UNTERSTÜTZUNG DER NIS2-COMPLIANCE IN DEUTSCHLAND MIT RAPID7

In Deutschland stellt das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) einen grundlegenden Wandel dar, wie Cybersicherheit reguliert und operativ umgesetzt wird. Durch eine umfassende Überarbeitung des BSI-Gesetzes (BSIG) geht es über traditionelle Compliance-Modelle hinaus und behandelt Cybersicherheit als eine kontinuierliche, risikobasierte Disziplin und nicht als einmalige Maßnahme.

Da digitale Infrastrukturen sowohl für die wirtschaftliche Stabilität als auch für die nationale Sicherheit zunehmend kritisch werden, haben jüngste Cybervorfälle die Fragilität vernetzter Systeme offengelegt. Als Reaktion darauf erweitert die deutsche Umsetzung von NIS2 sowohl den Kreis der regulierten Organisationen als auch die Tiefe der erforderlichen Sicherheitsmaßnahmen erheblich und erhöht die Abdeckung von etwa 4.500 auf rund 30.000 Einrichtungen.

Im Kern verlangt das Gesetz, dass Organisationen „dem Stand der Technik entsprechende technische und organisatorische Maßnahmen“ (§30 BSIG) implementieren, um Cybersicherheitsrisiken zu steuern. Dazu gehören nicht nur präventive Kontrollen, sondern auch kontinuierliches Monitoring, Angriffserkennung sowie Reaktions- und Wiederherstellungsfähigkeiten.

Das NIS2UmsuCG etabliert ein neues Betriebsmodell:

- Kontinuierliches Risikomanagement statt periodischer Compliance
- Echtzeit-Erkennung und strukturierte Vorfallmeldung mit strengen Fristen
- End-to-End-Sicherheit über den gesamten Lebenszyklus hinweg, einschließlich Lieferketten
- Verantwortung auf Führungsebene, wodurch Cybersicherheit zu einem Thema auf Vorstandsebene wird

Die Auswirkungen sind erheblich:

- Ein deutlich breiteres Spektrum an Branchen und Organisationen fällt in den Geltungsbereich
- Organisationen sehen sich strengeren Anforderungen, erhöhter regulatorischer Aufsicht und größerer Verantwortlichkeit der Führungsebene gegenüber
- Das Gesetz erstreckt sich auf zentrale Sektoren durch Anpassungen u. a. des Energiewirtschaftsgesetzes (EnWG) und des Telekommunikationsgesetzes (TKG)

Da sich Regulierungsbehörden zunehmend diesem Modell annähern, ist die Plattform von Rapid7, die Exposure Management und Continuous Threat Exposure Management (CTEM) mit Erkennungs-, Reaktions- und MDR-Funktionen vereint, optimal positioniert, um Organisationen dabei zu unterstützen, Compliance im Rahmen von NIS2 in Deutschland operativ umzusetzen und regulatorische Anforderungen in kontinuierliche, risikobasierte Sicherheitsmaßnahmen zu überführen.

Letztlich transformiert die deutsche Umsetzung NIS2 in einen konsequent durchsetzbaren nationalen Rahmen und hebt Cybersicherheit zu einem zentralen Geschäftsrisiko in der gesamten deutschen Wirtschaft.

Wer ist betroffen?

Die bisherige Unterscheidung zwischen KRITIS und Nicht-KRITIS wird weitgehend aufgehoben und durch eine breitere Kategorisierung ersetzt.

Grundsätzlich betroffen sind Unternehmen ab:

- 50 Mitarbeitenden oder
- 10 Mio. € Jahresumsatz

sofern sie in einem regulierten Sektor tätig sind.

Wichtig: Unternehmen müssen selbst prüfen, ob sie betroffen sind – eine Benachrichtigung durch Behörden erfolgt nicht.

Es werden zwei Kategorien unterschieden:

KATEGORIE	KRITERIEN	SEKTOREN (BEISPIELE)
Wesentliche Einrichtungen	• Große Unternehmen (≥ 250 Mitarbeitende oder > 50 Mio. € Umsatz) • Hochkritische Sektoren • Unabhängig von Größe z. B. DNS- oder kritische Telekommunikationsanbieter	Energie, Transport, Finanzwesen, Gesundheit, Wasser, digitale Infrastruktur, öffentliche Verwaltung
Wichtige Einrichtungen	• Mittelständische Unternehmen (50–249 Mitarbeitende, > 10 Mio. € Umsatz) in kritischen Sektoren • Große und mittlere Unternehmen in weiteren kritischen Bereichen	Zusätzliche Sektoren: Postdienste, Abfallwirtschaft, Chemie, Lebensmittel, Industrie, digitale Dienste, Forschung.

Zentrale Anforderungen

A. Risikomanagement

Unternehmen müssen technische und organisatorische Maßnahmen (TOMs) umsetzen, darunter:

- Risikoanalysen und Sicherheitskonzepte
- Incident Management
- Business Continuity (Backup, Disaster Recovery, Krisenmanagement)
- Lieferkettensicherheit
- Sichere Entwicklung und Wartung
- Verschlüsselung und Kryptografie
- Schulungen (inkl. Management)
- Multi-Faktor-Authentifizierung (MFA)

B. Meldepflichten

Erhebliche Sicherheitsvorfälle müssen gestaffelt gemeldet werden:

- 24 Stunden: Frühwarnung
- 72 Stunden: Erste Bewertung
- 1 Monat: Abschlussbericht

C. Registrierungspflicht

- Registrierung beim BSI
- Benennung eines Ansprechpartners

D. Managementhaftung

Ein zentraler Wandel: Cybersicherheit wird zur Chefsache.

- Persönliche Verantwortung der Geschäftsleitung
- Keine Delegation möglich
- Pflichtschulungen
- Potenzielle persönliche Haftung

Sanktionen

- Wesentliche Einrichtungen: bis zu 10 Mio. € oder 2 % Umsatz
- Wichtige Einrichtungen: bis zu 7 Mio. € oder 1,4 % Umsatz

Wie Rapid7 die NIS2-Compliance unterstützt

Ähnlich wie bei der DSGVO erfordert die Einhaltung des deutschen NIS2UmsuCG eine Kombination verschiedener Cybersicherheitsfähigkeiten, um die umfassenden und durchsetzbaren Anforderungen des Gesetzes zu erfüllen.

Im Folgenden wird dargestellt, wie Rapid7 diese Anforderungen unterstützt:

NIS2-ANFORDERUNG	RELEVANTE RAPID7-LÖSUNG	RAPID7 BEITRAG ZUR ERFÜLLUNG
Risikoanalyse	Exposure Command – Schwachstellenmanagement und Cloud-Sicherheit	Exposure Command unterstützt direkt die technische Komponente der NIS2-Anforderungen an die Risikoanalyse, indem es daten- und kontextbasierte Einblicke in Expositionen liefert und den Fokus auf tatsächliche Risiken statt nur auf die Schwere von Schwachstellen legt.
Incident Management	InsightIDR (SIEM/XDR) und MDR-Service	Erkennung und Reaktion: InsightIDR fungiert als zentrales System für Logging und Alarmierung. Es erkennt Anomalien und potenzielle Sicherheitsverletzungen in Echtzeit. Falls internes Personal fehlt, bietet der Managed Detection and Response (MDR)-Service von Rapid7 eine 24/7-Überwachung und Reaktion und deckt damit direkt die Anforderung zur „Behandlung von Sicherheitsvorfällen“ ab.
Business Continuity (Krisenmanagement)	Incident Response (IR) Retainer	Krisenunterstützung: Während NIS2 Backup- und Disaster-Recovery-Maßnahmen vorschreibt, erfüllt der IR-Retainer von Rapid7 die Anforderungen an Incident Response und Krisenmanagement und stellt einen erprobten Wiederherstellungsprozess nach Störungen sicher.
Supply chain security	Surface Command und Cloud Security	Externe Transparenz: Surface Command schafft Transparenz über die digitale Lieferkette, indem es „Shadow Assets“ und externe Abhängigkeiten identifiziert, die als Einstiegspunkte dienen könnten. So lässt sich die Sicherheitslage von Drittanbieter-Verbindungen bewerten. Cloud Security stellt sicher, dass öffentliche Cloud-Umgebungen sicher und compliant betrieben werden.
Sicherheit in Beschaffung, Entwicklung und Wartung	Exposure Command – Application Security und Cloud Security	Secure by Design: Application Security (DAST) testet Webanwendungen während der Entwicklung (DevOps-Integration) auf Schwachstellen. Cloud Security prüft Infrastructure-as-Code (IaC), um sicherzustellen, dass Systeme bereits vor dem Deployment sicher sind („Shift Left“).
Kryptografie und Verschlüsselung	Exposure Command – Schwachstellenmanagement und Cloud Security	Policy Auditing: Die Lösungen verschlüsseln nicht selbst, sondern überprüfen die Umsetzung. Sie scannen Netzwerke und Cloud-Umgebungen gezielt auf unverschlüsselte Daten, schwache SSL/TLS-Zertifikate oder veraltete Protokolle und stellen sicher, dass Verschlüsselungsrichtlinien tatsächlich eingehalten werden. So lässt sich gegenüber Auditoren nachweisen, dass „State-of-the-Art“-Vorgaben technisch umgesetzt sind.
Cybersecurity-Trainings	• Advisory Services • Tabletop Schulungen	Management-Training: Rapid7 bietet Tabletop-Übungen an, die reale Angriffsszenarien simulieren. Diese richten sich gezielt an Management- und Führungsebene (wie von NIS2 gefordert), um Entscheidungsfähigkeit in Krisensituationen zu trainieren.
Multi-Faktor-Authentifizierung (MFA)	InsightIDR	Verifizierung: InsightIDR verarbeitet Authentifizierungslogs (z. B. von Okta oder Active Directory), um die Nutzung von MFA zu überwachen. Es kann warnen, wenn Administratoren sich ohne MFA anmelden oder Umgehungsversuche stattfinden, und liefert damit den Nachweis gegenüber Auditoren, dass MFA durchgesetzt wird.

Einordnung: Von Compliance zu kontinuierlicher Sicherheit

Moderne Cybersicherheitsgesetzgebung wie NIS2 – und ihre nationalen Umsetzungen, einschließlich des deutschen NIS2UmsuCG – belohnt keine Checkbox-Compliance mehr. Stattdessen verlangt sie kontinuierliche Transparenz, priorisierte Risikoreduktion und nachweisbare Reaktionsfähigkeit. Compliance ist kein punktueller Zustand mehr, sondern das Ergebnis eines ausgereiften, kontinuierlich betriebenen Sicherheitsprogramms.

Organisationen, die Compliance als Nebenprodukt starker Sicherheit betrachten und nicht als Endziel, sind am besten positioniert, um erfolgreich zu sein. Die Rapid7 Command Platform wurde genau nach diesem Prinzip entwickelt und ermöglicht es Unternehmen, die NIS2-Anforderungen operativ umzusetzen – durch einheitliche Transparenz über hybride Umgebungen hinweg, risikobasierte Priorisierung auf Basis von Bedrohungsinformationen sowie integrierte Erkennungs- und Reaktionsfähigkeiten.

Zentral für diesen Ansatz ist der Wandel hin zu Continuous Threat Exposure Management (CTEM). Anstatt sich auf periodische Schwachstellenscans oder statische Berichte zu verlassen, liefert Rapid7 die Echtzeit-Telemetrie und den Kontext, die erforderlich sind, um die Angriffsfläche kontinuierlich zu verstehen und zu reduzieren. Dies ist insbesondere im Kontext von Regelwerken wie dem NIS2UmsuCG relevant, da Organisationen gegenüber Regulierungsbehörden wie dem BSI nachweisen müssen, dass sie Cyberrisiken aktiv und fortlaufend steuern – und nicht nur dokumentieren.

Compliance ist kein einmal jährlich erstellter Bericht mehr, sondern wird zu einem lebendigen, messbaren Prozess, der durch kontinuierliche Risikoanalysen und operative Dashboards sichtbar wird.

Dieser Ansatz wurde von Branchenanalysten anerkannt: Rapid7 wurde im Gartner® Magic Quadrant™ 2025 für Exposure Assessment Platforms als Leader eingestuft.

Da sich regulatorische Anforderungen kontinuierlich weiterentwickeln, bleibt Rapid7 bestrebt, seine Plattform an neue Standards anzupassen und Kunden Funktionen sowie Richtlinienframeworks bereitzustellen, die sowohl die Zeit bis zur Compliance verkürzen als auch eine messbare Risikoreduktion ermöglichen.

Letztlich ist der Wandel nicht nur regulatorisch, sondern auch operativ und strategisch. Organisationen, die kontinuierliches Risikomanagement in ihre Sicherheitsprogramme integrieren, erfüllen nicht nur die Anforderungen von NIS2 und NIS2UmsuCG, sondern bauen auch die notwendige Resilienz und das Vertrauen auf, um sich in einer zunehmend komplexen Bedrohungslandschaft sicher zu bewegen.

Weitere Informationen

Wenn Sie mehr darüber erfahren möchten, wie Rapid7 Sie bei der Umsetzung der NIS2-Anforderungen unterstützen kann, besuchen Sie bitte:

https://www.rapid7.com/products/command/exposure-management/

oder wenden Sie sich an Ihren lokalen Rapid7-Ansprechpartner oder Partner.

ÜBER RAPID7

Rapid7, Inc. (NASDAQ: RPD) ist ein weltweit führender Anbieter von KI-gestützten Managed Cybersecurity Operations und unterstützt Unternehmen dabei, ihre Cyber-Resilienz nachhaltig zu stärken. Die offene und erweiterbare Rapid7 Command Platform integriert Sicherheitsdaten und reichert diese mit künstlicher Intelligenz, Threat Intelligence sowie über 25 Jahren Erfahrung und Innovation an, um Risiken zu reduzieren und Angreifer effektiv zu stoppen.Als anerkannter Marktführer im Bereich präventiver Managed Detection and Response (MDR) vereint Rapid7 Exposure Management und Angriffserkennung, um die Sicherheitsprozesse von mehr als 11.500 Kunden weltweit grundlegend zu transformieren.Weitere Informationen finden Sie auf unserer Website, in unserem Blog oder auf unseren Profilen bei LinkedIn und X.

RAPID7

SICHERN SIE IHRE

Cloud | Anwendungen | Infrastruktur | Netzwerk | Daten

BESCHLEUNIGUNG MIT

Command-Plattform | Exposure Management | Angriffsflächen-Management | Schwachstellen-Management | Cloudnativer Anwendungsschutz | Anwendungssicherheit | Next-Gen SIEM | Threat Intelligence | MDR-Services | Incident-Response-Services | MVM-Services

SICHERHEIT, UM ANGREIFERN EINEN SCHRITT VORAUS ZU SEIN

Testen Sie unsere Sicherheitsplattform risikofrei – starten Sie Ihre Testversion auf **rapid7.com**