NIS2-Richtlinie

Pflichtaufgabe für Stadtwerke

[31.07.2025] Die nationale Umsetzung der NIS2-Richtlinie kommt – und betrifft auch kleinere Stadtwerke. Sie müssen rechtzeitig prüfen, ob sie betroffen sind. Ansonsten drohen Zeitdruck, hohe Kosten und sogar Bußgelder.

Aufgeschoben ist nicht aufgehoben: Die eigentlich schon für Oktober 2024 vorgeschriebene Überführung der europäischen NIS2-Richtlinie in nationales Recht wird die neue Bundesregierung jetzt zeitnah umsetzen. Dieses umfangreiche Regelwerk verpflichtet auch kleinere und mittlere Stadtwerke, die keine kritischen Anlagen selbst betreiben, den aktuellen Stand der Cybersicherheit umzusetzen. Erste Hürde: Die Unternehmen müssen ohne Aufforderung prüfen, ob sie betroffen sind. „Allein der deutschen Wirtschaft entsteht durch Cyberattacken jährlich ein Schaden von gut 179 Milliarden Euro“, so Ralf Wintergerst, Präsident des Branchenverbands Bitkom.

Genau hier setzt das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) an. Es gilt für Unternehmen definierter Sektoren mit mindestens 50 Beschäftigten und einem Jahresumsatz von zehn Millionen Euro. In besonders wichtigen Sektoren wie der Energieversorgung sind aber auch kleinere Unternehmen verpflichtet, ihre Betroffenheit selbst zu prüfen und sich zu registrieren. Es gibt dazu keine Aufforderung von Behörden – die Pflicht zur Betroffenheitsanalyse liegt aktuell allein bei den Unternehmen. Für den Bitkom-Präsidenten ist hierfür spezielles Know-how notwendig: „Insbesondere kleine und mittelständische Unternehmen brauchen Unterstützung, um festzustellen, ob und wie sie von dem Gesetz betroffen sind und welche Maßnahmen sie ergreifen müssen.“

Zeitig Unterstützung suchen

Sobald das Gesetz beschlossen wird, herrscht Zeitdruck, wie Ingbert Liebing, Hauptgeschäftsführer des Verbands kommunaler Unternehmen (VKU) hervorhebt: „Die strengen Regeln gelten dann für die Anlagensteuerung bis hin zur Office-IT. Umsetzungskosten spielen offenbar keine Rolle, Umsetzungsfristen sind nicht vorgesehen.“ Dabei gilt wie bei anderen großen Veränderungen immer die Faustregel: Je später Unternehmen mit der Umsetzung beginnen, desto teurer wird es, weil es nur eine begrenzte Zahl an wirklich erfahrenen IT-Sicherheitsexperten gibt – und die sind sehr schnell ausgebucht. Das Spektrum reicht von Selbstständigen bis hin zu den großen Beratungsunternehmen, von generischen Online-Fragebögen bis hin zu kompletten Beratungsteams. „Gerade bei der Umsetzung von NIS2 ist es wichtig, mit IT-Dienstleistern zusammenzuarbeiten, die Branchenerfahrungen haben und die Regulatorik in der Energiebranche genau kennen“, empfiehlt Thomas Mayerbacher, Geschäftsführer des Unternehmens prego services, das als IT- und Serviceprovider für Energieversorgungsunternehmen selbst der NIS2-Richtlinie unterliegt.

Prioritäten setzen

Für die Umsetzung der NIS2-Richtlinie empfiehlt Mayerbacher, konsequent zu priorisieren: Unternehmen im Energiesektor müssen als erstes eine Betroffenheitsanalyse mit einem Nachweis erstellen. Das gilt auch für Unternehmen, die bereits ein zertifiziertes IT-Informationssicherheits-Managementsystem (ISMS) eingeführt haben. „Für prego services ist die Betroffenheitsanalyse ein erster Baustein, mit dem wir EVUs

unterstützen“, so Thomas Mayerbacher. An zweiter Stelle steht eine umfassende Schwachstellenanalyse der IT-Infrastruktur – die Fit-Gap-Analyse. Diese kann große Sicherheitslücken aufdecken und Hinweise geben, was als erstes umgesetzt werden muss.

So muss eine Personal- und Zugangskontrolle vorhanden sein, das Passwortmanagement auf Multifaktor-Authentifizierung umgestellt, ein Vorfallmanagement eingeführt und Vorbereitungen zu Back-up und Krisenfallmanagement getroffen werden. Auch Geschäftsführer müssen neue Aufgaben übernehmen, denn sie sind persönlich verantwortlich für Vorsorgemaßnahmen wie kontinuierliche Mitarbeiterschulungen und die regelmäßige Überprüfung der Maßnahmen, damit sie immer dem aktuellen Stand der Technik entsprechen. Im vorliegenden Entwurf zur NIS2-Umsetzung wird dazu erstmals auch eine Haftung der Geschäftsführung mit Bußgeldern bei Verstößen oder Nichteinhalten der Meldepflichten vorgesehen.

Weniger komplexe Zertifizierung

Im Anschluss müssen Unternehmen prüfen, ob sie verpflichtet sind, ein Informationssicherheits-Managementsystem einzuführen. Für kleinere Stadtwerke interessant: Neben der komplexen Zertifizierung nach ISO 27001 können sie sich auch für die weniger komplexe Zertifizierung nach VdS 10000 entscheiden. Für betroffene Unternehmen gelten dann Nachweis- und Meldepflichten. Die Erstmeldung von erheblichen Cybersicherheitsvorfällen muss innerhalb von 24 Stunden nach Bekanntwerden erfolgen.

Neben diesen technischen Vorkehrungen umfasst NIS2 auch eine Reihe von prozessualen Themen, um die Resilienz der Unternehmen zu steigern. Die Analyse der IT-Strukturen und Prozesse bietet gerade kleineren und mittleren Stadtwerken auch Chancen über eine gehärtete IT-Sicherheit hinaus: Sie kann dazu beitragen, die digitale Transformation aller Prozesse zu beschleunigen und damit die Wettbewerbsfähigkeit nachhaltig zu stärken.

()

Der Beitrag ist im Schwerpunkt Cybersicherheit der Ausgabe Juli/August 2025 von stadt+werk erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: Politik, prego services, Bitkom, Cybersicherheit, NIS2-Richtlinie, Verband kommunaler Unternehmen (VKU)