DEUTSCHER LANDKREISTAG

Rundschreiben 1042/2022

- Mitglieder des **Arbeitskreises IuK-Technik**
- **Landesverbände**

des Deutschen Landkreistages

Ulrich-von-Hassell-Haus
Lennéstraße 11
10785 Berlin

Tel.: 030 590097-352
Fax: 030 590097-400

E-Mail: Christian.Stuffrein
@Landkreistag.de

AZ: II/Ref. 29

Datum: 28.12.2022

Sekretariat: Stefanie Langer

Richtlinie (EU) über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS 2) verkündet
Bezugsrundschreiben Nr. 982/2022 vom 13.12.2022, Nr. 217/2021 vom 04.03.2021

Zusammenfassung
Die Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS 2) ist im Amtsblatt der EU verkündet worden. NIS 2 soll die Grundlage für Risikomanagementmaßnahmen und Meldepflichten im Bereich Cybersicherheit in allen umfassten Sektoren bilden. Erstmals wird die öffentliche Verwaltung auf zentraler und regionaler Ebene in den Anwendungsbereich aufgenommen.

Im Amtsblatt der EU ist am 27.12.22 die Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS 2), zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 verkündet worden **(Anlage)**. Bis zum 17. Oktober 2024 ist die NIS 2-Richtlinie in nationales Recht umzusetzen. In Deutschland basierte die Umsetzung der ersten NIS-Richtlinie auf dem IT-Sicherheitsgesetz 2.0, dem BSI-Gesetz und der KRITIS-Verordnung. NIS 2 soll die Grundlage für Risikomanagementmaßnahmen und Meldepflichten im Bereich Cybersicherheit in allen Sektoren bilden, die unter die Richtlinie fallen, wie etwa Energie, Verkehr, Gesundheit und digitale Infrastruktur. Mit der überarbeiteten Richtlinie sollen die Anforderungen an die Cybersicherheit und die Umsetzung von Cybersicherheitsmaßnahmen zwischen den verschiedenen Mitgliedstaaten harmonisiert werden.

NIS 2 wird erstmals auch für öffentliche Verwaltungen auf zentraler und regionaler Ebene gelten (vgl. Kapitel I, Artikel 2). Darüberhinausgehend können die Mitgliedstaaten beschließen, dass diese auch für derartige Einrichtungen auf lokaler Ebene gilt und somit für die Kommunen. In Deutschland muss dies über Rechtsakte der Bundesländer erfolgen. Unterschiedliche Anforderungen von Bundesland zu Bundesland sollten aus Sicht der Hauptgeschäftsstelle vermieden werden, um einen Flickenteppich zu verhindern. Mit dem Thema soll sich deshalb auch eine Arbeitsgruppe des IT-Planungsrates beschäftigen, die Hauptgeschäftsstelle ist vertreten. Inwieweit die Bundesländer die Kommunen verpflichten, ist momentan noch nicht abzuschätzen.

Eine wichtige Neuerung ist die erstmalige Unterscheidung zwischen wesentlichen und wichtigen Einrichtungen, wobei ersteren eine höhere Kritikalität zugesprochen wird und für die teilweise unterschiedliche Vorschriften gelten. Zu den wesentlichen Einrichtungen (vgl. Anhang I) zählen u. a. die öffentliche Verwaltung, Energie, Verkehr und Gesundheitswesen, zu den wichtigen Einrichtungen (vgl. Anhang II) u. a. die Abfallbewirtschaftung.

Während nach der alten NIS-Richtlinie die Mitgliedstaaten dafür zuständig waren festzulegen, welche Einrichtungen die Kriterien für die Einstufung als Betreiber wesentlicher Dienste erfüllen, wird mit der neuen NIS 2-Richtlinie ein Schwellenwert für die Größe eingeführt, der als allgemeine Regel für die Ermittlung beaufsichtigter Einrichtungen dient. Das bedeutet, dass alle mittleren und großen Einrichtungen, die in den von der Richtlinie erfassten Sektoren tätig sind oder unter die Richtlinie fallende Dienste erbringen, in den Anwendungsbereich der Richtlinie fallen (mind. 50 Mitarbeiter und Jahresumsatz/-bilanz von mind. 10 Mio. EUR). Zu beachten ist allerdings, dass die NIS 2.0 hiervon eine Gegenausnahme für besonders kritische Dienste vorsieht.

Weiterhin definiert die NIS 2-Richtlinie Anforderungen an die Mitgliedstaaten, welche in Deutschland im Wesentlichen bereits durch das Bundesamt für Sicherheit in der Informationstechnik übernommen werden dürften (vgl. Kapitel II und III), dazu zählen:

- Erarbeitung einer nationalen Cybersicherheitsstrategie,
- Einrichtung einer zuständigen Behörde und zentralen Anlaufstelle,
- Aufbau eines nationalen Rahmens für das Cyberkrisenmanagement, Vorhalten von Ressourcen,
- Aufbau von Computer-Notfallteams,
- koordinierende Offenlegung von Schwachstellen und eine europäische Schwachstellendatenbank.

Kapitel IV greift Risikomanagementmaßnahmen und Berichtspflichten im Bereich der Cybersicherheit auf. Folgende Anforderungen an wesentliche und wichtige Einrichtungen werden u. a. definiert:

- Schulungen für Mitglieder der Leitungsorgane,
- Meldepflichten,
- 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 (vgl. ausführliche Ausführungen unter Nr. 49 der Begründung) 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.

Leitungsorgane der Einrichtungen sollen bei Verstößen gegen Maßnahmen nach Artikel 21 (Risikomanagementmaßnahmen) verantwortlich gemacht werden können. Für die öffentliche Verwaltung besteht eine Ausnahme, hier gelten die vorhandenen nationalen Haftungsregelungen.

Darüber hinaus wurde die neue Richtlinie an die sektorspezifischen Rechtsvorschriften angepasst, insbesondere an die Richtlinie über die Resilienz kritischer Einrichtungen (CER), um Rechtsklarheit zu schaffen und für Kohärenz zwischen NIS 2 und diesen Rechtsakten zu sorgen.

Im Auftrag

Stuffrein

Anlage