Cyber-Sicherheits Regulatorik – (k)ein Buch mit sieben Siegeln?

Abstract

Die Digitalgesetzgebung unterliegt derzeit sehr lebhaften Entwicklungen. Dadurch wird der IuK-Einsatz ganz wesentlich und weit über materiell-rechtliche Vorgaben („was“) hinaus reguliert („wie“). Infolge der bekanntlich permanent hohen Cyber-Risiken gilt das insbesondere auch für die anstehende Regulierung verpflichtender Maßnahmen zur Cyber-Sicherheit. Die neue Regulatorik erfordert nicht nur im privaten, sondern insbesondere auch im öffentlichen Sektor eine grundlegende und gesamtheitliche Auseinandersetzung mit der Thematik. Zur ersten Orientierung sind nachfolgend wesentliche Eckpunkte mit Schwerpunkt auf den öffentlichen Sektor kompakt zusammengefasst.

Inhalt

Stand:
08.09.2023

Verfasser-Kontakt:
Renfer@Magenta.de

1. Ausgangslage

Bislang finden sich Regelungen zur Cyber-Sicherheit insbesondere in der nationalen Gesetzgebung wie bspw. dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG ⬇) sowie der dazu ergangenen Verordnung zur Bestimmung Kritischer Infrastrukturen gem. § 10 Abs. 1 BSIG (BSI-Kritisverordnung - BSI-KritisV ⬇). Demnach gelten Grundregeln für die im BSIG referenzierten Behörden bzw. Unternehmen, während besonders herausgehobene, sog. kritische Infrastrukturen ergänzenden Anforderungen unterliegen. Diese werden als sog. KRITIS-Bereiche bezeichnet, die durch deren als bedeutend eingeschätzte Versorgungsrelevanz gekennzeichnet sind. Die Einordnung erfolgt gemäß branchen- bzw. sektoren-spezifischer Schwellwerte. Daneben können insbes. für Behörden föderale Landesregelungen gelten, auf die in Anbetracht der zwangsläufigen föderalen Ausdifferenzierungen hier nicht gesondert eingegangen wird.

2. Aktuelle Entwicklungen im Überblick

Zukünftig bedürfen die nationalen Regelungen grundlegender Novellierungen. Ursächlich dafür sind mehrere Richtlinien (RL) der Europäischen Union (EU), die teilweise bereits im Januar 2023 verabschiedet wurden bzw. deren Verabschiedung auf Basis veröffentlichter Entwürfe in den nächsten Monaten erwartet wird. Im Juli 2023 hat das dafür federführend zuständige Bundesministerium des Inneren und für Heimat (BMI) die nationalen Gesetzesentwürfe zur erforderlichen Novellierung der bisherigen nationalen Cyber-Digitalgesetzgebung (vgl. oben: Ausgangslage) veröffentlicht. Damit gehen verbindliche Umsetzungsfristen einher. Die Zusammenhänge skizziert nachfolgende Tabelle:

EU-RL	Inhalt	Inkraft-treten am	Wirksam-keit ab	nationale Novelle	Stand	Anmerk-ung
2022/2555 sog. NIS2 ⬇	Cyber-Prävention und Dokumenta-tion	16.01.23	17.10.24	NIS2 UmsuCG-E ⬇	03.07.23 *)	NIS2V-E zu §§ 28, 57 folgt
2022/2557 sog. CER ⬇	Härtung/ Resilienz physischer Infrastruktur	16.01.23	17.10.24	KRITIS-DachG-E ⬇	25.07.23	Anpas-sung der KRITIS-V folgt
2019/1020 sog. CRA ⬇	Cyber-Produkt-sicherheit	folgt (Entwurf liegt vor)	folgt	-	-	-

Fußnoten:

⬇ die Quellen-Dokumente in der Tabelle sind verlinkt
NIS: Network and Information Security
CER: Critical Entities Resilience
CRA: Cyber Resiliance Act
*) der jüngste Stand ist entscheidend; im Internet kursieren veraltete und tlw.stark abweichende Entwurfsfassungen („leaks“)

3. Praktische Auswirkungen in drei Handlungsfeldern

Wenngleich die bisherigen nationalen Entwürfe noch Änderungen im laufenden Abstimmungs- und Gesetzgebungsverfahren bis zur Verabschiedung erfahren werden, lassen sie weitgehende neue Unternehmens- und Behördenpflichten erwarten. Stichpunktartig und nicht abschließend werden aufgrund **NIS2** bzw. NIS2UmsuCG (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) drei Handlungsfelder mit vielfältigen Einzelanforderungen zu erwarten sein:

- Handlungsfeld 1: Risikomanagement

  - Etablierung bzw. Erweiterung/Anpassung des CyberSec-Risiko- und Krisenmanagements (als Teil sog. Business Continuity Managements BCM, ggf. [D]ISMS in BCM integrieren)

  - IuK-Lieferketten sowie deren Wechselwirkungen und Abhängigkeiten mittels abgestimmter SLAs (Service Level Agreements mit Dienstleistern) und SBOM (Software Bill Of Materials; „IuK-Stücklisten“, vgl. BSI-TR 03183-2 ⬇, ggf. in Ergänzung zu ITIL- bzw. COBIT-Standards, dort insbes. zur sog. Configuration Management Datenbase CMDB) feststellen

  - potentielles Schadens- als auch Sanktionspotential klären und durch geeignete Vorsorgemaßnahmen Schadens- bzw. Sanktionsrisiken wirksam reduzieren

- Handlungsfeld 2: Registrierungs- und Meldepflichten

  - dreistufige Meldepflichten für Cybervorfälle, fristgerecht an die jeweils zuständige Behörde

    - Basisinformationen innerhalb 24 Stunden

    - Ergänzungsinformationen innerhalb 72 Stunden

    - Ausführlicher Bericht innerhalb eines Monats

- Handlungsfeld 3: Nachweispflichten für getroffene Maßnahmen

  - Vorbereitung auf Sicherheitsprüfungen und ggf. vor-Ort-Kontrollen durch Aufsichts- bzw. Prüfbehörden

  - Infolge Beweislastumkehr geeignete Prozess- und Dokumentations-Gestaltung zur CyberSec-Überwachungspflicht der Unternehmensleitung (bspw. IS-Leitlinie nebst Anlagen anpassen/fortschreiben)

Darüber hinaus ist infolge **CER** bzw. KRITIS-DachG-E zu erwarten:

- Schutz kritischer Infrastrukturen vor nicht Cyber-, sondern physischer Gefahren wie bspw. Sabotage, Feuer, Klimakatastrophen (bspw. Hochwasser); bisher Teil der Inf.Sicherheit, steht in Wechselwirkung mit BCM (s. Handlungsfeld 1).

- Zum angemessenen technischen Gebäudemanagement sowie zur Gebäudeautomatisation stehen neuerdings bspw. die neuen BSI-Grundschutz-Bausteine 13 ⬇ und 14 ⬇ zur

Verfügung. Die Gestaltung von Rechenzentren kann sich an der DIN EN 50600 sowie der zukünftigen ISO 22237 orientieren.

Schließlich kann **CRA** nach dessen Verabschiedung zur Folge haben:

- Anpassung des IuK-Beschaffungsmanagements für CRA-konforme Produkte

- Wechselwirkung mit NIS2 bzgl. IuK-Lieferketten-Dokumentation (sog. SBOM, s.o.)

- Spezifische Auswirkungen auf den Einsatz von freier und open source Software (FOSS) werden derzeit in der Fachwelt diskutiert; daraus resultierende Ergebnisse bedürfen insbesondere für behördlichen IuK-Beschaffungsmaßnahmen besonderer Beachtung.

Regelungs-Details orientieren sich an Geeignetheit und Verhältnismäßigkeit des sog. „Stands der Technik", folgen also dem bereits aus der DSGVO bekannten risikobasierten Ansatz. Der Stand der Technik wird in aller Regel aus den jeweils gültigen Normen (insbes. DIN-, CEN-, ISO-Normen) und anerkannter Standards (bspw. BSI-Grundschutz, ISIS12, VdS10000) abgeleitet und durch deren Einhaltung nachgewiesen. Die bekanntermaßen hochvolatilen IuK-Innovationszyklen führen zur zwangsläufigen Folge, dass sich der Stand der Technik laufend ändert und daher auch die angemessenen und verhältnismäßigen CyberSec-Maßnahmen fortlaufend zu prüfen und anzupassen sind, damit der CyberSec-Digitalgesetzgebung genüge geleistet werden kann. Neu ist dabei nicht die Volatilität, sondern zukünftig konkrete Rechtsfolgen bei Nicht-Berücksichtigung derselben.

Deshalb ist neben erheblichem einmaligem Einführungsaufwand insbesondere mit laufendem Aufwand für die ständige Einhaltung zukünftiger CyberSec-Pflichten und damit Vermeidung von monetären als auch persönlichen Sanktionen zu rechnen. Zur Koordination ist soweit noch nicht vorhanden ein:e Informationssicherheitsbeauftragte:r (ISB) einzusetzen und die fachliche Qualifikation nachzuweisen. Die Entwurfsfassungen der nationalen Gesetzesentwürfe enthalten derzeit noch keine Angaben zum konkreten Erfüllungsaufwand, weil der gegenwärtig im Wege der Verbändeanhörung und nachfolgender Ressortabstimmung erhoben wird. Als Größenordnung kann bis dahin der Pauschalwert von 20% der IT-Betriebskosten dienen (§ 43 NIS2UmsuCG-E). Dem steht bei Verstößen in Anlehnung an die DSGVO die nationale Maximal-Sanktion von 10 Mio. Euro oder 2% des Jahresumsatzes bei Unternehmen gegenüber, bei Behörden individuelle aufsichtsrechtliche Maßnahmen.

4. Weiteres Vorgehen in vier Schritten

In Anbetracht absehbarer praktischer Auswirkungen der Cyber-Digitalgesetzgebung erscheint es angeraten, die dafür erforderlichen Vorbereitungen bereits jetzt zu starten. Dies gilt insbesondere vor dem Hintergrund, dass bei Verletzung zukünftiger Verpflichtungen ein umfassendes Sanktionswerk wirksam wird, dessen Konturen in den Entwürfen bereits heute gut erkennbar sind (vgl. bspw. § 60 NIS2UmsuCG-E). Für ausgewählte Einrichtungen wie bspw. die Träger der gesetzlichen Sozialversicherung sieht § 61 NIS2UmsuCG-E Besonderheiten vor.

Zur Erst-Befassung mit den zeitnah bis Herbst 2024 erforderlichen Maßnahmen können folgende Schritte sinnvoll sein:

Schritt 1: Betroffenheitsfeststellung

Die einschlägige Fachpresse geht davon aus, dass sich die Anzahl der durch NIS2-betroffenen Unternehmen und Behörden in D vsl. vervielfacht, während sich die der KRITIS-Betroffenen vorbehaltlich endgültiger Veröffentlichung der erwarteten nationalen Verordnung zum KRITIS-DachG etwa verdoppeln kann. Die Anforderungen treffen also einen weit größeren Kreis gegenüber Heute.

Breite und Tiefe der Betroffenheit muss individuell geprüft werden, was aufgrund der komplexen Zuordnungs-Vorgaben präzise Analysen erfordert. Die Betroffenheit wird innerhalb einer Matrix von vsl. 18 horizontalen Sektoren (Branchen-Schwellwerte) und vertikalen Zuordnungen festgestellt

- kritische Anlagen/Einrichtungen/Infrastrukturen

- besonders wichtige Anlagen/Einrichtungen

- wichtige Anlagen/Einrichtung und

- Anbieter digitaler Dienste

Da Behörden zukünftig und damit abweichend vom bisherigen status quo einen eigenen Sektor darstellen, wird deren Betroffenheit ganz Wesentlich von den vorgesehenen Schwellwerten, deren Auslegung bzw. Interpretation und daran anschließend der vertikalen Zuordnung abhängen. Über diese Matrix hinaus kann der Gesetz- und Verordnungsgeber kritische Anlagen explizit benennen.

Darüber hinaus weichen die Betroffenheits-Schwellwerte für Unternehmen (ab 50/250 Beschäftigte bzw. ab 10/50 Mio Euro Jahresumsatz) von denen für Behörden ab, so dass deren Betroffenheit spätestens ab einer Behördengröße von mind. 250 Beschäftigten wahrscheinlich sein wird.

Schritt 2: Zeitachsen-Sensibilisierung

Nach aktuellem Kenntnisstand werden einige Nachweispflichten sowie Sanktionsregeln erst nach dem Inkrafttreten mit Zeitversatz wirksam werden können. Daher kann der Realisierungs-Zeitplan mit entsprechenden Prioritäten versehen werden. Am generellen Zieltermin im Herbst 2024 ändert das natürlich nichts; es gilt deshalb, die Zeit bis dahin vorbereitend zu nutzen.

Schritt 3: Deltaanalyse

In aller Regel verfügen Unternehmen und Behörden bereits über Werkzeuge zum CyberSec-Management, wie bspw. ein Informations-Sicherheits-Management-System (ISMS) und daran orientierte Prozesse. Je nach Ausprägung und Aktualität bietet sich deren Spiegelung gegen die Betroffenheits-Analyse an. Dem schließen sich Risikoanalysen an, welche Geeignetheit und Verhältnismäßigkeit erforderlicher Maßnahmen nach dem sog. „Stand der Technik“ auf Basis der anerkannten Normen und Standards feststellen.

Schritt 4: Umsetzungsplanung

Aus Zeitablauf (vgl. 2.) und Deltaanalyse (vgl. 3.) können schließlich konkrete, unternehmensspezifische Maßnahmen abgeleitet und in einem Umsetzungsplan priorisiert

werden, dessen Umsetzung der ISB koordiniert und an die Behörden- bzw. Unternehmensleitung berichtet.

Die vorliegenden sog. Referenten-Entwürfe zur nationalen Umsetzung der EU-CyberSec-Digitalgesetzgebung müssen den nationalen Gesetzgebungsprozess noch vollständig durchlaufen. Bis dahin werden offenkundige Unschärfen in Begrifflichkeiten als auch deren Definitionen wie insbes. zur essenziell entscheidenden vertikalen Unternehmenszuordnung der Harmonisierung bedürfen. Sinngemäß Ähnliches gilt zur sog. Kohärenz der Novellen zu den nationalen CyberSec-Regelungen untereinander als auch in Wechselwirkung zur EU-DSGVO und dem BSDG als deren nationaler Umsetzung; bspw. würden nach aktuellem Entwurfsstand zukünftig mit dem BSI (für NIS2), dem BBK (für KritisV) und dem BfDI (für DSGVO) drei Aufsichts- und Meldebehörden parallel agieren, was häufig überlappende Meldepflichten zur Folge hätte. Gleichwohl ist sich die Fachwelt bereits jetzt ganz überwiegend einig, dass nach Abschluss des Gesetzgebungsverfahrens für die operative Umsetzung der notwendigen Maßnahmen und je nach Maß der Unternehmens-individuellen Betroffenheit kaum mehr ausreichend Zeit verbleibt. Insbesondere drängt daher die Zeit zum Abschluss der lfd. Gesetzgebungsprozesse sowie zur Veröffentlichung daran konkretisierend anschließender Verordnungen.

Abrundend sei zur Vollständigkeit angemerkt, dass neben der nationalen Umsetzung der drei neuen EU-Richtlinien zur Cybersicherheit und der dazu im Entwurf vorliegenden Bundesgesetzgebung weitere föderale Regelungen zu erwarten sind. So haben bspw. Hessen mit dem sog. HITSichG sowie der Freistaat Bayern mit der Bay. DigV zum Bay. DigG bereits im Mai 2023 entsprechende Entwürfe vorgelegt, die nach Verabschiedung bei den jeweiligen Landes- bzw. Kommunalbehörden zu beachten sein werden.

5. Ausblick

Nach belastbarer Auflösung vielfältiger Begriffsdefinitionen, der Kohärenz-Fragen und nicht zuletzt durch die anstehende(n) Verordnung(en), wird die erste grobe Betroffenheitsanalyse differenzierte Zuordnungen der konkreten Tiefe und Breite individueller Einzelmaßnahmen erlauben.

Zu gegebener Zeit kann daher ein konkretisierender Teil 2 dieser Veröffentlichung folgen.