becon GmbH

Hauptstraße 8b
82008 Unterhaching

www.becon.de
www.opencelium.io
www.datagerry.com

becon
we drive digital innovation

NIS2 CHECKLISTE

zur Erfüllung der neuen EU-Richtlinie

Praxisleitfaden zur Umsetzung der neuen EU-Vorgaben

Neue Anforderungen an Cybersicherheit

Die neue NIS2-Richtlinie bringt eine bedeutende Ausweitung der Anforderungen an die Cybersicherheit mit sich. Anders als ihr Vorgänger (NIS1) richtet sie sich nicht mehr nur an wenige, als „kritisch" eingestufte Infrastrukturen. Vielmehr rücken nun zahlreiche Unternehmen und Organisationen aus unterschiedlichsten Branchen in den Fokus: darunter Energie, Gesundheit, Transport, digitale Dienste, öffentliche Verwaltung und viele mehr.
Besonders relevant: Schon Betriebe mit mehr als 50 Mitarbeitenden oder mehr als 10 Millionen Euro Umsatz bzw. Jahresbilanzsumme fallen unter die Vorgaben – ganz gleich, ob sie bisher als „KRITIS" galten oder nicht.

Dieses Whitepaper gibt einen praxisorientierten Überblick über die Anforderungen und beschreibt Schritt für Schritt, wie sich Unternehmen systematisch auf die NIS2-Umsetzung vorbereiten können. Im Anschluss zeigen wir, wie das Open Source CMDB und Asset Management Tool **DataGerry** mit integriertem ISMS-Modul dabei unterstützen kann, regulatorische Vorgaben nicht nur zu erfüllen, sondern strukturiert und zukunftssicher umzusetzen.

Wer ist betroffen – und was bedeutet das konkret?

Die NIS2-Richtlinie gilt für Organisationen aus über einem Dutzend Sektoren – unter anderem Energieversorgung, Transport, Wasserwirtschaft, Gesundheit, Finanz- und Versicherungswesen, digitale Infrastruktur und IKT-Dienstleistungen.

Die entscheidende Neuerung gegenüber bisherigen Regelungen:

Die Richtlinie greift bereits ab einer bestimmten Unternehmensgröße. Wenn ein Unternehmen mindestens 50 Beschäftigte hat oder einen Jahresumsatz bzw. eine Bilanzsumme von mehr als 10 Millionen Euro erreicht, ist es mit hoher Wahrscheinlichkeit verpflichtet, sich mit NIS2 auseinanderzusetzen.

Es lohnt sich daher frühzeitig zu prüfen, ob das eigene Unternehmen betroffen ist – und wenn ja, in welchem Umfang. Dabei wird zwischen sogenannten „wichtigen" und „besonders wichtigen" Einrichtungen (Essential Entities und Important Entities) unterschieden. Die Abgrenzung basiert in erster Linie auf Sektorenzugehörigkeit (kritischer oder sonstiger relevanter Bereich), Größe des Unternehmens und Systemrelevanz der Tätigkeit. Die EU-Richtlinie listet in Anhang I und II konkret auf, welche Branchen unter welche Kategorie fallen.

Die Anforderungen sind in beiden Fällen hoch, allerdings ist bei „besonders wichtigen Einrichtungen" mit strengeren Kontrollen, Nachweispflichten und bei Verstößen mit hohen Bußgeldern zu rechnen.

Was fordert die NIS2-Richtlinie?

Im Kern verlangt NIS2 von betroffenen Organisationen, dass sie geeignete technische und organisatorische Maßnahmen zur Erhöhung ihrer Cybersicherheit umsetzen. Das Ziel: Systeme sollen widerstandsfähiger gegenüber Sicherheitsvorfällen werden.
Zu den zentralen Anforderungen gehören:

- Etablierung eines systematischen Risikomanagements
- Einführung technischer und organisatorischer Schutzmaßnahmen
  (z. B. Zugangskontrollen, Netzwerksicherheit, Patch- und Schwachstellenmanagement, Verschlüsselung sensibler Daten)
- Pflicht zur Meldung von Sicherheitsvorfällen innerhalb klar definierter Fristen
- Maßnahmen zur Schulung und Sensibilisierung von Mitarbeitenden
- Dienstleister und Lieferanten müssen aktiv in die Sicherheitsstrategie eingebunden werden
- Dokumentationspflichten und behördliche Nachweispflichten
  (z. B. Risikoanalysen, Maßnahmenpläne und deren Umsetzung, Vorfallsprotokolle, Schulungsnachweise, Lieferantenbewertungen)
- Klare Verantwortung der Geschäftsleitung für die Einhaltung der Vorgaben
- Notfall- und Krisenmanagement, Backup- und Wiederanlaufpläne
- Bußgelder und Sanktionen bei Nichteinhaltung

Sämtliche Anforderungen müssen nachvollziehbar dokumentiert und regelmäßig überprüft werden. Diese Dokumentation sollte zentral, strukturiert und revisionssicher erfolgen – etwa im Rahmen eines ISMS. Kein einmaliges Projekt also, sondern ein fortlaufender Managementprozess.

Ihre NIS2 Checkliste – Schritt für Schritt zur Umsetzung

Ausgangslage bewerten

Bevor Maßnahmen ergriffen werden, sollte geprüft werden, ob die NIS2-Richtlinie überhaupt auf das eigene Unternehmen zutrifft. Anschließend gilt es, Verantwortlichkeiten intern klar zuzuordnen. Eine GAP-Analyse hilft, bestehende Prozesse und Maßnahmen zu bewerten und mit den Anforderungen abzugleichen.

Ein ISMS aufbauen oder weiterentwickeln

Ein strukturiertes Informationssicherheits-Managementsystem (ISMS) bildet das Fundament jeder nachhaltigen Sicherheitsstrategie. Es umfasst Richtlinien, Verfahren und Werkzeuge zur systematischen Steuerung von Informationssicherheitsrisiken und sorgt dafür, dass Prozesse nicht nur aufgesetzt, sondern auch regelmäßig überprüft und verbessert werden.
Ein ISMS sollte risikobasiert sein, auf anerkannten Standards (z. B. ISO/IEC 27001, BSI IT-Grundschutz) beruhen und kontinuierlich überprüft werden. Auch kleinere Unternehmen profitieren von skalierbaren, schlanken ISMS-Ansätzen, sofern die Anforderungen dokumentiert, messbar und nachvollziehbar erfüllt werden.

Schutzmaßnahmen konkret umsetzen

Neben übergeordneten Strategien verlangt NIS2 auch konkrete technische Maßnahmen. Dazu gehören unter anderem Firewalls, Netzwerksegmentierung, Monitoring, rollenbasierte Zugriffskontrollen, Schwachstellenmanagement und regelmäßige Sicherheitsupdates.
Ebenso wichtig sind organisatorische Vorkehrungen, wie klar definierte Richtlinien zum Umgang mit IT-Systemen, Notfall- und Wiederherstellungspläne sowie geregelte Prozesse zur Rechtevergabe.
Alle Maßnahmen müssen dokumentiert, regelmäßig überprüft und an neue Bedrohungslagen angepasst werden. Ziel ist ein wirksames und überprüfbares Sicherheitsniveau, das über rein technische Lösungen hinausgeht.

Meldeprozesse aufsetzen

Bei sicherheitsrelevanten Vorfällen gilt eine Meldefrist von 24 Stunden für eine erste Meldung, 72 Stunden für weiterführende Informationen in einem Zwischenbericht und ein Monat für den Abschlussbericht. Das BSI (Bundesamt für Sicherheit in der Informationstechnik) agiert als zentrale Meldestelle und nationale Koordinationsstelle.Unternehmen sollten konkrete Schwellenwerte für Meldepflichten definieren (z. B. Ausfallzeiten, Datenverlust, Auswirkungen auf Dritte). Interne Meldewege, Ansprechpartner und Eskalationsketten müssen festgelegt und regelmäßig trainiert werden. Ergänzend dazu sind Notfallteams mit klaren Rollen und Entscheidungsbefugnissen zu bilden sowie Wiederanlaufpläne zu etablieren, die technische und organisatorische Maßnahmen zur schnellen Wiederherstellung des Geschäftsbetriebs beschreiben und regelmäßig getestet werden.

Mitarbeitende einbinden

Keine Sicherheitsmaßnahme funktioniert ohne das nötige Bewusstsein in der Belegschaft. NIS2 verlangt deshalb nicht nur regelmäßige Schulungen für IT-Fachkräfte, sondern auch die breite Sensibilisierung aller Mitarbeitenden – etwa im Umgang mit E-Mails, Passwörtern, mobilen Geräten und Cloud-Diensten.
Ergänzend sollten Schulungskonzepte für Führungskräfte sowie projekt- oder rollenbezogene Sicherheitsunterweisungen vorgesehen werden. Inhalte, Teilnahmen und Wirksamkeit sollten dokumentiert und überprüft werden.

Dienstleister und Lieferketten einbeziehen

Die Sicherheitsverantwortung endet nicht an der eigenen Bürotür. Auch IT-Dienstleister, Auftragsverarbeiter, Cloud-Anbieter, Systemlieferanten, Hosting-Partner und andere Externe müssen in die Sicherheitsarchitektur eingebunden werden. Dabei geht es u. a. um Sicherheitsanforderungen in Verträgen (SLA, AVV), regelmäßige Prüfungen und Audits, Notfallpläne bei Dienstleisterausfall und Risikoanalyse von Drittanwendungen und APIs.
Unternehmen sollten die Zusammenarbeit mit externen Partnern nicht als potenzielles Sicherheitsrisiko, sondern als integralen Bestandteil ihrer eigenen Schutzstrategie verstehen. Eine klare Dokumentation der Anforderungen, regelmäßige Überprüfungen und transparente Kommunikation mit Dienstleistern sind unerlässlich, um auch in komplexen Lieferketten ein konsistentes Sicherheitsniveau sicherzustellen.

Dokumentation sicherstellen und Nachweispflichten erfüllen

Ein zentrales Element der Richtlinie ist die Nachvollziehbarkeit. Unternehmen müssen gegenüber Behörden oder im Rahmen von Audits jederzeit in der Lage sein, ihre Schutzmaßnahmen, Entscheidungsprozesse, Zuständigkeiten und Reaktionsmaßnahmen nachvollziehbar zu belegen. Die Dokumentation sollte vollständig, strukturiert und versionssicher sein, in einem zentralen System gepflegt werden (z. B. ISMS- oder CMDB-Tool), regelmäßig überprüft und aktualisiert werden und technische sowie organisatorische Bereiche integrieren.

Fazit: Mit System zu mehr Cybersicherheit

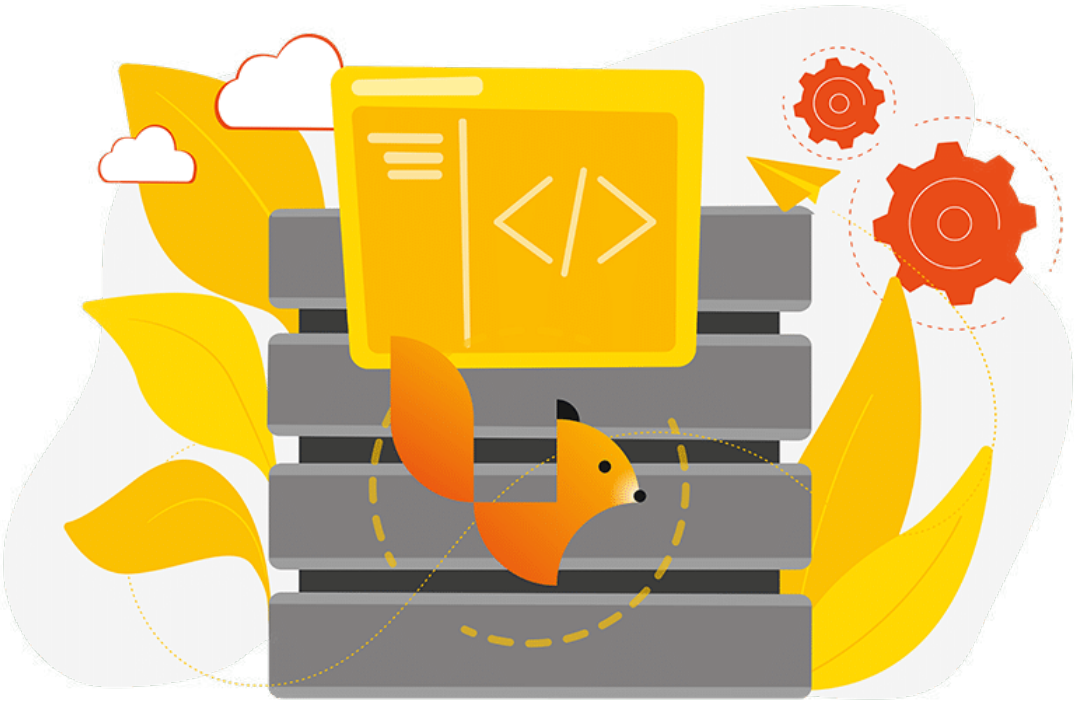
NIS2 bringt für viele Unternehmen neue Pflichten – aber auch die Chance, Informationssicherheit strukturiert und strategisch zu verankern. Wer die Umsetzung frühzeitig angeht, schafft die Voraussetzungen für mehr Resilienz, geringere Risiken und eine bessere Position im Wettbewerb.
Tools wie* DataGerry *unterstützen dabei, den Überblick zu behalten, zentrale Daten effizient zu verwalten und regulatorische Anforderungen nachvollziehbar zu erfüllen.

Strukturierte Umsetzung mit DATAGERRY

Die Umsetzung der NIS2-Richtlinie erfordert eine Vielzahl von strukturierten Informationen: über Systeme, Anwendungen, Verantwortlichkeiten, Prozesse, externe Dienstleister und deren Schnittstellen. Genau hier setzt DataGerry an und unterstützt Unternehmen dabei, ein ISMS praxisnah umzusetzen – von der strukturierten Risikobewertung über die Maßnahmenplanung bis zur revisionssicheren Nachweisführung.

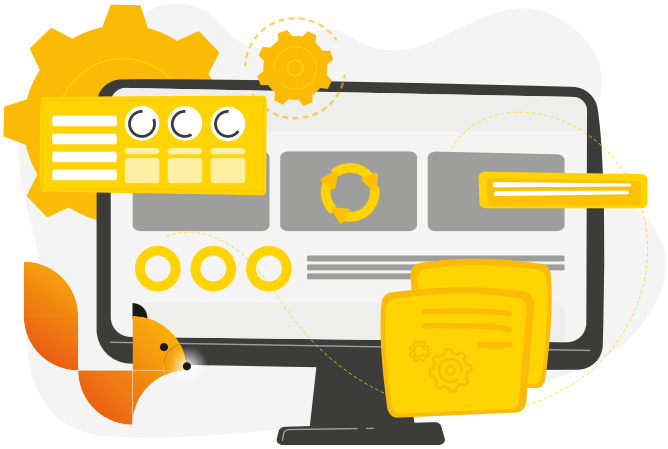
DataGerry ist eine flexible, quelloffene CMDB-Plattform zur Verwaltung strukturierter Informationen über technische Objekte, IT-Komponenten und deren Abhängigkeiten. Sie unterstützt Unternehmen dabei, individuelle Datenmodelle zu definieren und alle relevanten Informationen zentral und nachvollziehbar zu dokumentieren.

DataGerry bietet zwei Modelle: Eine kostenfreie Open-Source-Version für den On-Premise-Betrieb, sowie eine kostenpflichtige Cloud-Variante, die als SaaS-Lösung bereitgestellt wird. Beide Varianten ermöglichen eine sichere Verwaltung von Konfigurationsdaten nach höchsten Standards.



Die wichtigsten Funktionen von DataGerry

- Individuelle Objektdefinitionen über ein dynamisches Datenmodell
- REST API und Eventsystem zur Integration in bestehende ITSM-, ISMS- oder Monitoring-Umgebungen
- Benutzer- und Rollenverwaltung zur Steuerung von Zugriffsrechten
- Exporte und Automatisierungen über Skripte und Webhooks
- ISMS-Funktionalitäten zur zentralen Verwaltung sicherheitsrelevanter Assets und Prozesse für ISO-27001-konformes Arbeiten



Gerade für Unternehmen mit komplexen oder stark verteilten Infrastrukturen bietet DataGerry die nötige Transparenz, um den Anforderungen an Dokumentation, Nachweispflicht und strukturiertes Risikomanagement im Rahmen der NIS2-Richtlinie gerecht zu werden.

www.datagerry.com

Andreas Geist

Chief Solution Sales Officer, becon GmbH

info@datagerry.com
+49 (0) 89 608668-73
www.datagerry.com

DATA GERRY

Darum empfehlen wir DataGerry

Mit DataGerry können Sie Ihre IT-Assets und Abhängigkeiten zentral und transparent dokumentieren. So vermeiden Sie Dateninseln, reduzieren Risiken und steigern die Effizienz im Betrieb. Als Open-Source-Lösung bleiben Sie unabhängig und können das Tool exakt an Ihre Anforderungen anpassen.

Sie benötigen:

- Beratung zum Thema ISMS?
- Support bei der Umsetzung der NIS2-Richtlinie?
- Unterstützung bei der Einführung von DataGerry?

Sprechen Sie uns an. Wir beraten Sie gerne.

becon GmbH

Hauptstraße 8b
82008 Unterhaching

info@becon.de
T.: +49 (0) 89 608668-0

www.becon.de
www.datagerry.com
www.opencelium.io