SCHULUNGEN

NIS-2-Pflichtschulung für Verantwortliche
→ www.dvgw-veranstaltungen.de/9901

E-Learning „Informationssicherheit kompakt" – Mitarbeitende
→ www.dvgw-veranstaltungen.de/9004

E-Learning „Informationssicherheit kompakt" – Verantwortliche
→ www.dvgw-veranstaltungen.de/9005

Quelle: Garun Studios/stock.adobe.com

Informationssicherheit:

Schulungsanforderungen für Leitung und Beschäftigte

Mit der Umsetzung der europäischen NIS-2-Richtlinie in Deutschland steigen die Anforderungen an die Informationssicherheit insbesondere für kleine Unternehmen der Energie- und Wasserwirtschaft deutlich an. Der Beitrag beschreibt vor diesem Hintergrund, was dies für die Verantwortlichkeiten der Geschäftsleitung bedeutet und welche Schulungsangebote es bereits gibt.

von: Thomas Bender & Theresia von Zedtwitz (beide: DVGW Berufliche Bildung)

Das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG), mit dem die europäische NIS-2-Richtlinie in nationales Recht überführt wird, führt zu wesentlichen Änderungen des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG). Insbesondere werden die Verantwortlichkeiten der Geschäftsleitung verschärft (§ 38 BSIG). Zudem wird eine Schulungspflicht für die Geschäftsleitung eingeführt. Diese ist verpflichtet, Cyberrisiken zu verstehen, geeignete Cybersicherheitsmaßnahmen zu ermöglichen, deren wirksame Umsetzung zu überwachen und regelmäßig an entsprechenden Schulungen teilzunehmen. Sie trägt die Gesamtverantwortung für das Cybersicherheits-Risikomanagement und kann bei Verstößen persönlich haftbar gemacht werden.

Führung in der Pflicht: Governance, Aufsicht und Risikoverständnis

Vor diesem Hintergrund bietet die DVGW Berufliche Bildung eine speziell auf die Branche zugeschnittene Pflichtschulung für verantwortliche Leitungskräfte an. Vermittelt werden die regulatorischen Anforderungen aus dem BSIG, Organisations und Aufsichtspflichten sowie die Einordnung technischer und organisatorischer Sicherheitsmaßnahmen. Ziel ist es, die Rolle der Führung im Informationssicherheitsmanagement klar zu definieren und strategisch im Unternehmen zu verankern. Die Pflichtschulung basiert auf dem BISG, umfasst mindestens vier Stunden und muss spätestens alle drei Jahre nachgewiesen werden.

Risikominimierung im Alltag: Schulung der Beschäftigten

Informationssicherheit ist jedoch nicht allein Aufgabe der Unternehmensleitung. Auch technische Führungskräfte und Mitarbeitende müssen Risiken erkennen, sicherheitsrelevante Vorgaben verstehen und im Arbeitsalltag konsequent umsetzen. Hierzu stehen kompakte E-Learnings bereit, die Grundlagen zu aktuellen Bedrohungsszenarien, sicheren Prozessen, Phishing- und SocialEngineeringRisiken sowie zu internen Rollen und Zuständigkeiten vermitteln.

Compliance ohne Pflicht: Warum auch kleine Unternehmen profitieren

Gerade kleinere Unternehmen, die formal nicht unter den unmittelbaren Anwendungsbereich des BSIG fallen, können von diesen Schulungsangeboten profitieren. Denn unabhängig von regulatorischen Pflichten bestehen auch dort relevante Cyberrisiken sowie steigende Anforderungen von

INTERVIEW

„Cybersicherheit ist kein IT-Projekt – sie ist Managementpflicht“

Rainer Stecken ist Berater für Informationssicherheit bei der DVGW Service & Consult GmbH und unterstützt Unternehmen bei der Einführung entsprechender Managementsysteme. Er fungiert zudem als Informationssicherheitsbeauftragter (ISB) des DVGW sowie eines Stadtwerks.

Herr Stecken, NIS-2 macht die Cybersicherheit zur Chefsache. Wie ist die EU-Richtlinie in deutsches Recht überführt worden und wer fällt unter die Regelungen?

Rainer Stecken: Die NIS-2-Richtlinie der EU gilt nicht unmittelbar und ist in Deutschland im Wesentlichen über das neue BSI-Gesetz (BSIG neu) in deutsches Recht überführt worden. Es ist seit dem 6. Dezember 2025 in Kraft. Die Kriterien, nach denen Unternehmen den gesetzlichen Regelungen unterliegen, orientieren sich nicht mehr an der Versorgungsleistung für mehr als 500.000 Einwohner, sondern folgen den Größeneinteilungen der EU für Unternehmen. Damit sind Unternehmen mit mehr als 250 Mitarbeitenden und mehr als 50 Mio. Euro Umsatz und 43 Mio. Euro Bilanzsumme „besonders wichtige“ Einrichtungen; Unternehmen mit mehr als 50 Mitarbeitenden und jeweils mehr als 10 Mio. Euro Umsatz- und Bilanzsumme „wichtige“ Einrichtungen. Die gesamten Unternehmen fallen unter die Bestimmungen, nicht nur die unmittelbar am Versorgungsprozess beteiligten Mitarbeitenden. Kritis-Unternehmen sind automatisch „besonders wichtige Einrichtungen“. Die Zahl regulierter Organisationen erhöht sich damit von rund 4.500 auf etwa 29.500.

Quelle: privat

Was sind denn die wesentlichen Pflichten aus dem neuen BSIG?

Stecken: Zunächst einmal besteht Registrierungspflicht für alle „besonders wichtigen“ und „wichtigen“ Einrichtungen auf dem Portal des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Erhebliche Sicherheitsvorfälle müssen seit Inkrafttreten des Gesetzes innerhalb von 24 Stunden gemeldet werden. Die Geschäftsführung unterliegt der Verpflichtung, regelmäßig an Schulungen zum Risikomanagement teilzunehmen, und § 30 des Gesetzes listet auf, was mindestens an Risikomanagementmaßnahmen umzusetzen ist. Alle Anforderungen beziehen sich auf die gesamte Organisation. Es sind also grundsätzlich alle Prozesse und Mitarbeitenden einzubeziehen.

Wo stehen Unternehmen der Energie- und Wasserwirtschaft bei der Umsetzung – und wo besteht der größte Handlungsbedarf?

Stecken: Viele Unternehmen haben bereits solide Grundlagen in der Informationssicherheit etabliert. Was sich mit dem neuen BSIG deutlich verändert, ist der Druck auf die Leitungsebene: Das Gesetz verlangt eine klare strategische Einbindung des Top-Managements, regelmäßige Schulungen und eine aktive Steuerung des Risikomanagements. Genau hier sehe ich den größten Nachholbedarf – bei der Frage, wie Führung ihren Aufsichts und Organisationspflichten nachkommen kann und sie nachweisbar erfüllt. Ein Informationssicherheits-Managementsystem (ISMS) ist ein geeignetes Werkzeug dafür. Damit wird auch berücksichtigt, dass Beschäftigte ein entscheidender Faktor für die Sicherheitskultur sind. Der zugrunde gelegte Standard (ISO 27001, B3S WA) muss der Organisation angemessen sein.

Wie wird sich Ihrer Einschätzung nach das Thema Informationssicherheit in den kommenden Jahren entwickeln?

Stecken: Informationssicherheit wird sich zu einer dauerhaften Managementaufgabe entwickeln, vergleichbar mit Arbeitsschutz oder Compliance. Informationssicherheit ist dabei aber nur ein Baustein einer übergreifenden Resilienzstrategie. Am Ende geht es darum, unabhängig von jeder Ausfallursache die Versorgungsleistung durchgehend erbringen zu können. Im Kern ist das das Management der Betriebskontinuität. Dazu werden qualifizierte Mitarbeitende benötigt. Und auch die Frage nach der erforderlichen Organisationsgröße wird gestellt werden müssen, weil Unternehmen unterhalb der aktuellen Schwellwerte die erforderlich Breite in der Kompetenz der Mitarbeitenden kaum sicherstellen können.

Geschäftspartnern, Versicherern und Auftraggebern. Eine strukturierte Sensibilisierung der Belegschaft hilft, Sicherheitsstandards frühzeitig zu etablieren und die organisatorische Resilienz zu stärken.

Informationssicherheit als strategische Daueraufgabe

Die abgestufte Qualifizierung von Leitungsebene und operativer Praxis leistet damit einen wirksamen Beitrag dazu, Informationssicherheit als dauerhafte Organisationsaufgabe zu verankern – sowohl im regulierten Umfeld als auch darüber hinaus. ■

Kontakt:
Thomas Bender
DVGW Berufliche Bildung
Josef-Wirmer-Str. 1-3, 53123 Bonn
Tel.: 0228 9188-606
E-Mail: thomas.bender@dvgw.de
Internet: www.dvgw-veranstaltungen.de