geloggten Ereignisse basieren auf Server-Events für umfassend transparente **Traffic-Sichtbarkeit.** Frei definierbare Schwellenwerte leiten **automatische Reaktionen auf Angriffe** ein und stoßen **Eskalationspfade zur Benachrichtigung und Warnung** betroffener Organisationen an. ✓

7. Cyberhygiene und Schulungen im Bereich Cybersicherheit	Die Schutzdienstleistungen von Myra werden laufend aktualisiert und zur Abwehr neuer und akuter Bedrohungen optimiert. Darüber hinaus bietet Myra vielfältige **Funktionen zur Erhaltung der Cyberhygiene** wie z.B. **ein granulares Rechtemanagement** für Nutzerinnen und Nutzer der Plattform, **verpflichtende starke Passwörter sowie 2-Faktor-Authentifizierung oder Support von Client-Zertifikaten (mTLS) für Zero-Trust-Konzepte**. ✓
8. Einsatz von Kryptografie und Verschlüsselung	Die Dienste von Myra bieten ein Höchstmaß an Sicherheit. Die **SSL/TLS-Zertifikate** unserer Kunden werden in einem gesicherten Bereich unserer Infrastruktur gespeichert. Das Herunterladen oder Anzeigen bestehender SSL/TLS-Zertifikate von der Myra-Plattform ist ausdrücklich nicht möglich. Eine Dekodierung findet nur zur Überprüfung der Pakete **(Deep Package Inspection)** statt. Die gesamte Kommunikation in unserem Netzwerk nach außen, zum Nutzer und zu Ihrem Origin-Server, ist **vollständig verschlüsselt.** Die SSL/TLS-Terminierung findet bei Myra ausschließlich in Deutschland statt – **rechtssicher DSGVO-konform**. Als deutsches Unternehmen ist Myra nicht von den US-Überwachungsgesetzen FISA Section 702 und CLOUD Act betroffen. ✓
9. Sicherheit des Personals, Zugriffskontrollen und Anlagen-Management 10. Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung, sichere Kommunikation (Sprache, Video, Text), Notfallkommunikationssysteme	Das **User Management** von Myra erlaubt die granulare **Verwaltung von Zugriffs- und Verwaltungsrechten** für die Schutzdienstleistungen, **inkl. Richtlinien für Passwortstärke** und **verpflichtender 2-Faktor-Authentifizierung.** Zusätzlich unterstützt Myra den **Einsatz von Client-Zertifikaten (mTLS) für die Umsetzung von Zero-Trust-Konzepten.** ✓

Besondere Anforderungen an Betreiber kritischer Anlagen nach § 31	**Umsetzungsansatz von Myra**
1. Höhere Maßstäbe und aufwändigere Maßnahmen für das Risikomanagement nach § 30	Myra verfügt über **mehr als 10 Jahre Erfahrung bei der Absicherung kritischer Infrastrukturen** – die Umsetzung umfassender Sicherheitsanforderungen ist unser Tagesgeschäft. Als einer der führenden Anbieter erfüllt Myra alle 37 Kriterien des BSI für qualifizierte **DDoS-Mitigation-Dienstleister im Sinne § 3 BSI-Gesetz (BSIG)**. Darüber hinaus hat Myra selbst einen **Nachweis gemäß § 8a Abs. 3 BSIG für kritische Infrastrukturen (KRITIS)** erbracht und erfüllt damit die durch das BSI gestellten Anforderungen an KRITIS-Betreiber. Darüber hinaus entsprechen die Schutzdienstleistungen von Myra den Vorgaben gemäß **BSI C5 Typ 2** und sind nach **ISO 27001 auf Basis von IT-Grundschutz** zertifiziert. ✓
2. Einsatz von Systemen zur Angriffserkennung nach dem Stand der Technik	Dank **Echtzeit-Monitoring** erlaubt Myra die granulare **Identifikation, Klassifizierung und Protokollierung von Anomalien und Sicherheitsvorfällen auf Traffic-Ebene.** Alle geloggten Ereignisse basieren auf Server-Events für umfassend transparente **Traffic-Sichtbarkeit.** Frei definierbare Schwellenwerte leiten **automatische Reaktionen auf Angriffe ein** und stoßen Eskalationspfade zur Benachrichtigung und Warnung betroffener Organisationen an. ✓