

Auswirkungen der NIS2 Richtlinie auf Unternehmen der Internetwirtschaft

NIS2 für die Internetwirtschaft

- Betroffenenkreis neu adressiert
- Anforderungen verändert

Ausweitung des Regelungskreises

- In NIS1 „Betreiber wesentlicher Dienste“ (primär: DNS-Diensteanbieter, IXPs und TLS-Name-Registries.) und sog. „Anbieter digitaler Dienste“ (Suchmaschinen, Marktplätze, Cloud Computing) adressiert
- Mit NIS2 nun deutlich mehr Akteure erfasst und neues Regelungsschema (wesentliche und wichtige Einrichtungen erzeugt stärkeren Fokus auf Akteure),

Neue Akteurszuweisungen

NIS1	NIS2
<ul style="list-style-type: none">■ IXPs■ DNS-Diensteanbieter■ TLD Name Registries	<ul style="list-style-type: none">■ Betreiber von Internet-Knoten■ DNS-Diensteanbieter, ausgenommen Betreiber von Root-Namenservern■ TLD-Namenregister■ Anbieter von Cloud-Computing-Diensten■ Anbieter von Rechenzentrumsdiensten■ Betreiber von Inhaltzustellnetzen■ Vertrauensdiensteanbieter■ Anbieter öffentlicher elektronischer Kommunikationsnetze■ Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste■ Verwaltung von IKT-Diensten (Business-to-Business)■ Anbieter verwalteter Dienste■ Anbieter verwalteter Sicherheitsdienste

Digitale Dienste

NIS1	NIS2
<ul style="list-style-type: none">■ Online Marktplätze■ Online Suchmaschinen■ Cloud Computing Dienste	Digitale Dienste in dieser Form nicht mehr aufgegriffen

Wichtige Dienste?

NIS1	NIS2
Wichtige Dienste in dieser Form nicht in NIS1 enthalten	<ul style="list-style-type: none">▪ Anbieter von Plattformen für Dienste sozialer Netzwerke▪ Anbieter von Online-Suchmaschinen▪ Anbieter von Online-Marktplätzen

- Wobei „Wichtige Dienste“ auch teilweise als wesentliche Dienste klassifiziert werden können
- In DE existiert noch die Kategorie der UBI aus dem IT-SiG2.0, die wegfällt

Und die Internetwirtschaft in DE?

- Differenzierung zwischen besonders wichtigen (wesentlichen) und wichtigen Einrichtungen und on Top noch „Kritische Anlagen“

Neue Anforderungen im Zuge von NIS2

- Meldemechanismen wurden vis à vis NIS1 überarbeitet
- Zusätzliche Beschreibung von Sicherheitsmaßnahmen (im Vergleich zu NIS1)
- Spezifische Regelungen für DNS-Betreiber
- Regelungen für Geschäftsführer:innen
- Konkrete Auflagen zur Schaffung eines ISMS

Neuer Meldemechanismus

- Alte Meldepflicht aus NIS1 für wesentliche Einrichtungen und digitale Dienste wird für alle wesentlichen und wichtigen Einrichtungen geschaffen
- Meldepflichten sehen zweistufiges Meldewesen vor

Und Meldungen in Deutschland?

- Die Vorgaben des Meldewesens gem. NIS2 werden im derzeitigen Stand des NIS2UmsuCG adaptiert. Meldungen sollen hier über einen gemeinsamen Meldekopf laufen.
- Große Unbekannte hier: KRITISDachG und Zuständigkeit des BBK

Zusätzliche Sicherheitsmaßnahmen

NIS1	NIS2
<ul style="list-style-type: none"> ■ Vorgaben zu Maßnahmen für Betreiber wesentlicher Dienste ■ Vorgaben zu Maßnahmen zum Schutz von Netz- und Informationssystemen <p>➤ <i>Keine konkreten Vorgaben dazu, diese sollen Mitgliedsstaaten überlassen bleiben.</i></p>	<ul style="list-style-type: none"> ■ Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme; ■ Bewältigung von Sicherheitsvorfällen; ■ Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement; ■ Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern; ■ Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen; ■ Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit; ■ grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit; ■ Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung; ■ Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen; ■ Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Sicherheitsauflagen in Deutschland?

- Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,
- Bewältigung von Sicherheitsvorfällen,
- Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,
- Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
- grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Sicherheit in der Informationstechnik,
- Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle und für das Management von Anlagen,
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Spezifische Regelungen für DNS-Betreiber

- Erfassung aller DNS-Betreiber über nationale Aufsichtsbehörden
- Verpflichtung für Mitgliedsstaaten, Regelungen für DNS-Betreiber zu schaffen, um eine akkurate und aktuelle Datenbank zu betreiben.

Neue Regelungen für Geschäftsführer:innen

- NIS2 schafft die Anforderung der Verantwortlichkeit für Geschäftsführer:innen
- NIS2 sieht einen Sanktionsrahmen für diese vor, sollten Auflagen von Sicherheitsbehörden nicht erfüllt werden.

Neue Regelungen für Geschäftsführer:innen in Deutschland

- Regelungen in DE sehen eine Verunmöglichung des Haftungsausschlusses für Geschäftsleitungen vor
- Regelungen sehen Schulungspflicht vor
- Möglichkeit zur zeitweisen Untersagung der Tätigkeit, bis Defizite behoben

Konkrete Auflagen zur Schaffung eines ISMS

- Der delegierte Rechtsakt zur NIS2 Richtlinie sieht vor, dass wesentliche Einrichtungen ein Informationssicherheitsmanagementsystem (ISMS) unterhalten und betreiben.
 - Die Auflagen hierfür orientieren sich an ISO27001
- Der deutsche Gesetzgeber hat hierzu im Entwurf des NIS2UmsuCG analoge Regelungen getroffen.

**Vielen Dank für Ihre
Aufmerksamkeit!**