Öffentlicher Sektor - Zukunft gestalten Blog
By PwC Deutschland | 30. November 2023

Kritische Infrastrukturen besser schützen

Das neue NIS-2-Gesetz wird den öffentlichen Sektor besonders stark betreffen.

Hacker:innen dringen in die IT-Systeme eines Energieversorgers ein und legen die Stromversorgung einer deutschen Großstadt lahm – ein Horrorszenario, aber nicht gänzlich unrealistisch. Auch die nach wie vor ungeklärten Fälle durchtrennter Kommunikationskabel bei der Deutschen Bahn im Jahr 2022, die den Zugverkehr massiv behinderten, zeigen: Unsere täglich genutzte Infrastruktur ist sehr verletzlich. Und die Gefahren nehmen zu; nicht nur, aber insbesondere im virtuellen Raum.

Adressatenkreis wächst ständig

Deshalb wollen die Europäische Union und die Bundesregierung kritische Infrastrukturen (KRITIS) besser schützen. Dazu zählen Infrastrukturen der Daseinsvorsorge und Verwaltung, aber auch von Wirtschaftssektoren wie der Chemieindustrie und des Finanz- und Versicherungswesens. Das erste deutsche IT-Sicherheitsgesetz trat 2015 in Kraft. 2016 folgte eine europäische Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit, die sogenannte NIS-Richtlinie.

Angesichts zunehmender geopolitischer Spannungen folgte die zweite Generation der europäischen KRITIS-Regulierung: Ende 2022 trat die NIS-2- Richtlinie in Kraft, die die EU-Mitgliedsstaaten bis 2024 in nationales Recht umsetzen müssen. In Deutschland soll dies mit dem NIS-2-Umsetzungsund Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) geschehen, für das bereits ein Referentenentwurf vorliegt. Klar erkennbar ist: Jede neue Regulierung erweitert den Adressatenkreis und die vorgeschriebenen Sicherheitsmaßnahmen.

Betroffenheit prüfen

Diese Entwicklungen betreffen den öffentlichen Sektor besonders, denn er betreibt einen wesentlichen Teil der kritischen Infrastrukturen. So fallen praktisch alle gängigen Tätigkeitsbereiche eines kommunalen Versorgers unter die KRITIS-Regulierung. Verwaltungen und kommunale Unternehmen sollten deshalb unbedingt prüfen, inwieweit die neue Gesetzgebung sie betrifft. Und sie sollten generell die Sicherheit ihrer kritischen Infrastrukturen analysieren.

Der Referentenentwurf des NIS2UmsuCG unterscheidet zwischen „besonders wichtigen Einrichtungen" (auch „wesentliche Einrichtungen" genannt) und „wichtigen Einrichtungen: „Besonders wichtig" sind Organisationen, die „kritische Anlagen" betreiben. „Wichtig" sind solche, die keine „kritischen Anlagen" betreiben.

Zur ersten Gruppe gehören beispielsweise große Unternehmen oder sonstige Organisationen aus den Sektoren Energie, Verkehr und Gesundheit, aber auch mittelgroße Organisationen, die Telekommunikationsinfrastruktur betreiben. Zu den „wichtigen Einrichtungen" zählen mittelgroße Organisationen der Daseinsvorsorge und beispielsweise große und mittlere Unternehmen aus den Sektoren Chemie und Logistik.

Unangekündigte Prüfungen

Einrichtungen, die unter die NIS-2-Regelungen fallen, müssen geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen ergreifen, um Störungen der IT-Sicherheit zu vermeiden. Sie

müssen beispielsweise ein Back-up-Management betreiben, bestimmte Verschlüsselungsstandards erreichen und Konzepte für die Zugriffskontrolle auf ihre Systeme entwickeln. Erwerben oder entwickeln sie neue Systeme, müssen sie vorgeschriebene Sicherheitsmaßnahmen einhalten.

Außerdem müssen sie sich beim Bundesamt für Sicherheit in der Informationstechnik (BSI) registrieren, Zertifizierungen nachweisen und sich Audits unterziehen – besonders wichtige Einrichtungen darf das BSI auch unangekündigt überprüfen. Außerdem müssen sie Sicherheitsvorfälle nach einem Stufenmodell an das BSI und das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe melden. Dann müssen sie gegebenenfalls auch die Öffentlichkeit informieren.

Die Geschäftsleitung haftet

Verstoßen Organisationen fahrlässig oder vorsätzlich gegen die Vorschriften, drohen ihnen Bußgelder. Möglich sind bei besonders wichtigen Einrichtungen bis zu zehn Millionen Euro bzw. zwei Prozent des Vorjahresumsatzes. Im Zweifel haftet dafür auch die Geschäftsleitung: Sie ist dafür verantwortlich, dass ihre Einrichtung die Sicherheitsmaßnahmen einhält. Die NIS-2-Regulierung verbietet ausdrücklich, dass eine Organisation auf Ersatzansprüche gegen die Geschäftsleitung verzichtet.

Welche Einrichtungen wie stark von der NIS-2- Regulierung betroffen sind, ist nicht immer leicht festzustellen. Mit einem von PwC entwickelten Onlinetool können Organisationen vorab prüfen, inwieweit sie unter die Vorschriften fallen. Es liefert eine erste Einschätzung, ob die Organisation als „wesentlich“ bzw. „wichtig“ gilt oder ob das NIS-2 sie nicht betrifft.

Ansprechpartner:
André Glenzer

Zu weiteren PwC Blogs

Schlagwörter

Compliance, Digitalisierung, IT-Sicherheit, IT-Systeme, Informationstechnologie (IT)

Kontakt

Prof. Dr. Rainer Bernnat
Frankfurt am Main
rainer.bernnat@pwc.com