expertenReport

Quelle: DALL-E

Cybersicherheit wächst – politische Eingriffe auch

Michael Fiedler

Deutschland verschärft seine Cybersicherheitsregeln. Während Bitkom die NIS-2-Umsetzung als überfällig bezeichnet, sorgt eine zentrale Neuerung für Kritik: Das Innenministerium kann künftig den Einsatz „kritischer Komponenten“ verbieten.

Durch das Gesetz wird die Definition kritischer Infrastrukturen und essenzieller Dienste deutlich ausgeweitet. Damit fallen künftig erheblich mehr Unternehmen unter die verschärften Anforderungen an Risikomanagement, Meldepflichten und IT-Sicherheitsprozesse. Bitkom-Präsident Dr. Ralf Wintergerst bewertet den Schritt positiv: „Cyberangriffe bedrohen Wirtschaft, Verwaltung und Gesellschaft. Die Umsetzung der NIS-2-Richtlinie war überfällig.“

Bundesbehörden erstmals selbst stärker reguliert

Besonders begrüßt der Verband, dass das Gesetz den Anwendungsbereich auf nachgelagerte Bundesbehörden ausdehnt. Für Wintergerst ist dies ein notwendiger Bestandteil einer glaubwürdigen Cybersicherheitsstrategie: „Eine wirksame und glaubwürdige Cybersicherheitsarchitektur setzt voraus, dass der Staat selbst höchste Sicherheitsstandards einhält. Es ist nur konsequent und richtig, dass Bundesbehörden künftig denselben Anforderungen beim Risikomanagement unterliegen wie regulierte Unternehmen.“

Neuregelungen zu „kritischen Komponenten“ sorgen für Kritik

Deutlich kritischer bewertet Bitkom allerdings die neuen Befugnisse des Bundesinnenministeriums zur Definition und Untersagung sogenannter kritischer Komponenten. Das BMI kann künftig – nach Rücksprache mit anderen Ressorts – selbst bestimmen, welche Komponenten als kritisch gelten und deren Einsatz im Unternehmen verbieten. Für den Verband birgt das Risiken:

- fehlende Planungssicherheit,
- mögliche Investitionsstopps,
- Verzögerungen bei Digitalisierungsprojekten,
- unzureichende technische Kriterien.

Wintergerst fordert, dass die Definition weiterhin primär durch Fachbehörden wie Bundesnetzagentur und BSI erfolgen sollte – und dass betroffene Unternehmen vorab konsultiert werden müssen. „Unternehmen brauchen verlässliche Rahmenbedingungen. Verbote können erhebliche Auswirkungen auf die Geschäftstätigkeit haben.“

Was jetzt folgen muss

Aus Bitkom-Sicht bleiben zwei zentrale Handlungsfelder:

Begleitung der Unternehmen durch das BSI: Die neuen Pflichten führen zu erheblichen organisatorischen und technischen Anforderungen. Unternehmen bräuchten praxisnahe Unterstützung. Schnelle Anpassung des KRITIS-Dachgesetzes: Damit alle Regulierungen konsistent sind, müsse das Dachgesetz zeitnah verabschiedet und auf die NIS-2-Umsetzung abgestimmt werden.

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4946925/Cybersicherheit-waechst---politische-Eingriffe-auch/