VERBAND DER INTERNETWIRTSCHAFT E.V.

Infopapier

zur aktuellen Cybersicherheitspolitik

Berlin, 01. Juli 2026

Die Cybersicherheitspolitik befindet sich in einer Phase struktureller Verdichtung. Mit NIS2, KRITIS-Dachgesetz, Cyber Resilience Act, der Revision des Cybersecurity Act und den nationalen Plänen zur Stärkung der Cyberabwehr wird der Ordnungsrahmen für digitale und physische Resilienz erweitert und umstrukturiert. Für Unternehmen bedeutet das nicht nur zusätzliche Compliance, sondern einen grundlegenden Wechsel: Cybersicherheit wird stärker zur Managementaufgabe, zur Produktanforderung, zur Lieferkettenfrage und zum Bestandteil staatlicher Sicherheitsarchitektur.

Die zentrale politische Herausforderung liegt daher nicht mehr allein in der Schaffung neuer Vorgaben. Entscheidend ist, ob die verschiedenen Regelwerke kohärent ineinandergreifen, ob Zuständigkeiten zwischen BSI, BBK, Sicherheitsbehörden und europäischen Stellen klar abgegrenzt sind und ob regulatorische Pflichten tatsächlich zu höherer Sicherheitsreife führen. Gerade die Diskussionen der vergangenen Wochen, unter anderem bei der Potsdamer Konferenz für Nationale Cybersicherheit, machen deutlich, dass Deutschland von strategischen Ankündigungen in die wirksame Umsetzung kommen muss. Das gilt insbesondere für die praktische Anwendung von NIS2, die Verzahnung mit dem KRITIS-Dachgesetz, den Aufbau des Cyberdome, die Ausgestaltung des GAZ Hybrid und die neuen Befugnisse aus dem Gesetz zur Stärkung der Cybersicherheit.

Daran wird sich gute Cybersicherheitspolitik messen lassen müssen. Unternehmen müssen tatsächlich widerstandsfähiger werden, staatliche Zuständigkeiten müssen im Krisenfall tragfähig sein und neue Pflichten müssen im betrieblichen Alltag umsetzbar bleiben. Cybersicherheitspolitik schafft dann einen Mehrwert, wenn sie Orientierung gibt, Vertrauen stärkt und die Fähigkeit verbessert, Angriffe zu verhindern oder ihre Folgen wirksam zu begrenzen.

1. Konsolidierung statt weiterer Schichtung im Cybersicherheitsrecht

Die aktuellen Vorhaben setzen an unterschiedlichen Stellen an. NIS2 nimmt Unternehmen und Einrichtungen stärker in die Pflicht. Das KRITIS-Dachgesetz ergänzt die digitale Sicherheit um physische Resilienz. Der Cyber Resilience Act verankert Cybersicherheit als Produkteigenschaft. Die Revision des Cybersecurity Act soll Zertifizierung und europäische Koordinierung weiterentwickeln. Nationale Konzepte wie der Cyberdome betreffen die staatliche Abwehrfähigkeit.

Diese Regelungsstränge dürfen nicht isoliert behandelt werden. Für Unternehmen ist entscheidend, dass sie einen klaren, strukturierten und nachvollziehbaren Rechtsrahmen haben. Relevant ist, ob Pflichten zueinander passen, ob Begriffe einheitlich verstanden werden und ob Verfahren im Ernstfall funktionieren. Wo Unternehmen mehreren Regimen zugleich unterfallen, sind konsistente Auslegung, abgestimmte Aufsicht und möglichst einheitliche digitale Meldewege unabdinglich.

Der Staat sollte deshalb klarer darstellen, wie sich die einzelnen Instrumente zu einer gemeinsamen Sicherheitsregulierung fügen. Neue Regulierung darf nicht dazu führen, dass dieselben Risiken

mehrfach bewertet, dokumentiert und gemeldet werden müssen. Cybersicherheit gewinnt nicht durch zusätzliche Schichten an Wirkung, sondern durch rechtliche Klarheit undoperative Anschlussfähigkeit.

2. NIS2 konsequent an Sicherheitswirkung ausrichten und Befähigungsrolle des BSI stärken

NIS2 führt Cybersicherheit aus der Nische der Spezialregulierung. Viele Unternehmen werden erstmals unmittelbar erfasst oder mittelbar über Lieferketten und Vertragsbeziehungen von den Regelungen betroffen sein. Die Vorgaben zu Risikomanagement, Sicherheitsmaßnahmen, Vorfallmeldung und Geschäftsleitungsverantwortung verändern die interne Organisation erheblich.

Für die Praxis bedeutet das, dass Cybersicherheit nicht länger als rein technische Aufgabe verstanden werden kann. Sie muss in Unternehmensführung, Budgetentscheidungen, Beschaffung und Krisenorganisation verankert werden. Besonders anspruchsvoll ist dies für Unternehmen, die bisher nicht im klassischen KRITIS-Umfeld standen und nun innerhalb kurzer Zeit belastbare Strukturen aufbauen müssen.

Gerade deshalb sollte bei der praktischen Anwendung der NIS2-Vorgaben kein Misstrauensverhältnis zwischen Aufsicht und Wirtschaft entstehen. Das BSI braucht eine starke Rolle, diese Rolle muss aber auf Befähigung und rechtssichere Orientierung ausgerichtet sein. Unternehmen benötigen verständliche Maßstäbe, praktikable Verfahren und eine Aufsichtspraxis, die den jeweiligen Risikokontext berücksichtigt.

3. Physische und digitale Resilienz zusammenführen

Das KRITIS-Dachgesetz setzt an einem richtigen Punkt an. Kritische Infrastrukturen sind nicht nur durch digitale Angriffe verwundbar. Auch physische Sabotage, Abhängigkeiten in Lieferketten, Ausfälle zentraler Dienste und hybride Bedrohungen können die Versorgungssicherheit gefährden. Eine moderne Resilienzpolitik muss diese Zusammenhänge abbilden.

Gleichzeitig liegt hier eine der größten Umsetzungsfragen. Das KRITIS-Dachgesetz darf nicht zu einem parallelen Pflichtenregime neben NIS2 werden. Unternehmen können digitale und physische Risiken im Krisenfall nicht getrennt behandeln. Wer getrennte Verfahren schafft, riskiert auch getrennte Verantwortlichkeiten. Erforderlich ist ein Ansatz, der Sicherheitskonzepte, Notfallplanung und Wiederanlauffähigkeit zusammenführt.

Besonders wichtig bleibt die Abstimmung zwischen BSI und BBK. Betreiber brauchen eindeutige Ansprechpartner und belastbare Lageinformationen genauso wie Verfahren, die vor einem Vorfall eingeübt werden können und im Vorfall nicht zusätzliche Unsicherheit erzeugen. Das KRITIS-Dachgesetz ist dann ein Fortschritt, wenn es die tatsächliche Widerstandsfähigkeit kritischer Dienste erhöht. Es wäre dagegen verfehlt, wenn es vor allem neue Nachweise ohne spürbaren Sicherheitsgewinn hervorbringt.

4. Produktsicherheit stärken und Pflichten entlang der Wertschöpfungskette klar abgrenzen

Der Cyber Resilience Act (CRA) verändert den regulatorischen Blick auf digitale Produkte. Cybersicherheit wird nicht erst beim Betreiber relevant, sondern bereits bei Entwicklung, Inverkehrbringen und Wartung. Hersteller müssen künftig stärker nachweisen, dass Produkte mit digitalen Elementen über ihren Lebenszyklus sicher gestaltet, gepflegt und bei Schwachstellen adressiert werden können.

Das ist sachgerecht, weil viele Risiken später im Betrieb nur noch begrenzt beherrschbar sind, etwa wenn vernetzte Geräte ohne verlässlichen Updatepfad dauerhaft in Unternehmensnetzen eingesetzt werden. Unsichere Produkte oder fehlende Prozesse für Schwachstellenmeldungen belasten nicht nur einzelne Nutzer, sondern ganze Wertschöpfungsketten. Mit dem CRA wird Sicherheit stärker zu einem Marktzugangskriterium und damit auch zu einem Wettbewerbsfaktor.

Damit dieser Ansatz jedoch trägt, ist Augenmaß in der Umsetzung erforderlich. Hersteller benötigen klare Standards und handhabbare Konformitätsverfahren, wohingegen Anwenderunternehmen nachvollziehen können müssen, welche Sicherheitseigenschaften ein Produkt bietet und welche Pflichten beim Hersteller verbleiben. Gerade an der Schnittstelle zu NIS2 ist dabei Präzision erforderlich. Betreiberpflichten und Herstellerpflichten dürfen nicht unklar ineinanderlaufen.

5. Zertifizierung als Vertrauensinstrument stärken und politische Eingriffe begrenzen

Die Revision des Cybersecurity Act bietet die Chance, europäische Cybersicherheitszertifizierung stärker als Vertrauensinstrument des Binnenmarkts auszugestalten. Ein wirksamer European Cybersecurity Certification Framework kann Beschaffung erleichtern, Nachweise vereinfachen und die Umsetzung unterschiedlicher Cybersicherheitsvorgaben besser miteinander verbinden. Dafür müssen Zertifizierungsverfahren transparent, risikobasiert und eng an europäischen sowie internationalen Standards ausgerichtet bleiben.

Zertifizierung darf nicht zu einem zusätzlichen Marktzugangshindernis werden. Wenn Anforderungen aus NIS2, dem Cyber Resilience Act oder sektorspezifischem Recht bereits erfüllt werden, muss Zertifizierung diese Nachweise nutzbar machen und darf keine doppelten Prüf-, Berichts- oder Compliancepflichten auslösen. Ihr Mehrwert liegt gerade darin, Vergleichbarkeit zu schaffen und Fragmentierung im Binnenmarkt zu vermeiden.

Kritisch ist der aktuelle Vorschlag der EU Kommission dort, wo neben die technische Zertifizierung weitreichende Eingriffsmöglichkeiten im Bereich der ICT-Lieferketten treten. Lieferantenbezogene Beschränkungen, Hochrisikoeinstufungen oder faktische Austauschpflichten für bestehende Infrastruktur dürfen nicht zum Regelinstrument europäischer Cybersicherheitspolitik werden. Sie kommen nur dort in Betracht, wo konkrete, belegbare und verhältnismäßig zu adressierende Risiken vorliegen. Andernfalls droht die Zertifizierung als zentrales Vertrauensinstrument entwertet zu werden. Auch eine stärkere Rolle von ENISA sollte an diesem Maßstab ausgerichtet werden. ENISA kann europäische Koordinierung verbessern und technische Expertise bündeln. Diese Rolle muss aber klar technisch, transparent und standardorientiert bleiben.

6. Cyberdome mit klar defensiver Ausrichtung

Die Pläne für einen Cyberdome zeigen, dass die Bundesregierung Cybersicherheit stärker strategisch organisieren will. Dieser Anspruch ist richtig. Deutschland braucht bessere Lagebilder, frühere Warnungen und eine engere Zusammenarbeit zwischen Staat und Wirtschaft. Gerade groß angelegte Angriffskampagnen lassen sich nicht allein auf Ebene einzelner Unternehmen bewältigen.

Der Begriff Cyberdome bleibt jedoch erklärungsbedürftig. Politisch tragfähig ist er nur, wenn er als defensive Schutzarchitektur verstanden wird. Dazu gehören bessere Detektion, rechtssichere Warn- und Reaktionsmechanismen, schneller Informationsaustausch und verlässliche Unterstützung betroffener Unternehmen. Problematisch wird es dort, wo der Begriff mit offensiven Eingriffen oder unklaren Vorstellungen aktiver Cyberabwehr verbunden wird.

Aus rechtsstaatlicher Sicht braucht Cyberabwehr klare Grenzen. Maßnahmen, die in fremde Systeme eingreifen oder Daten verändern, werfen erhebliche verfassungsrechtliche, völkerrechtliche und technische Fragen auf. Eine wirtschaftsnahe Cybersicherheitspolitik sollte deshalb auf Schutz, Prävention und Wiederherstellung setzen. Hackback-Rhetorik schafft keine Sicherheit. Sie kann im Gegenteil Vertrauen beschädigen und Verantwortlichkeiten verwischen.

7. Rechtssichere Cyberabwehr statt weitreichender Eingriffsbefugnisse

Das Gesetz zur Stärkung der Cybersicherheit gehört in diesem Zusammenhang zu den politisch zentralen Vorhaben. Es soll die Handlungsfähigkeit des Bundes bei Cyberangriffen erhöhen und erweitert dafür die Befugnisse von BSI, BKA und Bundespolizei. Der Ansatz ist im Grundsatz nachvollziehbar. Eine bessere staatliche Reaktionsfähigkeit darf jedoch nicht dazu führen, dass tiefgreifende Eingriffe in digitale Infrastrukturen, unklare Mitwirkungspflichten für Anbieter oder faktische Hackback-Befugnisse normalisiert werden.

Gerade Maßnahmen auf DNS-Ebene zeigen, wie schmal der Grat zwischen wirksamer Abwehr und unverhältnismäßigen Kollateralschäden ist. Domainweite Eingriffe können auch rechtmäßige Angebote und unbeteiligte Dritte treffen, insbesondere wenn ursprünglich legitime Domains kompromittiert wurden oder mehrere Akteure dieselbe Infrastruktur nutzen. Vorrang müssen deshalb präzise, reversible und zeitlich eng begrenzte Maßnahmen haben.

Auch der Datenaustausch mit dem BSI sollte kooperativ und zweckgebunden ausgestaltet werden. Unternehmen können einen wichtigen Beitrag zu Lagebildern und schneller Reaktion leisten. Dafür sind aber klare Schutzstandards, praxistaugliche Schnittstellen und ein erkennbarer Mehrwert für die betroffenen Anbieter erforderlich. Eine einseitige Herausgabepflicht hochsensibler technischer Daten würde Vertrauen eher schwächen als stärken.

8. Koordination hybrider Bedrohungen verbessern und Wirtschaft wirksam einbinden

Die Eröffnung des Gemeinsamen Zentrums zur Abwehr hybrider Bedrohungen (GAZ Hybrid) passt zur veränderten Sicherheitslage. Hybride Angriffe verbinden digitale Operationen mit Sabotage, Spionage, Desinformation und wirtschaftlichem Druck. Ein gemeinsames Lagebild kann helfen, Entwicklungen früher zu erkennen und staatliches Handeln besser zu koordinieren.

Für Unternehmen ist dieser Ansatz relevant, weil sie häufig früh betroffen sind. Angriffe auf Netze, Dienste, Lieferketten oder öffentliche Wahrnehmung treffen die Wirtschaft unmittelbar. Das GAZ Hybrid sollte deshalb nicht nur als behördeninterne Struktur verstanden werden. Dafür sind belastbare Schnittstellen zur Wirtschaft und Informationen, die für betroffene Branchen praktisch verwertbar sind, erforderlich.

Dabei muss der rechtsstaatliche Rahmen klar bleiben. Die Zusammenarbeit verschiedener Behörden darf nicht zu intransparenten Datenflüssen oder unklaren Verantwortlichkeiten führen. Das Trennungsgebot und die Zweckbindung staatlicher Datenverarbeitung sind keine Formalien, sondern Voraussetzungen für Vertrauen. Das GAZ Hybrid ist dann ein Gewinn, wenn es Orientierung schafft und Krisenreaktionen verbessert. Es darf nicht zu einer weiteren Ebene werden, die neue Pflichten erzeugt, ohne die Sicherheitslage der Unternehmen spürbar zu verbessern.

Über eco: Mit rund 1.000 Mitgliedsunternehmen ist eco (www.eco.de) der führende Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, schafft Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. eco hat Standorte in Köln, Berlin und Brüssel. eco setzt sich in seiner Arbeit vorrangig für ein leistungsfähiges, zuverlässiges und vertrauenswürdiges Ökosystem digitaler Infrastrukturen und Dienste ein.