NIS2-Umsetzung à la Deutschland: Ein Lehrstück in verpassten Chancen

Zwischen regulatorischer Eile, behördlicher Bequemlichkeit und einer Unternehmenslandschaft im Dornröschenschlaf, so mutet die Umsetzung der NIS2-Richtlinie aus Sicht von Dr. Frank Schemmel an. In unserem Aufmacher beschreibt er den aktuellen Stand zu NIS2 in Deutschland.

© IMAGO / Dreamstime

Wurde auch Zeit: Licht am Ende des Tunnels der NIS2-Umsetzung.

„In einer idealen Welt haben wir NIS2 im Herbst im Parlament und vor Ende des Jahres im Amtsblatt", so Dr. Daniel Meltzian, Leiter des BMI-Grundsatzreferats für Cybersicherheit, jüngst im Tagesspiegel. Leider leben wir nicht in einer idealen Welt – sondern in Deutschland. Die Umsetzung der NIS2-Richtlinie nimmt hierzulande zwar wieder Fahrt auf – allerdings mit dem Charme eines Berliner Flughafens in Bauphase vier. Innenminister Dobrindt plant das Gesetz noch 2025 durch den Bundestag zu bringen. Ein finaler Referentenentwurf wurde bis Mitte Juni zwischen BMI und Digitalministerium abgestimmt – mit anschließender Verbändeanhörung. Ziel ist, einen politisch tragbaren Kabinettsentwurf noch vor der Sommerpause in den Bundestag einzubringen. Ambitioniert? Durchaus. Realistisch? Fraglich.

Die EU-Kommission hat bereits genug bzw. eher zu wenig gesehen. Gemeinsam mit 18 anderen Staaten steht Deutschland im zweiten Stadium eines entsprechenden Vertragsverletzungsverfahrens. Es droht ein ähnliches Trauerspiel wie seinerzeit bei der Umsetzung der Whistleblower-Richtlinie.

Der Anfang Juni veröffentlichte Referentenentwurf? Licht und Schatten. Viele aus der Praxis wichtige Punkte, die bereits bei der Abstimmung der Vorgängerregierung heftig diskutiert wurden, werden mithin in einem Anflug von Zeitmanagement großzügig ausgespart. „Es wird aber wichtig sein, dass die kommenden Abstimmungen so kurz wie möglich gehalten werden, um die zügige Umsetzung sicherzustellen", so eine offizielle Stimme aus dem BMI im Tagesspiegel zu möglichen Abstrichen. Es geht dabei zunächst um die abgespeckte Regulierung der Verwaltung. Dies verwundert, sind doch gerade Behörden und Verwaltungen oft am wenigsten vorbereit in Sachen Cybersecurity. Offenbar vertraut man auf eine wundersame Selbstheilung der IT-Landschaft von Behörden.

Bedauerlich aus Praxissicht ist auch, dass der bisher vorliegende Entwurf weder ausreichende Ergänzung bislang fehlender Definitionen noch dringend benötigte Klarstellung bei der Berechnung der Schwellenwerte enthält. So könnte man durch eine einfache Ergänzung im Umsetzungsgesetz tausende Shared-Service Center von Unternehmensgruppen entlasten. Denn die Erbringung von Rechenzentrums- und Clouddienstleistungen für andere Konzernunternehmen würde derzeit aufgrund einer Regelungslücke in ErwG 35 der Richtlinie wohl NIS2 unterfallen.

Und das BSI? Möchte laut eigener Aussage „mehr Helfer als Verhinderer" sein. Nett. Konkret äußert sich das darin, dass man nur dort Orientierungshilfen zu NIS2 bereitstellen möchte, wo noch keine anderweitigen existieren – was in der Praxis bedeutet: eher selten bis gar nicht. Die Begründung? „Stand der Technik" sei ein juristischer Begriff, also zu heikel für technische Hinweise. Aha.

Andere Länder – wie etwa Italien – liefern währenddessen brauchbare Leitlinien und Praxisbeispiele für Unternehmen. Deutschland hingegen hält es lieber mit der Devise: Keine Hilfe ist auch eine Hilfe. Immerhin: In einem Webinar der Allianz für Cybersicherheit hat das BSI eingeräumt, dass Aufklärung wichtiger sei als Bußgelder. Letzteres scheint auch dringend geboten, zeigt doch eine aktuelle repräsentative Cybersecurity-Studie des TÜV in Kooperation mit dem BSI, dass nur etwa die Hälfte der befragten Unternehmen überhaupt schon etwas von NIS2 gehört hat.

Was also tun in dieser regulatorischen Sedisvakanz? Auch hier gab es im vorgenannten Webinar die beste und gleichzeitig pragmatischste Empfehlung: „Macht mal die offensichtlichen Dinge und kümmert euch um die Details später." Sprich: NIS2-Betroffenheit prüfen, Gap-Analyse durchführen, Risiken neu bewerten, priorisieren und dann die größten Risiken erstmal adressieren. Hat man bereits ein nach ISO 27001, TISAX® oder anderweitig zertifiziertes ISMS, ist das Delta zu NIS2 nicht mehr allzu groß.

Klar ist zumindest: NIS2 wird künftig zum generellen Sorgfalts- und Haftungsmaßstab im Bereich Cybersicherheit – und damit zwingender Bestandteil jedes guten CMS. Das Umsetzungsgesetz wird wie sein gescheiterter Vorgänger wohl keine Übergangsfristen enthalten – also sollten Organisationen, die das Thema bisher eher stiefmütterlich betrachtet haben, spätestens die nächsten sechs Monate nutzen, um hier aufzuholen. Dann gibt es hoffentlich mehr Licht als Schatten für die Cybersicherheit in Deutschland.

© privat

Dr. Frank Schemmel, Compliance Officer (Univ.), ist Senior Director Privacy, Compliance & Public Affairs bei DataGuard in München. Schwerpunkt seiner Arbeit sind Datenschutz- und Datenwirtschaftsrecht, Informationssicherheit, Whistleblowing und die rechtlichen Herausforderungen der Digitalisierung.