Gesetzentwurf des Bundes

Neue Cybersecurity-Regeln betreffen auch die Food-Branche

Von Gerrit-Milena Falker Mittwoch, 31. Juli 2024

Die Bundesregierung will das IT-Sicherheitsrecht reformieren. Dadurch unterfallen künftig viele Lebensmittelbetriebe erstmals strengen Regeln – womöglich ohne davon zu wissen.

Das Bundeskabinett hat vergangene Woche einen lang und heftig diskutierten Gesetzentwurf von Bundesinnenministerin Nancy Faeser (SPD) zur Modernisierung des IT-Sicherheitsrechts beschlossen. Konkret geht es um die nationale Umsetzung der "NIS-2-Richtlinie" – das sogenannte "NIS-2-Umsetzungsgesetz", mit dem Berlin das "Gesetz über das Bundesamt für Sicherheit in der Informationstechnik" (BSIG) reformieren will. Die EU-Richtlinie weitet die Regeln zu Cybersicherheit auf weitere Branchen aus und erhöht die Sicherheitsanforderungen.

10

Mio. Euro Jahresumsatz genügen, um den Regeln für ITSicherheit zu unterfallen

Künftig müssen alle Unternehmen, die zur sogenannten "Kritischen Infrastruktur" zählen, ihre Maßnahmen zur IT-Sicherheit überprüfen und gegebenenfalls anpassen. "Die Bestimmung, ob ein Unternehmen in den Anwendungsbereich der neuen Regeln fällt, ist komplex. In dem Kontext

erhalten wir zahlreiche Anfragen", sagt Patrick Grosmann von der Kanzlei FPS. "Viele Unternehmen – auch Lebensmittelhändler und -hersteller – sind wegen niedrigen Schwellenwerten erstmals erfasst, ohne das bislang auch nur zu ahnen", warnt der Frankfurter Jurist. So sind künftig alle Lebensmittelunternehmen mit mindestens 50 Beschäftigten oder einem Jahresumsatz beziehungsweise -bilanzsumme über 10 Mio. Euro erfasst.

"'Lebensmittelunternehmen' sind dabei aber nur solche Betriebe, die im Großhandel und in der industriellen Produktion und Verarbeitung tätig sind. Es gibt also beim Vertrieb eine Einschränkung auf den Großhandel. Einzelhändler sind – vereinfacht gesagt – nur erfasst, wenn sie auch selbst produzieren.

Berlin muss das Umsetzungsgesetz bis Mitte Oktober verabschieden und verkünden. "Was bis dahin sicher noch für Debatten sorgen wird: Sobald das geänderte BSIG in Kraft tritt, sollen die neuen Pflichten sofort greifen", unterstreicht Grosmann den akuten Handlungsbedarf.

Dass es bislang keine Übergangsfrist gibt, sei vor allem mit Blick auf die Haftung fatal. "Wenn es zu einem Cybersicherheitsvorfall kommt und die Geschäftsleitung eine Pflicht aus der NIS-2-Richtlinie schuldhaft verletzt hat – beispielsweise Risikomanagementmaßnahmen vernachlässigt, Meldungen an das Bundesamt für Sicherheit in der Informationstechnik unterlassen oder nicht geschult hat –, droht sie, direkt persönlich zu haften", so Rechtsanwalt Grosmann weiter.