

KURZKOMMENTIERUNG

zum „Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)“ (Bearbeitungsstand 24.06.2024)

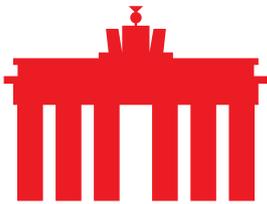
Berlin, 3. Juli 2024

Am 26. Juni hat das Bundesministerium des Innern und für Heimat infolge der Verbändebeteiligung und einer öffentlichen Anhörung einen überarbeiteten Entwurf für das NIS2UmsuCG vorgestellt und den Verbänden zur Kommentierung überlassen.

eco – Verband der Internetwirtschaft verweist auf seine [Stellungnahme vom 28. Mai 2024](#), aus der verschiedene dort angesprochene Aspekte, insbesondere das Regulierungsgefüge (§§ 30ff.) betreffend, weiterhin einer genaueren Betrachtung und Würdigung bedürfen.

Ergänzend zu dieser Stellungnahme hält eco folgende Aspekte fest:

- In der Definition für DNS-Diensteanbieter in § 2 Ziffer 8 ist der Begriff „anbieten“ problematisch. Dies würde dazu führen, dass auch Akteure von der Regelung erfasst werden, die DNS-Dienste lediglich von Betreibern entsprechender Dienste zukaufen. eco plädiert dafür, hier auf den Begriff „betreiben“ abzustellen.
- Der Begriff der Domain-Name-Registry-Dienstleister in § 2 Ziffer 9 kann zu Missverständnissen der Rollen der Anbieter führen, da insbesondere bei generischen Domain Namen der Registrar nicht Dienstleister der Registry ist. Klarer wäre "Domain-Name-Registrierungs-Dienstleister".
- § 38 wurde dahingehend geändert, dass Geschäftsführungen nun Sicherheitsmaßnahmen „umsetzen“ sollen. Dies steht aus Sicht der Internetwirtschaft im Widerspruch zum Wortlaut und Gedanken der NIS2-Richtlinie. eco plädiert dafür, hier zum ursprünglichen Wortlaut des vorigen Referentenentwurfs zurückzukehren und Geschäftsführer:innen die „Billigung von Risikomanagementmaßnahmen“ aufzuerlegen. Gegebenenfalls wäre eine Klarstellung dahingehend sinnvoll, Geschäftsführungen dazu zu verpflichten, ihre entsprechenden Mitarbeiter in die Lage zu versetzen, die Umsetzung von Risikomanagementmaßnahmen zu gewährleisten.



- Die Haftungsregeln in § 38 (2) für Geschäftsführungen lassen im Unklaren, in welchem Umfang Geschäftsführer:innen am Ende tatsächlich für schuldhaft verursachten Schaden in Anspruch genommen werden können oder genommen werden müssen. Vor dem Hintergrund, dass dieser Passus möglicherweise auch bestehende Arbeitsverträge betrifft, wäre hier mehr Klarheit erforderlich.
- In § 51 (4) wäre eine Klarstellung hilfreich, dass für juristische Personen Namen und Mailadressen veröffentlicht werden müssen. Eine Rechtsgrundlage für die Veröffentlichung würde den Anbietern die aufwändige und oft nur manuelle Prüfung ersparen, ob Firmen und Mailadressen Personenbezug haben.
- Die explizite Streichung der Verbändeanhörungen, insbesondere in § 58 erzeugen ebenso wie die nachlaufenden Detaillierungen der Zertifikate-Festlegungen und Anerkennungen per Rechtsverordnung geschäftliche Unsicherheit, die nicht dem Gedanken der Erhöhung der Cybersicherheit der betroffenen Industrie und ihrer Lieferanten entspricht. Daher sollte die Streichung von ‚nach Anhörung der betroffenen Wirtschaftsverbände‘ zurückgenommen werden.
- eco möchte noch einmal auf den Umstand hinweisen, dass die in § 62 festgelegte Zuständigkeit des Bundesamtes für die Einhaltung der Vorschriften aus Teil 3 (§§ 28-50) für wichtige Einrichtungen und besonders wichtige Einrichtungen sowie für kritische Anlagen in Deutschland nicht hilfreich ist. Mit § 63 wird diese Zuständigkeit bei IT-Dienstleistungen auf Unternehmensteile oder Beteiligungen in EU-Mitgliedsstaaten erweitert, wenn der Hauptsitz des Unternehmens/Konzerns in Deutschland liegt. Das hätte in der jetzigen Formulierung die Konsequenz, dass es auch kritische Anlagen im europäischen Ausland geben kann, wenn der Hauptsitz des Betreibers in Deutschland liegt. Dies führt zum Export der erhöhten deutschen KRITIS-Anforderungen in das europäische Ausland. Dies könnte sich als problematisch erweisen, weil damit über die eigentlichen Anforderungen der NIS2 hinaus Regulierung erlassen wird, die in anderen EU-Mitgliedsstaaten u.U. nicht umsetzbar wäre.