Die neue Richtlinie NIS2 – Schutz vor Hackerangriffen

Das Europäische Parlament in Brüssel und der EU-Rat in Straßburg haben dem Entwurf für die **überarbeitete Richtlinie zur Sicherheit von Netz- und Informationssystemen (NIS2)** zugestimmt. Die neue Direktive soll Netz- und Informationssysteme in Europa besser vor Hackerangriffen schützen. Alle 27 EU-Mitgliedsstaaten müssen die Vorgaben nun in nationales Recht überführen.

Was genau verbirgt sich hinter NIS und NIS2?
Bei **NIS** handelt es sich um die **„EU Network and Information Security Directive"**. Diese Richtlinie hat die bis dahin bestehenden Cybersicherheitskapazitäten auf nationaler Ebene verbessert, da die EU-Mitglieder staatliche Sicherheitsstrategien aufstellen und entsprechende Behörden benennen mussten. In Deutschland wurde die NIS-Direktive 2017 unter anderem mit dem IT-Sicherheitsgesetz umgesetzt, das inzwischen durch das IT-Sicherheitsgesetz 2.0 abgelöst ist.
Mit dem Entwurf zu NIS2 will die EU der verschärften Bedrohungslage und den wachsenden Anforderungen im Cyberraum Rechnung tragen. Dazu ist der aktuelle Rechtsrahmen modernisiert und erweitert worden.

Für wen ist die NIS2 Richtlinie relevant?
NIS2 erweitert die betroffenen Bereiche auf 11 Essential (wesentliche) und 7 Important (wichtige) Sektoren:
Essential: Energie, Transport, Banken, Finanzmärkte, Gesundheit, Trinkwasser, Abwasser, Digitale Infrastruktur, Öffentliche Verwaltung und Raumfahrt.
Important: Post und Kurier, Abfallwirtschaft, Chemikalien, Ernährung, Industrie (Herstellung), Digitale Dienste und Forschung.

BT Nord Systemhaus GmbH
Siemensstr. 28, 25813 Husum
+49 4841 89680
info@btnord.de
www.btnord.de

Geschäftsführer:
Thomas Holst, CEO,
Dipl.-Ing.(FH) Thies Kracht, CTO
Prokurist:
Frank Thomsen

Amtsgericht Flensburg
HRB 354 HU

Umsatzsteuer-ID:
DE134657285

Bankverbindungen:
Nord-Ostsee Sparkasse
BIC: NOLADE21NOS
IBAN: DE70 2175 0000 0186 0948 19

VR Bank Westküste eG
BIC: GENODEF1HUM
IBAN: DE70 2176 2550 0004 0133 36

Was kommt auf die Betroffenen zu?
Neben der Erweiterung des Adressatenkreises von kritischen Sektoren hin zu wesentlichen und wichtigen Sektoren sind vor allem die Vorschriften für Aufsichtsmaßnahmen, Zusammenarbeit und Kooperation sowie die Anforderungen an das Risikomanagement verschärft worden.
Mit NIS2 wird Unternehmen ein Risikomanagementkonzept vorgeschrieben, in dem grundlegende Sicherheitselemente enthalten sind. Es gibt klare Bestimmungen zu Meldeverfahren von Cybervorfällen, den Inhalten der Berichte und den Fristen.

Anforderungen der NIS2 Richtlinie für Unternehmen

Achtung: Sanktionen und Strafen werden deutlich ausgeweitet! Es drohen – abhängig vom Sektor - Maximalstrafen von mindestens 7 bis 10 Mio. Euro oder 2 % des weltweiten Jahresumsatzes.

BT Nord Systemhaus GmbH
Siemensstr. 28, 25813 Husum
+49 4841 89680
info@btnord.de
www.btnord.de

Geschäftsführer:
Thomas Holst, CEO,
Dipl.-Ing.(FH) Thies Kracht, CTO
Prokurist:
Frank Thomsen

Amtsgericht Flensburg
HRB 354 HU

Umsatzsteuer-ID:
DE134657285

Bankverbindungen:
Nord-Ostsee Sparkasse
BIC: NOLADE21NOS
IBAN: DE70 2175 0000 0186 0948 19

VR Bank Westküste eG
BIC: GENODEF1HUM
IBAN: DE70 2176 2550 0004 0133 36

Wie sehen die wichtigsten Anforderungen aus?
Betreiber in der EU müssen mindestens folgende Cyber Security Maßnahmen umsetzen, um die IT und Netzwerke ihrer kritischen Dienstleistungen zu schützen:

- **Policies:** Richtlinien für Risiken und Informationssicherheit
- **Incident Management:** Prävention, Detektion und Bewältigung von Cyber Incidents
- **Business Continuity:** BCM mit Backup Management, DR, Krisen Management
- **Supply Chain:** Sicherheit in der Lieferkette — bis zur sicheren Entwicklung bei Zulieferern
- **Einkauf:** Sicherheit in der Beschaffung von IT und Netzwerk-Systemen
- **Effektivität:** Vorgaben zur Messung von Cyber und Risiko Maßnahmen
- **Training:** und Cyber Security Hygiene
- **Kryptographie:** Vorgaben für Kryptographie und wo möglich Verschlüsselung
- **Personal:** Human Resources Security
- **Zugangskontrolle**
- **Asset Management**
- **Authentication:** Einsatz von Multi Factor Authentisierung und SSO
- **Kommunikation:** Einsatz sicherer Sprach-, Video- und Text-Kommunikation
- **Notfall-Kommunikation:** Einsatz gesicherter Notfall-Kommunikations-Systeme

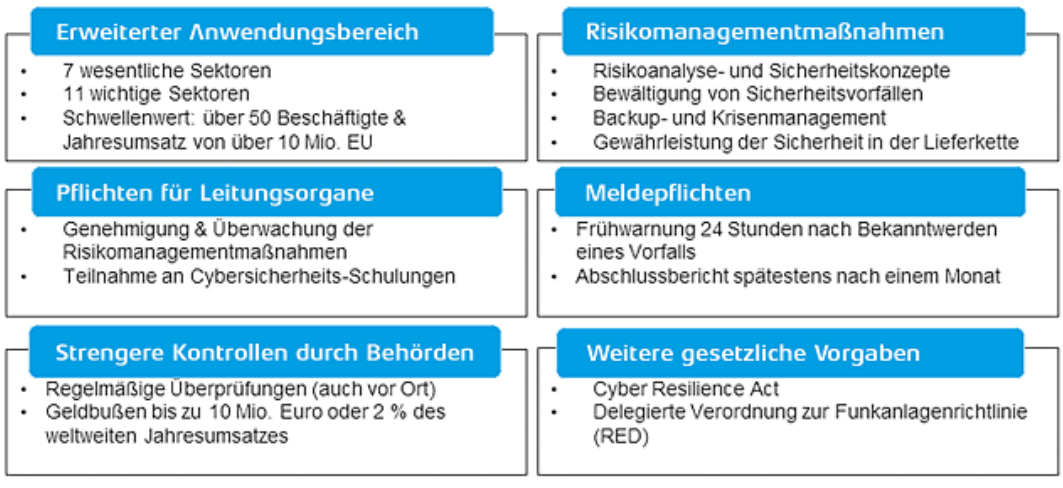
Wann sollten Betroffene aktiv werden?
Die überarbeitete Richtlinie zur Sicherheit von Netz- und Informationssystemen (NIS2) birgt für Unternehmen, Einrichtungen und Organisationen verschiedenster Größe beträchtliche Herausforderungen. Unternehmen sollten bereits **jetzt aktiv werden** und sich vorbereiten, um nicht ins Hintertreffen zu geraten, sondern der Regulatorik einen Schritt im Voraus sein. Unter den aktuellen Rahmenbedingungen bleibt die Bedrohungslage weiterhin hoch.

Handlungsbedarf für Betroffene: Die wesentlichen Neuerungen der Reglungen betreffen das aktive Risikomanagement, die Ausweitung auf weitere Unternehmen und den Handlungsrahmen der Aufsichtsbehörden.

Das heißt im ersten Schritt müssen alle Einrichtungen und Organisationen **fundierte Risikoanalysen** durchführen. Wie hoch ist das Potenzial von Cybervorfällen, wie groß sind die Auswirkungen und welche organisatorischen und technischen Maßnahmen sind zu implementieren, um adäquat auf das Risiko reagieren zu können?

Die Mindestanforderungen an die Cybersicherheitsstrategie, die in der NIS2 Richtlinie festgelegt sind, bieten hierzu mehr als nur eine Orientierungshilfe. Darüber hinaus werden die Unternehmen dazu verpflichtet, erhebliche **Cybersicherheitsvorfälle** zu **melden**. Und zwar so schnell wie möglich. Der Meldung folgt anschließend ein umfangreicher Bericht sowie einen **Abschlussbericht**, wenn der Vorfall behoben und die internen **Maßnahmen** komplett abgeschlossen sind.

Zusammenfassung: 6 Punkte zur Umsetzung der NIS2 Richtlinie



BT Nord Systemhaus GmbH
Siemensstr. 28, 25813 Husum
+49 4841 89680
info@btnord.de
www.btnord.de

Geschäftsführer:
Thomas Holst, CEO,
Dipl.-Ing.(FH) Thies Kracht, CTO
Prokurist:
Frank Thomsen

Amtsgericht Flensburg
HRB 354 HU

Umsatzsteuer-ID:
DE134657285

Bankverbindungen:
Nord-Ostsee Sparkasse
BIC: NOLADE21NOS
IBAN: DE70 2175 0000 0186 0948 19

VR Bank Westküste eG
BIC: GENODEF1HUM
IBAN: DE70 2176 2550 0004 0133 36

1. Betroffenheit prüfen

Unternehmen sollten prüfen, ob sie dem Anwendungsbereich der NIS2 Richtlinie unterfallen, da dieser erheblich erweitert wurde. Erfasst werden alle Unternehmen, die über 50 Personen beschäftigen, einen Jahresumsatz bzw. eine Jahresbilanz von über 10 Mio. EUR haben und einem der kritischen Sektoren unterfallen.

2. Risikomanagement etablieren

Die NIS2 Richtlinie legt in Art. 21 ausdrücklich fest, dass die betroffenen Einrichtungen unter Berücksichtigung des Stands der Technik geeignete und verhältnismäßige technische, organisatorische sowie operative Maßnahmen ergreifen müssen, um Cybersicherheitsrisiken zu beherrschen und Auswirkungen von Sicherheitsvorfällen zu vermeiden.

3. Cybersecurity ist Chefsache

Die zentrale Verantwortung für das Risikomanagement nach der NIS2 Richtlinie tragen die Leitungsorgane. Sie sind insbesondere verpflichtet, die Umsetzung von Cybersicherheitsmaßnahmen zu überwachen, und können im Falle der Nichteinhaltung persönlich zur Verantwortung gezogen werden. Darüber hinaus müssen die Leitungsorgane an Cybersicherheits-Schulungen teilnehmen und sicherstellen, dass allen Mitarbeitern bei Bedarf entsprechende Schulungen angeboten werden.

4. Meldepflichten berücksichtigen

Unternehmen unterliegen künftig strengen Meldepflichten. Einrichtungen, die der NIS2 Richtlinie unterliegen, müssen über jeden Sicherheitsvorfall, der erhebliche Auswirkungen auf die Erbringung ihrer Dienste hat, Bericht erstatten. In besonders schweren Fällen sind zudem unverzüglich die Nutzer zu benachrichtigen und ggfs. sogar die Öffentlichkeit zu informieren. Um den Meldepflichten zu genügen, sollten Unternehmen daher eine effektive Krisenkommunikation etablieren und diese für den Notfall erproben.

5. Behördliche Maßnahmen vermeiden

Zur Durchsetzung der Cybersicherheits-Vorgaben werden den nationalen Behörden künftig zahlreiche Kontroll- und Sanktionsmaßnahmen zur Verfügung stehen. Zu nennen sind u.a. Vor-Ort-Kontrollen, Sicherheitsprüfungen sowie Anweisungen oder Anordnungen. Darüber hinaus werden die nationalen Behörden auch

befugt sein, Warnungen über Verstöße herauszugeben. Neben der bisherigen Befugnis des Bundesamtes für Sicherheit in der Informationstechnik, Produktwarnungen auszusprechen, drohen mit Umsetzung der Richtlinie damit vermehrt öffentliche Warnungen, die Unternehmen erheblich belasten können.

6. Weitere Regelungen beachten

Das Recht wird zum Treiber der Cybersicherheit. Die EU hat auf die fortschreitende Bedrohungslage im Cyberraum reagiert und es wird zukünftig europaweit verbindliche Vorgaben zur Cybersicherheit geben. Neben den unternehmensbezogenen Anforderungen der NIS2 Richtlinie werden mit dem Cyber Resilience Act auch produktbezogene Vorgaben zur Cybersicherheit auf Unternehmen zukommen.

Was leistet BT Nord?

Wir sind zertifizierter IT-Sicherheitsexperte und führen Ihr Unternehmen professionell durch den Prozess. Informations- und Cybersicherheit wird von vielen heute als Kostenfaktor gesehen. Doch funktionierende Prozesse werden in Zukunft auch Ihnen einen erheblichen Wettbewerbsvorteil verschaffen.
Neben dem Thema NIS2 - diesbezüglich suchen wir immer auch einen aktiven Dialog zu den Verbänden und der Politik – wir beraten Unternehmen in allen Punkten rund um ihre IT, vom Aufbau der Infrastruktur bis zum sicheren Betrieb. Und im Ernstfall stehen wir bereit und helfen mit Sofortmaßnahmen sowie nachhaltigem Krisenmanagement. Dabei haben wir auch immer die Optimierung der Digitalisierung von Unternehmen im Blick.

Wir erläutern Ihnen gerne, wie Sie die Herausforderung als Ihre Chance nutzen können. Kontaktieren Sie uns jederzeit gerne für ein persönliches Gespräch.

BT Nord Systemhaus GmbH
Siemensstr. 28, 25813 Husum
+49 4841 89680
info@btnord.de
www.btnord.de

Geschäftsführer:
Thomas Holst, CEO,
Dipl.-Ing.(FH) Thies Kracht, CTO
Prokurist:
Frank Thomsen

Amtsgericht Flensburg
HRB 354 HU

Umsatzsteuer-ID:
DE134657285

Bankverbindungen:
Nord-Ostsee Sparkasse
BIC: NOLADE21NOS
IBAN: DE70 2175 0000 0186 0948 19

VR Bank Westküste eG
BIC: GENODEF1HUM
IBAN: DE70 2176 2550 0004 0133 36