DriveLock

NIS2

6 Punkte, die Sie jetzt wissen müssen

Einleitung

Wasser, Strom, Lebensmittel oder der öffentliche Nahverkehr sind für uns alltägliche Dinge, die jedoch lebensnotwendig sind. Die Versorgung mit diesen und weiteren unentbehrlichen Gütern und Dienstleistungen übernehmen in Deutschland sogenannte kritische Infrastrukturen – kurz KRITIS.

Dazu gehören beispielsweise die Energie- und Wasserversorgung, der Verkehr, aber auch die medizinische Versorgung. Wie bedeutsam kritische Infrastrukturen sind, erkennt man erst, wenn es zu Störungen kommt. Denn sie bilden die Grundlage für das Funktionieren unserer Gesellschaft.[1]

Das Risiko für Cyberangriffe auf Unternehmen, Organisationen und Einrichtungen mit kritischen Infrastrukturen (KRITIS) steigt durch die zunehmende Bedrohungslage aus dem Cyberraum und durch die aktuellen geopolitischen Entwicklungen.

Die Europäische Union verfolgt das Ziel, über den KRITIS-Sektor hinaus auch weitere „wesentliche und wichtige Einrichtungen" künftig besser zu schützen und ein EU-weit einheitliches, hohes Niveau an Cybersicherheit zu etablieren.[2]

Stand Oktober 2023

Auf den folgenden Seiten informieren wir Sie über sechs relevante Punkte zu NIS2, die Sie jetzt wissen müssen

1 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
2 Richtlinie (EU) 2022/2555 (NIS2)
3 digital-strategy.ec.europa.eu

NIS2

6 Punkte, die Sie jetzt wissen müssen

1

Was ist NIS2?

Was ist NIS2?

NIS2 ist eine EU-Richtlinie und steht für „Network and Information Systems Directive 2".

Sie verpflichtet EU-Mitgliedstaaten zur Entwicklung nationaler Cybersicherheitsstrategien und zur Einrichtung von Behörden und Anlaufstellen für Cybersicherheit. Darüber hinaus umfasst sie Richtlinien zur Netzwerk- und Informationssicherheit. Die Einführung von NIS2 erfolgte aufgrund der Erkenntnis, dass die vorherige Richtlinie NIS1 nicht ausreichend war und es an einer EU-weit einheitlichen Umsetzung der rechtlichen Anforderungen fehlte.

Das Hauptziel von NIS2 besteht darin, in der EU eine einheitliche Sicherheitskultur zu etablieren und das Cybersicherheitsniveau auf ein gemeinsames Level zu heben. Dies soll eine effektivere Reaktion auf Sicherheitsvorfälle ermöglichen. Durch die Umsetzung der Risikomanagementmaßnahmen können Sicherheitsvorfälle vermieden oder zumindest in ihren Auswirkungen minimiert werden.

Die Mitgliedsstaaten haben bis Oktober 2024 Zeit, NIS2 in nationales Recht umzusetzen, und Unternehmen und Organisationen müssen diese neuen Vorschriften dann rechtlich verbindlich einhalten.

Der Referentenentwurf des NIS2UmsuCG-Gesetzes vom 23. April 2023 zielt darauf ab, die durch NIS2 festgelegten Anforderungen in der Bundesverwaltung umzusetzen und die Cybersicherheit zu stärken. Das ist entscheidend für die Wirtschaft, die soziale Stabilität und die politische Sicherheit.[1]

Die NIS2-Richtlinie hat das Ziel, ein hohes einheitliches Cybersicherheitsniveau insbesondere für kritische Einrichtungen, Dienstleister und Behörden in der EU zu erreichen.[2]

1 Referentenentwurf NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)
2 digital-strategy.ec.europa.eu

NIS2 – die wichtigsten Änderungen im Überblick

Die wichtigsten Änderungen Im Vergleich zur vorherigen EU-Richtlinie NIS1

Wer betroffen ist

» Erweiterter Adressatenkreis auf insgesamt 18 Sektoren, darunter Unternehmen mit mindestens 50 Beschäftigten und einem Mindestjahresumsatz von 10 Mio. Euro

Einbezug des Managements der betroffenen Unternehmen

» Betont die Verantwortung des Managements und sieht schärfere Sanktionen für Verstöße vor

Konkrete Vorgaben im Bereich Cybersicherheit

» Konkretere Vorgaben für Maßnahmen bezüglich Cybersicherheit, die Unternehmen ergreifen müssen

Meldepflichten

» Dreistufige Meldepflichten für erhebliche Sicherheitsvorfälle mit entsprechenden Sanktionen[1]

Staatliche Kontrolle

» Erweiterung der Befugnisse des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur Aufsicht

Juristisches

» NIS2 ist keine Verordnung und somit nicht unmittelbar in den Mitgliedsstaaten anwendbar. Sie muss in das nationale Cybersicherheitsrecht umgesetzt werden.[2]

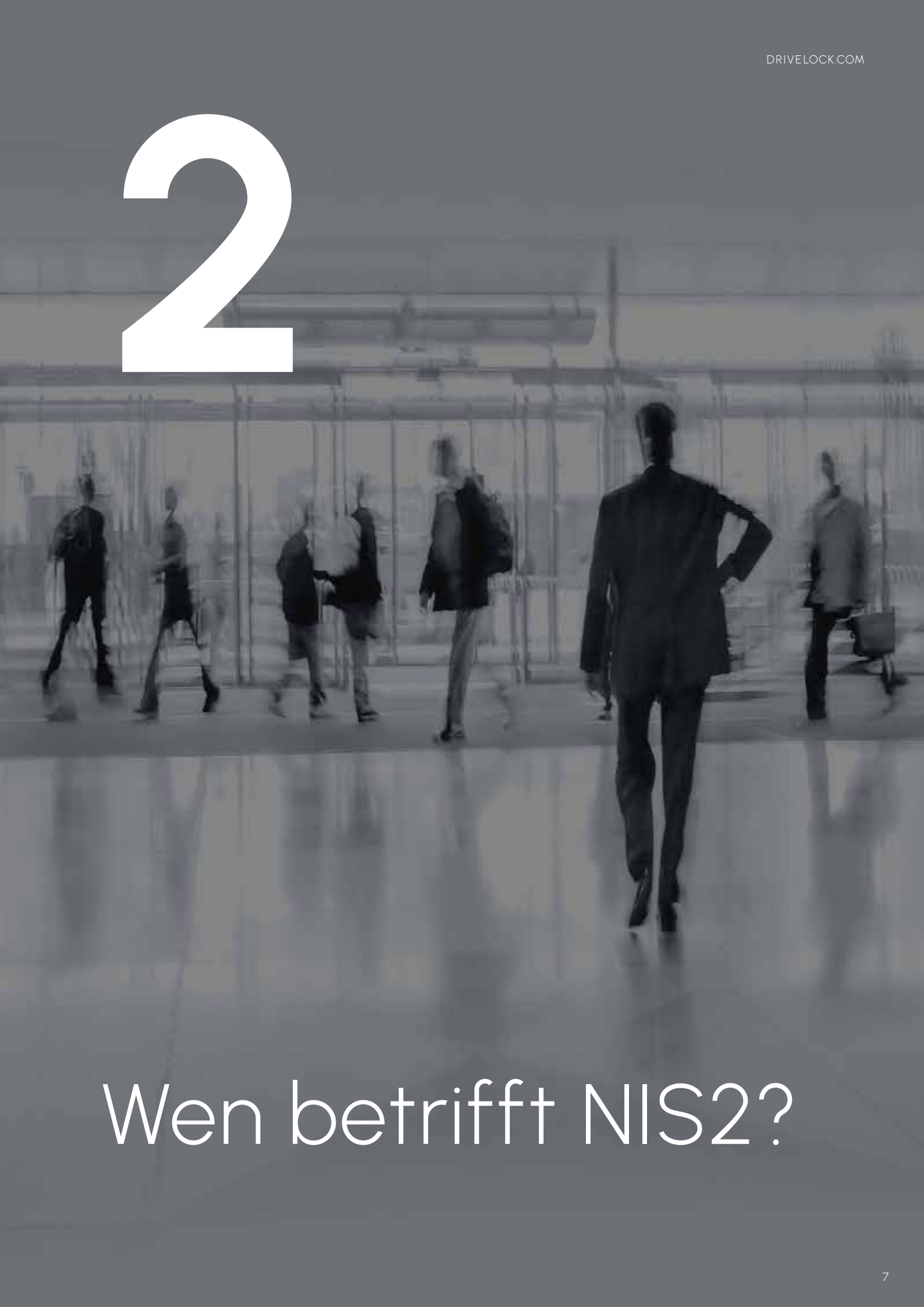
» Klare Strukturierung des BSI-Gesetzes

Die EU-Richtlinie NIS2 muss bis Oktober 2024 in nationales Recht in den EU-Mitgliedsstaaten umgesetzt werden. Der Referentenentwurf des NIS2UmsuCG-Gesetzes zielt darauf ab, diese Anforderungen in der Bundesverwaltung umzusetzen.

Auf nationaler Ebene spielt das BSI-Gesetz (BSIG)[3] eine führende Rolle. Dieses Gesetz wurde in der Vergangenheit mehrfach aktualisiert. Der aktuelle Referentenentwurf, NIS2UmsuCG, wird voraussichtlich das BSI-Gesetz um die NIS2-Anforderungen erweitern.

1 Zeile 462 ff. § 31 Meldepflichten
2 Verordnungen wie beispielsweise GDPR sind dagegen unmittelbar anwendbar.
3 BSI-Gesetz

2



Wen betrifft NIS2?

NIS2 Anwendungsbereich

NIS2 formuliert einen erweiterten Anwendungsbereich als bisher. Die Sektoren umfassen nach wie vor alte Bekannte, wie Versorger und Gesundheitswesen, aber auch neue Player wie die öffentliche Verwaltung oder Nischenbranchen wie Weltraum. Eine wesentliche Erweiterung hat der Bereich der digitalen Infrastruktur erfahren, welchem beispielsweise Cloud-Provider oder Rechenzentren zuzuordnen sind.

Mitgliedsstaaten

Die Mitgliedsstaaten sind aufgefordert:

» Nationale Cybersicherheitsstrategien zu entwickeln.
» Behörden für Cybersicherheit einzurichten.
» Anlaufstellen für Cybersicherheit einzurichten.

Personen

NIS2 betrifft:

» Geschäftsführer
» Chief Information Security Officers (CISOs)
» IT-Sicherheitsverantwortliche

Branchen und Sektoren

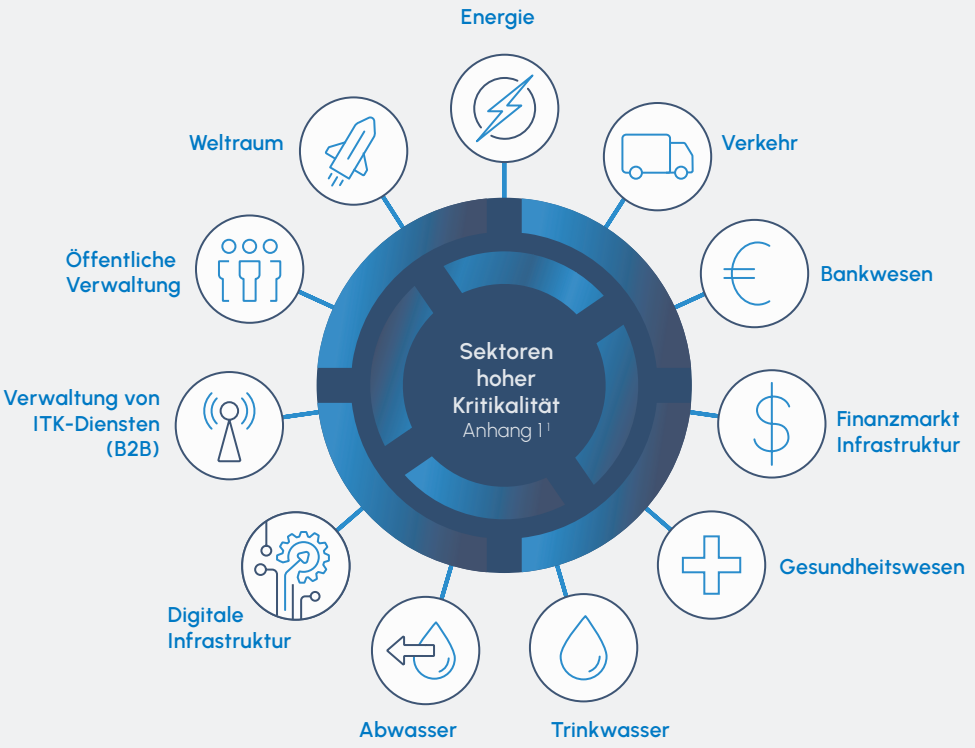
Betroffen sind alle Unternehmen, die folgende Kriterien erfüllen:

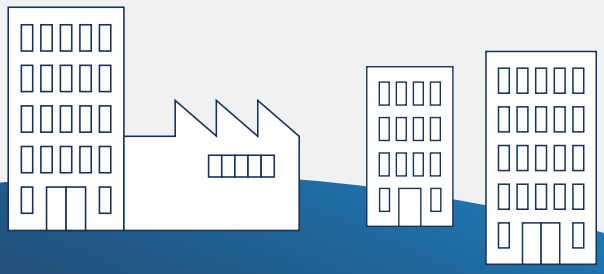
» Beschäftigung von mindestens 50 Mitarbeitenden
» Ein Mindestjahresumsatz von 10 Mio. EUR

NIS2 gliedert die betroffenen Wirtschaftszweige in „besonders wichtige" und „wichtige" Branchen bzw. Sektoren hoher Kritikalität und sonstige kritische Sektoren. Nationale Gesetzgeber können zusätzliche konkrete Einrichtungen benennen.

NIS2 Anwendungsbereich

Dienstleister und Lieferanten der folgenden Branchen sind betroffen





Pflichten und Sanktionen innerhalb der Sektoren variieren je nach Größe und wirtschaftlicher Leistungsfähigkeit:

Wesentliche Einrichtung

Sektor in Anhang 1

- Minimum 250 Beschäftigte
  oder
- mehr als 50 Mio. EUR Jahresumsatz
- Sonderfälle
  z. B. Zentralregierung, DNS-Diensteanbieter oder staatliche Einstufung als wesentliche Einrichtung

Wichtige Einrichtung

Sektor in Anhang 1 und 2

- Minimum 50 Beschäftigte
  oder
- mehr als 10 Mio. EUR Jahresumsatz
- Größenunabhängige Sonderfälle
  z. B. staatliche Einstufung als wichtige Einrichtung

1 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#d1e32-143-1
2 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#d1e32-148-1

3 Legal & Compliance

Neue Rechtslage

Der EU-Gesetzgeber schränkt den Spielraum der Mitgliedstaaten ein und gibt vor, welche Einrichtungen betroffen sind.

NIS2 gilt für öffentliche und private Einrichtungen in nunmehr 18 Sektoren.

Die Sektoren sind in den Anhängen I (Sektoren mit hoher Kritikalität) und II (Sonstige kritische Sektoren) konkretisiert.

Compliance

Geschäftsführer sind verpflichtet, alle Maßnahmen zur Einhaltung von Artikel 21 zu billigen und deren Durchführung zu überwachen. Geschäftsführer könnten in der nationalen Rechtsprechung für Verstöße gegen Artikel 21 haftbar gemacht werden. Ein Verzicht auf Ersatzansprüche oder Vergleiche soll unwirksam sein.[1]

Die Geschäftsleitung ist verpflichtet, regelmäßig an Schulungen teilzunehmen, um Kenntnisse und Fähigkeiten zur Erkennung, Bewertung und Minimierung von Risiken im Bereich Cybersicherheit zu erwerben. Dies soll auch für Mitarbeitende in Betracht gezogen werden.

Bußgelder für Verstöße sind gestaffelt:

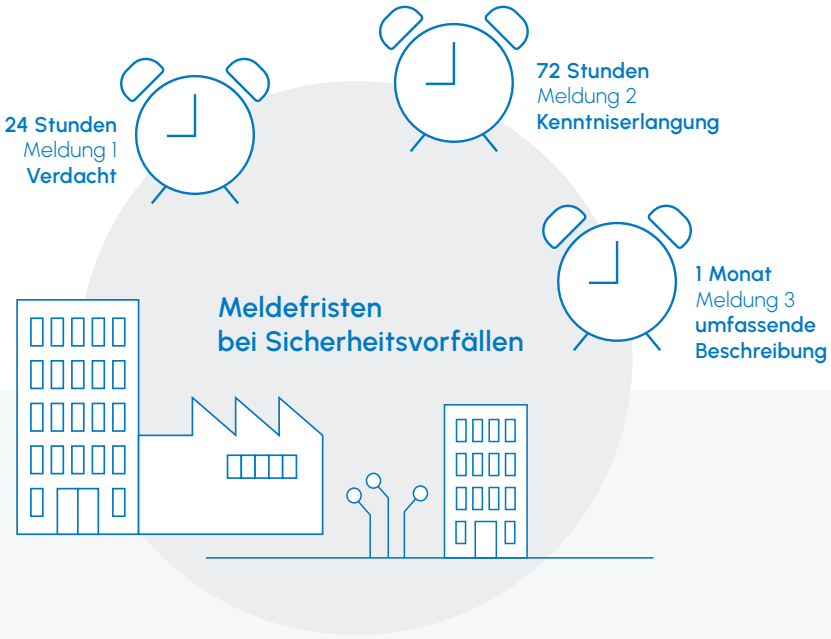
- Wichtige Einrichtungen:
  Unter 7 Mio. EUR oder 1,4 % des Umsatzes
- Besonders wichtige Einrichtungen oder KRITIS-Betreiber:
  Unter 10 Mio. EUR oder 2 % des gesamten weltweiten Vorjahresumsatzes

1 NIS2 Art. 21 (2)

4

Meldepflichten bei Sicherheitsvorfällen

NIS2 – Meldepflichten bei Sicherheitsvorfällen



Unternehmen müssen bei schwerwiegenden Sicherheitsvorfällen dreistufige Meldepflichten beachten, die bei Betriebsstörungen oder finanziellen Verlusten gelten. Verspätete Meldungen können zu Sanktionen führen. Daher ist es ratsam, ein Meldekonzept zu etablieren, um die knappen Fristen einzuhalten.

Die Meldungen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) müssen folgende Informationen enthalten:

Meldung 1
Innerhalb von 24 Stunden nach Kenntniserlangung:
Erstmeldung über den Vorfall, inklusive Verdacht auf rechtswidrige Handlungen oder grenzüberschreitende Auswirkungen.

Meldung 2
Innerhalb von 72 Stunden nach Kenntniserlangung:
Bestätigte oder aktualisierte Meldung mit erster Bewertung des Vorfalls, Schweregrad, Auswirkungen und Kompromittierungsindikatoren.

Meldung 3
Innerhalb eines Monats nach der Erstmeldung eines Sicherheitsvorfalls müssen Unternehmen eine Abschlussmeldung abgeben. Diese enthält eine detaillierte Beschreibung des Vorfalls, Angaben zur wahrscheinlichen Ursache, zu den ergriffenen Maßnahmen und gegebenenfalls zu den grenzüberschreitenden Auswirkungen.

5

Maßnahmen im Risikomanagement

NIS2 – Regelung des Risikomanagements

1. Gefahrenanalyse

Die Gefahrenanalyse erfordert im ersten Schritt eine umfassende Bestandsaufnahme möglicher physischer und digitaler Gefahrenquellen.

Zu den physischen Gefahren gehören unter anderem Diebstahl, Feuer und Stromausfälle. Bei der Analyse verlangt NIS2, dass der Stand der Technik berücksichtigt wird.

Dies bedeutet, dass eine kontinuierliche Evaluierung und kontinuierliche Verbesserung der getroffenen Maßnahmen erforderlich sind.

2. Konkrete Schutzmaßnahmen

Um sich vor Cyberangriffen und dem Verlust wertvoller Daten zu schützen, müssen „Wesentliche" und „Wichtige Einrichtungen" konkrete Schutzmaßnahmen implementieren, die ein aktives Risikomanagement in Bezug auf die jeweiligen Cybergefahren gewährleisten.

Diese Maßnahmen sollen...

- » ...Sicherheitsvorfälle verhindern oder ihre Auswirkungen minimieren.
- » ...angemessene technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für ihre Netz- und Informationssysteme zu kontrollieren
- » ...dem Stand der Technik entsprechen und ggfs. einschlägige europäische und internationale Normen berücksichtigen, z. B. ISO 27001/2
- » ...ein Sicherheitsniveau bieten, das zum bestehenden Risiko passt, wobei Faktoren wie Risikoexposition, Einrichtungsgröße und die Wahrscheinlichkeit von Sicherheitsvorfällen berücksichtigt werden

Bis zum 17. Oktober 2024 werden genaue technische und methodische Anforderungen festgelegt, die beschreiben, wie bestimmte Dienstanbieter im Internet, Cloud-Computing, Rechenzentrumsdienste, verwaltete Dienste, Sicherheits-dienste, Online-Marktplätze, Suchmaschinen, soziale Netzwerke und Vertrauensdienste ihre technischen und organisatorischen Sicherheitsmaßnahmen gestalten sollen.

Nach Feststellung, dass ein Unternehmen von NIS2 betroffen ist, müssen spezifische Schritte unternommen werden. NIS2 sieht ein zweistufiges Vorgehen vor. Zunächst müssen Betriebe ihre Gefahrensituation analysieren. Im zweiten Schritt müssen Einrichtungen auf Grundlage dieser Analyse konkrete Maßnahmen ergreifen.

Konkrete Schutzmaßnahmen

Die konkreten Maßnahmen im Risikomanagement laut NIS2 Artikel 21 Abs. 2 sollen dazu beitragen, die Cybersicherheit zu erhöhen und die Einhaltung der NIS2-Richtlinie sicherzustellen. Diese Maßnahmen umfassen die folgenden Punkte.[1]

Richtlinien
Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme

Incident Management
Bewältigung von Sicherheitsvorfällen

Prevention & Detection
Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen

Business Continuity
Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement

Supply Chain
Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern

Zero Trust
Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung

DLP / Verschlüsselung
Konzepte und Verfahren für den Einsatz von Kryptografie und ggfs. Verschlüsselung

Awareness
Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit

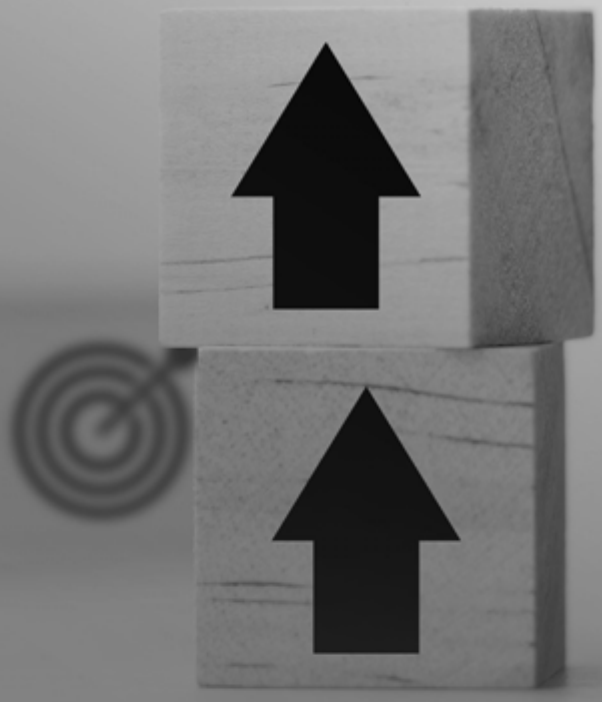
Access Control
Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen

Risk & Compliance
Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit

NIS2

1 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#d1e3335-80-1

6



Ihre Schritte zum Erfolg

Welche konkreten Schritte gibt es zu tun?

NIS2 verlangt, dass die Maßnahmen den Stand der Technik unter Berücksichtigung einschlägiger europäischer und internationaler Normen einhalten. Aktuell gibt es jedoch keine konkreten Vorgaben zu den erforderlichen Maßnahmen und Umsetzungsanleitungen.

In dieser Übergangszeit können sich Unternehmen und Organisationen an anderen bewährten Regelwerken und Standards orientieren, darunter:

» IT-Grundschutz des BSI[1]
» Normenreihe ISO 27000
» Zero Trust Maturity Model der CISA
» ISO/IEC 27001:2022 Annex 1 und ISO 27002
» NIST Cybersecurity Framework
» CIS Critical Security Controls
» BSI-Gesetz

Aus unserer Perspektive gibt es fünf Aspekte, die alle von NIS2 betroffenen Unternehmen, Organisation und Einrichtungen jetzt berücksichtigen sollten: Eine Anleitung in fünf Schritten finden Sie auf den folgenden Seiten.

1 www.bsi.bund.de

Ihre 5 Schritte zum Erfolg

Sensibilisierung der Geschäftsleitung

Die Geschäftsleitung muss sich ihrer Rolle und Verantwortung in Bezug auf Cybersicherheit bewusst sein. Dies ist der wichtigste Schritt, um sicherzustellen, dass die erforderlichen Maßnahmen zur Einhaltung von NIS2 aktiv unterstützt und genehmigt werden. Fahrlässigkeit bei der Umsetzung kann zu Haftung für Schäden oder Strafen nach Cyberattacken führen.

Analyse des aktuellen Zustands

Eine genaue Analyse des aktuellen Zustands des Unternehmens in Bezug auf Informationssicherheitsrisiken ist unerlässlich. Dies beinhaltet die Identifizierung aller relevanten Unternehmensressourcen, darunter Hardware, Räumlichkeiten, IT-Geräte, Software-Anwendungen und externe Cloud-Dienste. Diese Informationen dienen als Grundlage für eine erste Risikoeinschätzung.

Übersicht über Prozesse und Verantwortlichkeiten

Identifizieren Sie die wichtigsten Prozesse in Ihrem Unternehmen. Weisen Sie jeden Prozess einem Prozessverantwortlichem zu, der in der Lage ist, die Prozesse und die damit verbundenen Informationen und Vermögenswerte zu beschreiben. Dies ermöglicht eine Verknüpfung der gesammelten Daten mit den Prozessen und die Ableitung von Risiken.

Beurteilung von Lieferketten und von externen Dienstleistern

Die NIS2-Richtlinie fordert, dass Lieferketten und Dienstleister in die Risikobeurteilung einbezogen werden. Daher ist es notwendig, alle externen Serviceunternehmen zu identifizieren und einzeln zu bewerten. Dieser Prozess erfordert Zeit und Vertrauen, da Nachweise erbracht und Informationen ausgetauscht werden müssen, um die Umsetzung der Informationssicherheitsstrategie eines Dienstleisters beurteilen zu können. Zertifizierungen werden voraussichtlich eine wichtige Rolle spielen.

Etablierung eines Meldekonzepts

Die Etablierung eines Meldekonzepts ist von entscheidender Bedeutung, um sicherzustellen, dass Unternehmen und Organisationen angemessen auf schwerwiegende Sicherheitsvorfälle reagieren können. Dieses Meldekonzept sollte klare Richtlinien und Verfahren für die Erfassung, Bewertung und Meldung von Sicherheitsvorfällen festlegen, um eine effektive Reaktion und Zusammenarbeit sowohl intern als auch extern zu ermöglichen. Unternehmen sollten ihre Mitarbeitenden entsprechend schulen und sensibilisieren, um sicherzustellen, dass sie sich der Meldepflicht bewusst sind und wissen, wie sie im Falle eines Sicherheitsvorfalls handeln sollen. Ein gut durchdachtes Meldekonzept trägt dazu bei, die Auswirkungen von Sicherheitsvorfällen zu minimieren und die Gesamtsicherheit Ihrer Netzwerke und Informationssysteme zu stärken.

NIS2

EU-weite Gesetzgebung zur Cybersicherheit

Fazit

Die EU führte am 13. Januar 2023 die strengere NIS2-Richtlinie ein, da die bisherige NIS1-Richtlinie unzureichend ist. Mitgliedsstaaten sind aufgefordert, die Vorgaben bis Oktober 2024 in nationales Recht zu überführen. Ziel ist es, ein hohes einheitliches Cybersicherheitsniveau insbesondere für kritische Einrichtungen, Dienstleister und Behörden in der EU zu erreichen.

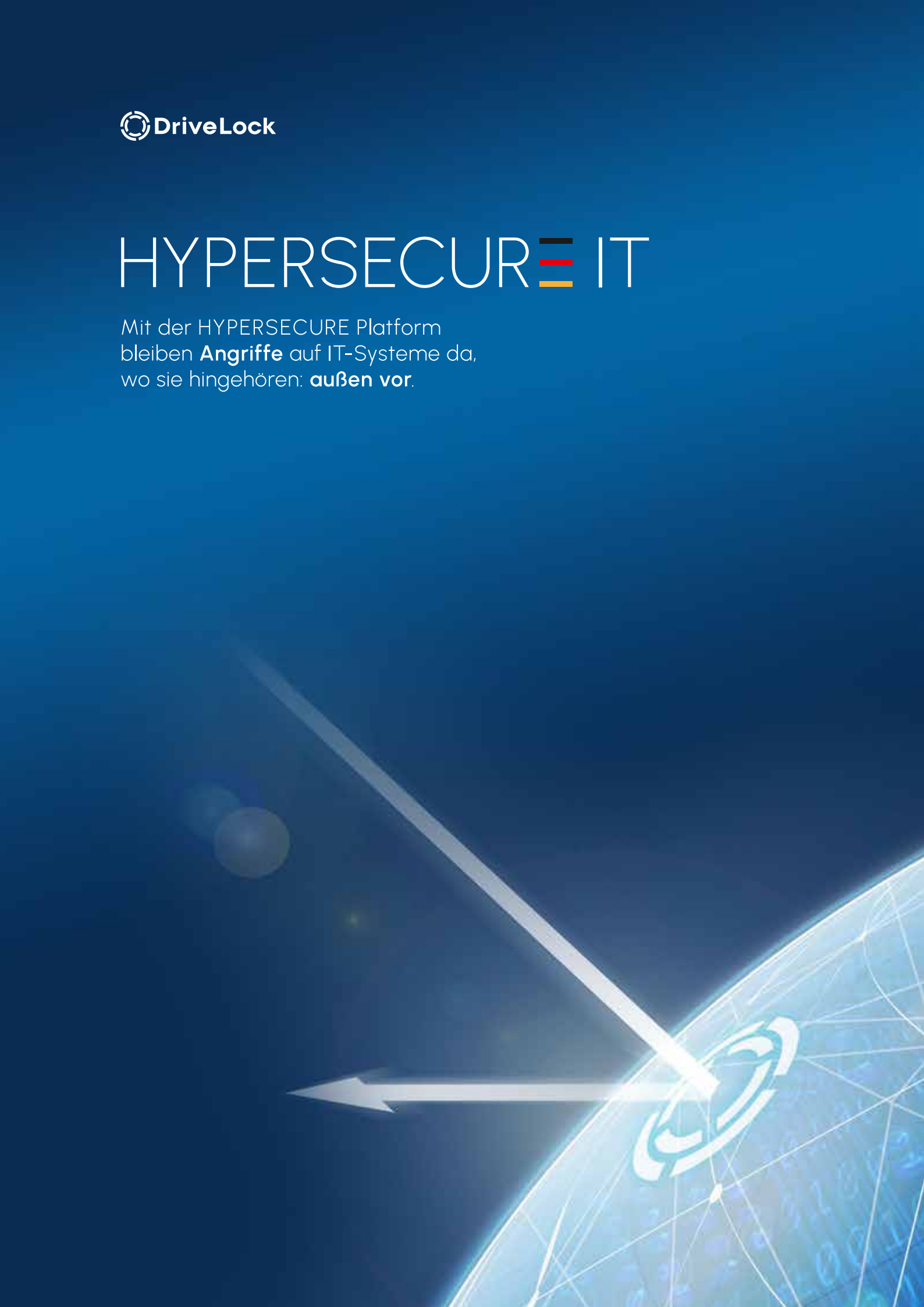
Insgesamt sind 18 Sektoren betroffen und somit ein deutlich erweiterter Adressatenkreis von Unternehmen mit mindestens 50 Beschäftigten und einem Mindestjahresumsatz von 10 Mio. Euro. Nationale Gesetzgeber können zusätzliche konkrete Einrichtungen benennen, die sie als „Wesentliche" oder „Wichtige" Einrichtungen einstufen und als solche reguliert werden sollen.
NIS2 ist mit konkreten Vorgaben zu den Mindestanforderungen an Risikomanagementmaßnahmen, einer verstärkten Verantwortung des Managements und zeitlich eng definierten Meldefristen verbunden. Bei Nichtbeachtung drohen empfindliche Geldstrafen.

Nicht nur die betroffenen Unternehmen selbst müssen effektive Maßnahmen zum Schutz der Informationssicherheit umsetzen, sie sind auch gefordert eine Sicherheitsbewertung aller Lieferanten und Dienstleister vorzunehmen und in ihre Risikobeurteilung miteinzubeziehen. Auch wenn die NIS2 Richtlinie keine konkreten Checklisten für Sicherheitsmaßnahmen liefert, bieten vorhandene Modelle wie der BSI IT-Grundschutz oder die ISO 27000 Normenreihe Best Practice Vorgaben, die entsprechende Security Controls enthalten, um das Informationssicherheitsrisiko dauerhaft und nachweislich zu reduzieren. DriveLock bietet Kunden bereits heute eine Vielzahl dieser Security Controls und kann die hohe Sicherheit seiner Produktentwicklung durch Zertifizierungen nachweisen. Insgesamt tragen umfassende Sicherheitskontrollen dazu bei, die Integrität, Verfügbarkeit und Vertraulichkeit von Systemen und Daten zu gewährleisten. Die Kombination von Präventions-, Erkennungs- und Reaktionsmechanismen bildet eine robuste Verteidigungslinie gegen eine Vielzahl von Cyberbedrohungen.

DriveLock

HYPERSECURE IT

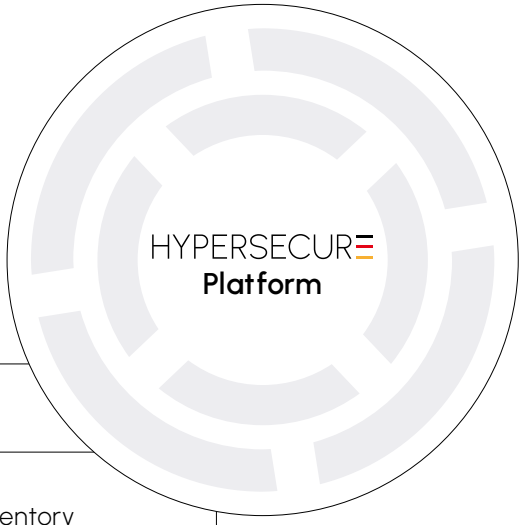
Mit der HYPERSECURE Platform
bleiben **Angriffe** auf IT-Systeme da,
wo sie hingehören: **außen vor**.



DriveLock

Ihre Cybersicherheit mit DriveLock

Die DriveLock HYPERSECURE Platform und ihre Module zielen darauf ab, die in ISO 27001 Annex A aufgeführten kritischen Sicherheitskontrollen mit einer umfassenden und kontext-bezogenen Sicherheitsstrategie anzugehen.



Welches DriveLock Modul übernimmt welchen Bereich der kritischen Sicherheitskontrollen

Security Control	DriveLock Modul
Inventory	Discovery Hardware & Software Inventory
Media Protection	Device Control
Malware Defense	Application Control Defender Antivirus
Secure Configuration	Security Configuration Management
Data Protection	Encryption BitLocker Management
Security Awareness	Security Awareness Campaigns
Vulnerability Management	Vulnerability Management
Privilege Control	User & Groups Management / SSO
Incident Response	Threat Detection & Response MITRE ATT&CK® Framework

HYPERSECURE IT

MADE IN GERMANY

Jetzt unverbindlich
30 Tage gratis testen

Testversion

Sprechen Sie mit
einem unserer Experten

Termin

HYPERSECURE mit DriveLock

HYPERSECURE IT aus Deutschland: DriveLock ist der führende Spezialist für präventive IT-Sicherheitslösungen aus Deutschland. Die digitalisierte Welt erfordert kompromisslose IT-Sicherheit, um Organisationen, Menschen und Dienste vor Cyberrisiken und Datenverlust zu schützen und digitales Arbeiten für alle sicher zu gestalten.

Die HYPERSECURE Platform von DriveLock gleicht einer schlagkräftigen Counter-Force aus spezialisierten Abwehrkräften, die in ihrer jeweiligen Disziplin zu den besten zählen. Sie bietet mehrschichtige Sicherheit, ist cloud-basiert, sofort verfügbar und wirtschaftlich effizient mit niedrigen Investitions- und Betriebskosten.

Die neue **Hochleistungsklasse der IT-Sicherheit** schützt digitale Arbeitsplätze konsequent und schafft Synergien aus den folgenden Elementen:

» **Data & Endpoint Protection**

» **Data Loss Prevention**

» **Data Encryption**

» **Security Awareness**

» **Risk & Vulnerability Management**

» **Security Configuration Management**

Die DriveLock-Lösungen Device Control und Application Control sind nach Common Criteria EAL3+ zertifiziert: Diese international anerkannte Zertifizierung attestiert die hohe Vertrauenswürdigkeit und den Sicherheitsstandard des DriveLock Agents.

DriveLocks wegweisende Tools und ein engagiertes Team sorgen dafür, dass Cyberattacken dort bleiben, wo sie hingehören: außen vor.

Erfahren Sie mehr und besuchen Sie uns auf drivelock.com.

DriveLock Lösungen sind Made in Germany und ohne Backdoor.

» Schutz von mehreren Millionen verwalteter Endgeräte weltweit

» Kompromisslos abgesicherte Kundenumgebungen mit über 180.000 verwalteten Endgeräten

» Made in Germany: Entwicklung und technischer Support aus Deutschland

HYPERSECURE IT

ISG – Leader Data Leakage/Loss Prevention 2023
Als Ergebnis der Marktuntersuchung „Cyber Security – Solutions & Services Germany 2023" des Technologieberatungsunternehmens ISG wurde DriveLock erneut als ein Leader im Segment „Data Leakage/Loss Prevention" ausgezeichnet.

techconsult – Champion Endpoint Protection 2022
In der Anwenderbefragung „Professional User Rating Security Solutions 2022 (PUR-S)" des Analystenhauses techconsult positionierten mehr als 2.000 Anwenderunternehmen DriveLock als Champion im Bereich Endpoint Protection unter 37 IT-Lösungsanbietern und deren Lösungen in Deutschland.

DriveLock SE
Landsberger Str. 396
81241 München

Tel. +49 (89) 546 36 49-0
E-Mail info@drivelock.com

DRIVELOCK.COM

HYPERSECURE IT

Mit der HYPERSECURE Platform
bleiben **Angriffe** auf IT-Systeme da,
wo sie hingehören: **außen vor**.