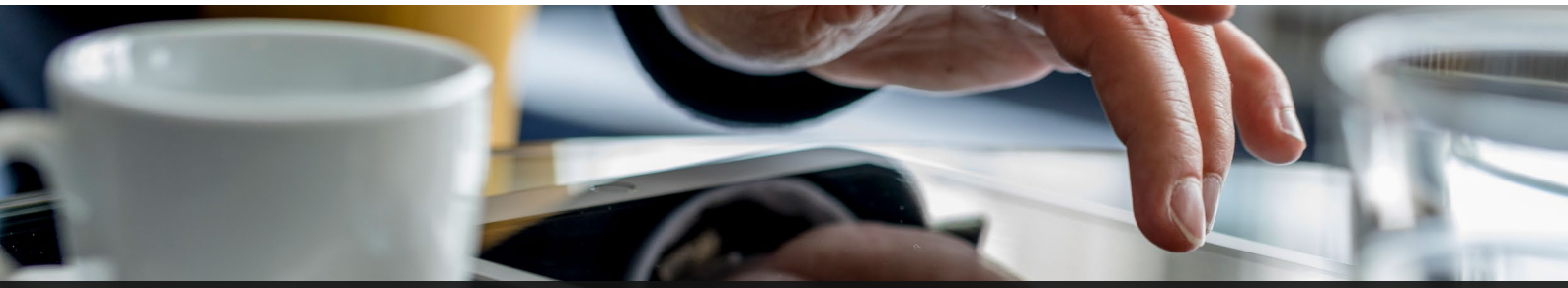

ÜBERSICHT DER ANFORDERUNGEN VON KRITIS, DORA & NIS 2

EINLEITUNG

Die Anforderungen von KRITIS, DORA und NIS 2 betreffen unterschiedliche Bereiche der Cybersicherheit und des Schutzes kritischer Infrastrukturen, die jedoch in vielen Aspekten Überschneidungen aufweisen. Hier ist eine Übersicht über die Anforderungen der jeweiligen Regulierungen.

1. KRITIS (Kritische Infrastrukturen)

KRITIS bezieht sich auf die Infrastruktur von Unternehmen und Institutionen, die für das Gemeinwohl von entscheidender Bedeutung sind und deren Ausfall oder Beeinträchtigung gravierende Auswirkungen auf die Gesellschaft haben würde.

- **Sektoren:** Zu den kritischen Infrastrukturen gehören Sektoren wie Energie, Wasser, Ernährung, Gesundheit, Informationstechnik, Transport und Kommunikation.
- **Schutzanforderungen:** Betreiber kritischer Infrastrukturen müssen geeignete Sicherheitsvorkehrungen treffen, um ihre Systeme vor Cyberangriffen und anderen Bedrohungen zu schützen.
- **Sicherheitsmanagement:** Einrichtung von Sicherheitsmanagementsystemen, regelmäßige Risikobewertungen und Sicherheitsmaßnahmen zum Schutz vor Cyberbedrohungen.
- **Notfall- und Krisenmanagement:** Planungen und Maßnahmen für Notfälle und Krisen müssen vorhanden sein, einschließlich der Möglichkeit, die Betriebsfähigkeit in Krisensituationen aufrechtzuerhalten.
- **Berichtspflichten:** Es gibt Berichtspflichten an die zuständigen Behörden, insbesondere im Falle von Sicherheitsvorfällen.

2. DORA (Digital Operational Resilience Act)

DORA ist eine EU-Verordnung, die darauf abzielt, die digitale operative Resilienz des Finanzsektors zu stärken, insbesondere hinsichtlich der Cybersicherheit.

- **Geltungsbereich**: DORA richtet sich an Finanzmarktteilnehmer wie Banken, Versicherungen, Wertpapierfirmen und auch Drittanbieter von IT-Diensten.
- **Anforderungen an Cybersicherheit:** Finanzunternehmen müssen sicherstellen, dass sie gegen Cyberangriffe gewappnet sind und eine hohe betriebliche Resilienz im digitalen Bereich gewährleisten.
- **Betriebliche Resilienz:** Es müssen Vorkehrungen getroffen werden, um die Funktionsfähigkeit bei IT-Ausfällen und Cyberangriffen sicherzustellen.
- **Risikomanagement:** Implementierung eines Risikomanagementrahmens, der die Risiken im digitalen Betrieb identifiziert, bewertet und steuert.
- **Third-Party-Risiko:** Anbieter von kritischen IT-Diensten müssen einer besonderen Überwachung unterzogen werden, um Risiken zu minimieren.
- **Berichterstattung und Aufsicht:** Bei schwerwiegenden Sicherheitsvorfällen müssen die zuständigen Behörden informiert werden.

3. NIS 2 (Network and Information Systems Directive 2)

Die NIS 2-Richtlinie ist eine EU-Vorgabe, die die Cybersicherheit von Netzwerken und Informationssystemen in kritischen Bereichen verbessern soll.

- **Erweiterter Geltungsbereich:** Die NIS 2-Richtlinie erweitert den Geltungsbereich auf mehr Sektoren und mehr Unternehmen. Sie umfasst nicht nur Betreiber kritischer Infrastrukturen, sondern auch wichtige digitale Dienste wie Cloud-Computing-Dienste, Suchmaschinen und Online-Marktplätze.
- **Risikomanagement:** Unternehmen müssen ein Risikomanagementsystem implementieren, das Sicherheitslücken und Bedrohungen identifiziert und darauf basierend Schutzmaßnahmen ergreift.
- **Cybersicherheitsvorkehrungen:** Betriebe müssen technische und organisatorische Maßnahmen ergreifen, um Netzwerke und Informationssysteme vor Cyberangriffen und Sicherheitsvorfällen zu schützen.
- **Berichtspflichten:** Im Falle von Sicherheitsvorfällen müssen Unternehmen die zuständigen Behörden informieren und gegebenenfalls auch betroffene Kunden oder Partner.
- **Regelungen zu Aufsicht und Sanktionen:** Es gibt Regelungen zur Überwachung der Umsetzung und auch zu Sanktionen bei Nichteinhaltung der Anforderungen.

Gemeinsamkeiten und Unterschiede:

- **Gemeinsamkeiten:** Alle drei Regulierungen betonen die Notwendigkeit eines robusten Risikomanagements, Sicherheitsvorkehrungen für IT-Systeme und die Fähigkeit zur Krisenbewältigung bei Cybervorfällen. Auch die Berichtspflichten bei Vorfällen und Sicherheitslücken sind in allen drei Regulierungen festgelegt.
- **Unterschiede:** Während KRITIS vor allem auf den Schutz kritischer Infrastrukturen fokussiert ist, richtet sich DORA speziell an den Finanzsektor und legt besonderen Wert auf digitale operative Resilienz. NIS 2 hat einen breiteren Anwendungsbereich und umfasst auch digitale Dienste wie Cloud-Anbieter und Online-Marktplätze, die nicht direkt als kritische Infrastruktur gelten, jedoch für die Gesellschaft wichtig sind.

Diese Anforderungen stellen sicher, dass in einer zunehmend vernetzten Welt die Resilienz und Sicherheit der kritischen Infrastruktur und digitaler Dienste gestärkt werden.

CCP Software GmbH
Rudolf-Breitscheid-Straße 1-5
35037 Marburg

+49 6421 1701-0
sales@ccpsoft.de
ccpsoft.de