VDA Verband der Automobilindustrie

Stellungnahme

Zum Referentenentwurf eines Gesetzes zur Stärkung der Cybersicherheit

März 2026

1. Einführung

Der Verband der Automobilindustrie (VDA) bedankt sich für die Gelegenheit zur Stellungnahme zum Referentenentwurf eines Gesetzes zur Stärkung der Cybersicherheit vom 24. Februar 2026. Mit dem Referentenentwurf verfolgt die Bundesregierung das Ziel, die Fähigkeiten staatlicher Stellen zur Erkennung, Analyse und Abwehr von Cyberangriffen weiter auszubauen und hierfür insbesondere die gesetzlichen Grundlagen im Bundespolizeigesetz, im Bundeskriminalamtgesetz sowie im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik weiterzuentwickeln.

Cyberangriffe stellen eine zunehmende Herausforderung für Staat, Wirtschaft und Gesellschaft dar. Mit der fortschreitenden Digitalisierung von Produkten, Produktionsprozessen und Dienstleistungen wächst zugleich die Bedeutung sicherer informationstechnischer Systeme. Ihre Funktionsfähigkeit ist eine zentrale Voraussetzung für die Stabilität moderner Volkswirtschaften sowie für die Wettbewerbsfähigkeit des Wirtschaftsstandorts Deutschland.

Eine leistungsfähige staatliche Cyberabwehr ist ein zentraler Bestandteil der digitalen Resilienz Deutschlands. Klare Zuständigkeiten der Sicherheitsbehörden, wirksame Instrumente zur Gefahrenabwehr sowie eine verbesserte Lageerkennung im Cyberraum können wesentlich dazu beitragen, digitale Infrastrukturen zu schützen und Cyberangriffe frühzeitig zu erkennen.

Der Referentenentwurf sieht hierzu eine Weiterentwicklung der Aufgabenverteilung zwischen verschiedenen Bundesbehörden vor. Während das Bundesamt für Sicherheit in der Informationstechnik (BSI) seine Rolle bei der technischen Analyse, der Lageerkennung sowie der Unterstützung betroffener Einrichtungen weiter ausbauen soll, erhalten die Polizeibehörden des Bundes zusätzliche operative Befugnisse zur Abwehr schwerwiegender Cyberangriffe. Hierzu zählen insbesondere Maßnahmen zur Einschränkung oder Umleitung von Datenverkehr sowie Eingriffe in informationstechnische Systeme.

Darüber hinaus sieht der Referentenentwurf zusätzliche Aufgaben und Befugnisse für staatliche Behörden sowie neue Mitwirkungs- und Auskunftspflichten für Unternehmen und Anbieter digitaler Dienste vor. Diese Regelungen gehen mit Erfüllungsaufwänden für Verwaltung und Wirtschaft einher. Aus Sicht der Automobilindustrie ist es wichtig, dass solche zusätzlichen Anforderungen verhältnismäßig ausgestaltet werden und sich auf das für eine wirksame Cyberabwehr erforderliche Maß beschränken.

Unternehmen der Automobilindustrie investieren bereits heute erhebliche Ressourcen in den Schutz ihrer informationstechnischen Systeme sowie in die Umsetzung bestehender regulatorischer Anforderungen im Bereich der Cybersicherheit. Neue gesetzliche Verpflichtungen sollten daher klar definiert, technisch praktikabel ausgestaltet und mit bestehenden europäischen Regelungen abgestimmt werden, um zusätzliche bürokratische Belastungen und Doppelregulierungen zu vermeiden.

Die Automobilindustrie ist als hochinnovative und stark digitalisierte Branche in besonderem Maße auf sichere informationstechnische Systeme angewiesen. Fahrzeuge entwickeln sich zunehmend zu softwaredefinierten Systemen, die über digitale Plattformen, Cloud-Infrastrukturen und Kommunikationsnetze miteinander verbunden sind. Entwicklungs-, Produktions- und Logistikprozesse sind stark digitalisiert und auf stabile IT-Infrastrukturen angewiesen. Darüber hinaus erstrecken sich die Wertschöpfungsnetzwerke der Branche über globale Lieferketten mit einer Vielzahl miteinander vernetzter Systeme und Akteure.

Vor diesem Hintergrund können staatliche Maßnahmen zur Cyberabwehr unmittelbare oder mittelbare Auswirkungen auf industrielle IT-Strukturen haben. Neue gesetzliche Regelungen sollten daher die besonderen Anforderungen komplexer industrieller IT-Ökosysteme berücksichtigen und gleichzeitig ein hohes Maß an Rechtssicherheit für Unternehmen gewährleisten.

Der VDA unterstützt daher grundsätzlich das Ziel des Referentenentwurfs, die Cyberabwehrfähigkeiten Deutschlands weiterzuentwickeln. Gleichwohl sieht die Automobilindustrie in einzelnen Punkten Anpassungsbedarf, um eine Balance zwischen effektiver Gefahrenabwehr, dem Schutz sensibler Unternehmensdaten sowie stabilen industriellen Prozessen zu gewährleisten.

Vor diesem Hintergrund hebt die Automobilindustrie insbesondere folgende zentrale Anliegen hervor:

• Staatliche Eingriffe in informationstechnische Systeme
Der Referentenentwurf sieht weitreichende Eingriffsbefugnisse staatlicher Behörden in IT-Systeme vor, die in komplexen industriellen IT-Umgebungen unbeabsichtigte Auswirkungen auf Produktionsprozesse, digitale Dienste oder Lieferketten haben können.
Staatliche Maßnahmen sollten daher klar auf schwerwiegende Gefahrenlagen begrenzt und – soweit möglich – unter Einbeziehung der betroffenen Unternehmen umgesetzt werden.

• Schutz sensibler Unternehmensdaten
Bei möglichen Zugriffen auf Unternehmenssysteme können auch hochsensible Datenbestände wie Entwicklungsdaten, Softwarecode oder Geschäftsgeheimnisse betroffen sein. Der gesetzliche Rahmen sollte daher sicherstellen, dass Zugriffe strikt zweckgebunden erfolgen, technisch auf notwendige Datenbereiche begrenzt werden und klare Lösch- und Schutzregelungen bestehen.

• Verpflichtungen für digitale Diensteanbieter
Der Referentenentwurf sieht zusätzliche Informations- und Mitwirkungspflichten für Anbieter digitaler Dienste vor, die auch Unternehmen der Automobilindustrie betreffen können.
Neue Verpflichtungen sollten daher verhältnismäßig ausgestaltet und eng mit bestehenden europäischen Cybersicherheitsregelungen abgestimmt werden, um Doppelregulierungen zu vermeiden.

• Domain-Blocking und DNS-Maßnahmen
Die vorgesehenen Befugnisse zur Änderung von Nameserver-Einträgen oder zur Umleitung von Datenverkehr können auch legitime digitale Dienste betreffen und unbeabsichtigte Beeinträchtigungen verursachen. Solche Maßnahmen sollten daher nur auf Grundlage klar definierter Gefahrenlagen erfolgen und durch transparente Verfahren sowie wirksame Korrekturmechanismen flankiert werden.

• Zusammenarbeit zwischen Staat und Wirtschaft
Eine wirksame Cyberabwehr erfordert einen engen Austausch zwischen staatlichen Stellen und der Wirtschaft, da Unternehmen häufig frühzeitig über technische Informationen zu Angriffsmustern verfügen. Bestehende Kooperations- und Informationsformate sollten daher weiterentwickelt und praxisnah ausgestaltet werden, um einen vertrauensvollen und effizienten Informationsaustausch zu ermöglichen.

• **Angriffserkennungssysteme bei kritischen Anlagen**
Die verpflichtende Nutzung und mögliche Anbindung von Angriffserkennungssystemen an staatliche Stellen kann für Betreiber kritischer Anlagen zusätzlichen technischen und organisatorischen Aufwand bedeuten. Die konkreten Anforderungen sollten daher transparent ausgestaltet und in enger Abstimmung mit der Wirtschaft entwickelt werden.

• **Threat Hunting und Incident Response durch das BSI**
Die vorgesehene Erweiterung der technischen Unterstützungsmöglichkeiten des BSI kann zur Verbesserung der Cyberabwehr beitragen, erfordert jedoch klare und transparente Verfahren für den Zugriff auf Unternehmenssysteme. Entsprechende Maßnahmen sollten weiterhin auf Grundlage eines Ersuchens der betroffenen Einrichtung erfolgen und klar nachvollziehbar ausgestaltet sein.

• **Internationale Cyberoperationen**
Cyberangriffe sind häufig grenzüberschreitend organisiert, sodass internationale Zusammenarbeit notwendig ist, gleichzeitig aber rechtliche Risiken für global tätige Unternehmen entstehen können. Der gesetzliche Rahmen sollte daher sicherstellen, dass Mitwirkungs- und Zugriffspflichten grundsätzlich auf Systeme im deutschen Hoheitsgebiet beschränkt bleiben.

• **Bußgelder und Sanktionen**
Der Referentenentwurf sieht Bußgelder für Verstöße gegen Mitwirkungs- und Informationspflichten vor, deren Anwendung für Unternehmen nachvollziehbar und rechtssicher ausgestaltet sein muss. Sanktionsregelungen sollten daher an klar definierte Pflichten anknüpfen und so ausgestaltet sein, dass sie die Kooperation zwischen Wirtschaft und Behörden unterstützen.

Im Einzelnen:

2.Bedeutung von Cybersicherheit für die Automobilindustrie

Cybersicherheit ist für die Automobilindustrie von zentraler Bedeutung. Fahrzeuge entwickeln sich zunehmend zu softwaredefinierten Systemen, die über digitale Plattformen, Cloud-Infrastrukturen und Kommunikationsnetze miteinander verbunden sind. Parallel dazu sind Entwicklungs-, Produktions- und Logistikprozesse weitgehend digitalisiert und auf eine zuverlässige IT-Infrastruktur angewiesen.

Die Automobilindustrie gehört zu den am stärksten digitalisierten Industriezweigen. Moderne Fahrzeuge bestehen aus komplexen softwarebasierten Systemen, die über drahtlose Schnittstellen, Cloud-Infrastrukturen und digitale Plattformen miteinander verbunden sind. Gleichzeitig sind Entwicklungs-, Produktions- und Logistikprozesse in der Branche hochgradig digitalisiert und international vernetzt.

Störungen informationstechnischer Systeme können daher nicht nur wirtschaftliche Schäden verursachen, sondern auch erhebliche Auswirkungen auf Produktionsabläufe, Lieferketten sowie auf digitale Fahrzeugfunktionen haben. Cyberangriffe können daher nicht nur wirtschaftliche Schäden verursachen, sondern auch Auswirkungen auf sicherheitsrelevante Systeme haben. Entsprechend investiert die Automobilindustrie bereits heute erhebliche Ressourcen in umfassende Cybersecurity-Strukturen. Dazu gehören unter anderem unternehmensweite Cybersecurity-Managementsysteme, kontinuierliche Risikoanalysen sowie umfangreiche Test- und Monitoringmaßnahmen.

Darüber hinaus unterliegt die Branche bereits zahlreichen regulatorischen Anforderungen im Bereich der Cybersicherheit, insbesondere auf europäischer Ebene. Ziel dieser Regelungen ist es, ein hohes Sicherheitsniveau für Fahrzeuge, digitale Dienste und industrielle Systeme sicherzustellen.

3. Auswirkungen staatlicher Eingriffe auf industrielle Systeme

Der Referentenentwurf sieht unter bestimmten Voraussetzungen operative Maßnahmen staatlicher Behörden zur Abwehr schwerwiegender Cyberangriffe vor. Hierzu zählen insbesondere Maßnahmen wie die Untersagung des Betriebs informationstechnischer Systeme, die Umleitung oder Unterbindung von Datenverkehr sowie Eingriffe in informationstechnische Systeme zur Erhebung, Löschung oder Veränderung von Daten gemäß § 41a Absatz 2 BPolG-RefE sowie §§ 62c bis 62e BKAG-RefE.

Solche Maßnahmen können im Falle gravierender Cyberangriffe ein wichtiges Instrument zur Gefahrenabwehr darstellen. Dabei ist jedoch zu berücksichtigen, dass industrielle IT-Strukturen häufig hochkomplexe und eng miteinander vernetzte Systeme umfassen. Eingriffe in einzelne Komponenten können daher unbeabsichtigte Auswirkungen auf andere Systeme oder Prozesse haben.

In industriellen IT-Umgebungen sind Systeme häufig eng miteinander verzahnt. Eingriffe in einzelne Komponenten können daher weitreichende Auswirkungen auf Produktionsprozesse oder logistische Abläufe haben.

Beispielsweise können Maßnahmen wie die Umleitung von Datenverkehr oder die Einschränkung von Systemfunktionen auch Systeme betreffen, die für Produktionssteuerung, Software-Updates von Fahrzeugen oder die Koordination globaler Lieferketten erforderlich sind.

Gerade in global organisierten Lieferketten können Störungen einzelner IT-Systeme Auswirkungen auf Produktionsabläufe oder logistische Prozesse haben. Vor diesem Hintergrund ist es wichtig, dass staatliche Maßnahmen zur Cyberabwehr – insbesondere Eingriffe in informationstechnische Systeme gemäß § 41a Absatz 2 Nummer 3 BPolG-RefE beziehungsweise § 62e BKAG-RefE – die besonderen Strukturen industrieller IT-Architekturen berücksichtigen.

Zudem sollte sichergestellt werden, dass Unternehmen nicht für Schäden haftbar gemacht werden können, die unmittelbar aus staatlichen Cyberabwehrmaßnahmen resultieren. Wenn staatliche Behörden Maßnahmen wie die Einschränkung von Systemfunktionen oder die Umleitung von Datenverkehr nach § 41a Absatz 2 Nummer 1 und 2 BPolG-RefE beziehungsweise §§ 62c und 62d BKAG-RefE anordnen oder durchführen, sollten klare Regelungen bestehen, die eine Haftung betroffener Unternehmen für daraus entstehende Schäden ausschließen.

4. Schutz sensibler Unternehmensdaten

Unternehmen der Automobilindustrie verarbeiten in ihren IT-Systemen umfangreiche sensible Datenbestände. Dazu zählen insbesondere Entwicklungs- und Konstruktionsdaten, Softwarecodes sowie strategische Forschungsinformationen, aber auch wesentliche Geschäfts- und Unternehmenskennzahlen, Vertrags- und Lieferketteninformationen sowie Kundendaten. Der Schutz dieser Daten ist eine zentrale Voraussetzung für Innovationsfähigkeit, Wettbewerbsfähigkeit und das Vertrauen von Kunden und Geschäftspartnern. Neben klassischen Geschäftsgeheimnissen können auch technische Betriebsdaten oder Nutzungsdaten aus digitalen Diensten

Rückschlüsse auf interne Prozesse, Geschäftsstrategien oder Kundenbeziehungen zulassen und sind daher ebenfalls besonders schutzbedürftig. Der Schutz dieser Daten ist eine zentrale Voraussetzung für Innovationsfähigkeit und internationale Wettbewerbsfähigkeit.

Der gesetzliche Rahmen für Maßnahmen der Cyberabwehr sollte daher sicherstellen, dass ein Zugriff auf Unternehmensdaten auf das notwendige Maß beschränkt bleibt und klare Vorgaben für Speicherung, Nutzung und Löschung solcher Daten bestehen. Dies könnte beispielsweise dadurch gewährleistet werden, dass Zugriffe auf Unternehmenssysteme ausschließlich zweckgebunden erfolgen, technisch auf die für die Gefahrenabwehr erforderlichen Datenbereiche begrenzt werden und erhobene Daten nach Abschluss der jeweiligen Maßnahme unverzüglich gelöscht werden, sofern sie für die weitere Gefahrenabwehr nicht mehr erforderlich sind.

5. Verpflichtungen für digitale Diensteanbieter

Der Referentenentwurf sieht zusätzliche Verpflichtungen für Anbieter digitaler Dienste und Telekommunikationsanbieter vor. Hierzu gehört insbesondere die Verpflichtung zur Bereitstellung sicherheitsrelevanter technischer Informationen gegenüber dem BSI in der Informationstechnik gemäß § 15 Absatz 6 BSIG-RefE.

Auch Unternehmen der Automobilindustrie betreiben zunehmend digitale Dienste im Zusammenhang mit vernetzten Fahrzeugen, Mobilitätsplattformen und digitalen Serviceangeboten. Vor diesem Hintergrund ist es wichtig, dass neue Verpflichtungen verhältnismäßig ausgestaltet werden und bestehende europäische Regulierung berücksichtigen.

6. Domain-Blocking / Domain Name Service -Maßnahmen

Der Referentenentwurf sieht Maßnahmen zur Bekämpfung schädlicher Internet-Domains vor. Hierzu werden neue Befugnisse des BSI geschaffen, insbesondere zur Anordnung von Änderungen an Nameserver-Einträgen gemäß § 16a BSIG-RefE sowie zur Umleitung oder Unterbindung von Datenverkehr gemäß § 17 Absatz 2 BSIG-RefE. Ergänzend werden Verpflichtungen für DNS-Diensteanbieter zur Bereitstellung eines DNS-basierten Schutzes vorgesehen, etwa nach § 16 Absatz 6 BSIG-RefE. Aus Sicht der Automobilindustrie ist das Ziel, schädliche Domain-Infrastrukturen und Angriffsinfrastrukturen frühzeitig zu erkennen und einzudämmen, grundsätzlich nachvollziehbar. Gleichzeitig sollten entsprechende Maßnahmen klar begrenzt, transparent und verhältnismäßig ausgestaltet werden. Insbesondere sollte sichergestellt werden, dass Maßnahmen zur Änderung von Nameserver-Einträgen oder zur Umleitung von Datenverkehr nur auf Grundlage klar definierter Gefahrenlagen erfolgen und technisch so ausgestaltet sind, dass unbeabsichtigte Beeinträchtigungen legitimer Dienste („Overblocking“) vermieden werden.

Darüber hinaus sollte gewährleistet sein, dass betroffene Betreiber über entsprechende Maßnahmen informiert werden und geeignete Möglichkeiten bestehen, mögliche Fehlmaßnahmen zeitnah zu korrigieren.

7. Zusammenarbeit zwischen Staat und Wirtschaft

Eine wirksame Cybersicherheit und Cyberabwehr setzen eine enge Zusammenarbeit zwischen staatlichen Institutionen und der Wirtschaft voraus. Unternehmen verfügen

über umfangreiche technische Expertise sowie über wichtige Informationen zu aktuellen Bedrohungslagen, etwa zu Angriffsmustern, Schwachstellen oder missbräuchlich genutzten IT-Infrastrukturen. Ein strukturierter Austausch solcher Informationen kann wesentlich dazu beitragen, Cyberangriffe frühzeitig zu erkennen und geeignete Gegenmaßnahmen einzuleiten.

Der Referentenentwurf stärkt insbesondere die Informationsbasis staatlicher Stellen. So sieht er insbesondere Auskunfts- und Informationspflichten gegenüber dem BSI vor, etwa im Hinblick auf sicherheitsrelevante technische Informationen nach § 15 Absatz 6 BSIG-RefE. Darüber hinaus werden durch neue Befugnisse zur Analyse von Angriffsinfrastrukturen sowie zur Auswertung technischer Daten zusätzliche Erkenntnismöglichkeiten für staatliche Stellen geschaffen.

Aus Sicht der Automobilindustrie ist es wichtig, dass diese Maßnahmen durch geeignete Kooperationsformate zwischen staatlichen Stellen und Unternehmen ergänzt werden. Gerade bei komplexen Cyberangriffen verfügen Unternehmen häufig über frühzeitige technische Erkenntnisse, die für eine gesamtstaatliche Lagebewertung relevant sein können. Ein vertrauensvoller, möglichst zeitnaher Austausch zwischen Wirtschaft und staatlichen Stellen kann daher einen wichtigen Beitrag zur Verbesserung der Lageerkennung im Cyberraum leisten.

Vor diesem Hintergrund scheint es sinnvoll, bestehende Informations- und Kooperationsformate zwischen Behörden und Wirtschaft weiterzuentwickeln und möglichst praxisnah auszugestalten. Dabei sollte insbesondere darauf geachtet werden, dass der Austausch von Informationen unter Wahrung von Geschäftsgeheimnissen erfolgt und für Unternehmen keine unverhältnismäßigen zusätzlichen bürokratischen Belastungen entstehen.

8. Angriffserkennungssysteme bei kritischen Anlagen

Der Referentenentwurf sieht eine stärkere Nutzung von Systemen zur Angriffserkennung bei kritischen Anlagen vor. Betreiber kritischer Anlagen sollen verpflichtet werden, Systeme zur Angriffserkennung einzusetzen und diese an das BSI anzubinden. Entsprechende Anforderungen ergeben sich aus § 31 Absatz 2 BSIG-RefE. Danach sollen die eingesetzten Systeme kontinuierlich geeignete Parameter, Merkmale aus dem laufenden Betrieb sowie Verfügbarkeitsindikatoren erfassen und automatisiert an das Bundesamt übermitteln, soweit eine entsprechende Anbindung vorgesehen ist.

Aus Sicht der Automobilindustrie können Systeme zur Angriffserkennung einen wichtigen Beitrag zur Verbesserung der Lageerkennung im Cyberraum leisten. Gleichzeitig ist zu berücksichtigen, dass Betreiber kritischer Anlagen bereits heute umfangreiche Maßnahmen zur Angriffserkennung und zur Überwachung ihrer IT-Systeme einsetzen. Eine gesetzliche Verpflichtung zur Anbindung solcher Systeme an staatliche Stellen kann daher mit zusätzlichem technischen und organisatorischen Aufwand verbunden sein. Vor diesem Hintergrund sollten neue Anforderungen verhältnismäßig ausgestaltet werden und den zusätzlichen Erfüllungsaufwand für Unternehmen angemessen berücksichtigen.

Durch die kontinuierliche Analyse technischer Parameter lassen sich potenzielle Angriffe frühzeitig identifizieren und geeignete Gegenmaßnahmen einleiten.

Gleichzeitig ist darauf zu achten, dass die Anforderungen an solche Systeme technisch umsetzbar bleiben und den Stand der Technik berücksichtigen. Dabei sollte insbesondere sichergestellt werden, dass die übermittelten Daten auf sicherheitsrelevante technische Parameter beschränkt bleiben und keine Rückschlüsse auf Geschäftsgeheimnisse, interne Produktionsprozesse, Systemarchitekturen oder

Entwicklungsaktivitäten möglich sind. Insbesondere sollte sichergestellt werden, dass Umfang und Ausgestaltung der Datenerhebung sowie der Datenübermittlung an staatliche Stellen auf das für die Gefahrenabwehr notwendige Maß beschränkt bleiben. Darüber hinaus sollte vermieden werden, dass durch die Übermittlung technischer Informationen Rückschlüsse auf sensible Unternehmensdaten, interne Produktionsprozesse oder Entwicklungsaktivitäten möglich werden.

Vor diesem Hintergrund scheint es uns wichtig, die konkreten Anforderungen an die Anbindung und Ausleitung von Daten transparent auszugestalten und frühzeitig mit betroffenen Unternehmen abzustimmen. Eine enge Abstimmung mit der Wirtschaft kann dazu beitragen, praktikable technische Lösungen zu entwickeln und gleichzeitig ein hohes Maß an Cybersicherheit zu gewährleisten.

9. Threat Hunting / Incident Response durch das BSI

Der Referentenentwurf sieht eine Erweiterung der technischen Unterstützungsmöglichkeiten des BSI bei der Analyse von IT-Sicherheitsvorfällen vor. Entsprechende Befugnisse werden insbesondere in § 11 Absatz 1 BSIG-RefE geregelt. Danach kann das Bundesamt bei einer Beeinträchtigung oder bei Anhaltspunkten für eine mögliche Beeinträchtigung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme auf Ersuchen der betroffenen Einrichtung Maßnahmen durchführen, die zur Suche und Identifikation solcher Beeinträchtigungen oder zur Wiederherstellung der Sicherheit und Funktionsfähigkeit der betroffenen Systeme erforderlich sind.

Die Regelung schafft damit eine gesetzliche Grundlage dafür, dass das Bundesamt betroffene Einrichtungen künftig nicht nur bei bereits eingetretenen IT-Sicherheitsvorfällen unterstützen kann, sondern auch bei der Identifikation möglicher vorbereitender Angriffsaktivitäten in informationstechnischen Systemen. Solche Maßnahmen – häufig als „Threat Hunting“ bezeichnet – können insbesondere dazu beitragen, sogenannte „Prepositioning“-Aktivitäten von Angreifern frühzeitig zu erkennen und damit mögliche spätere Angriffe zu verhindern.

Aus Sicht der Automobilindustrie ist eine Stärkung der technischen Unterstützung durch das BSI grundsätzlich zu begrüßen. Gerade bei komplexen Cyberangriffen kann die technische Expertise staatlicher Stellen einen wichtigen Beitrag zur Analyse von Angriffsmustern sowie zur Stabilisierung betroffener IT-Systeme leisten.

Dabei ist es wichtig, dass entsprechende Maßnahmen weiterhin auf Grundlage eines Ersuchens der betroffenen Einrichtung erfolgen und transparent ausgestaltet sind. Unternehmen müssen nachvollziehen können, welche technischen Maßnahmen durchgeführt werden und in welchem Umfang dabei auf informationstechnische Systeme oder Daten zugegriffen wird. Eine klare Ausgestaltung der entsprechenden Verfahren kann dazu beitragen, Vertrauen zwischen staatlichen Stellen und betroffenen Unternehmen zu stärken und eine effektive Zusammenarbeit im Falle von IT-Sicherheitsvorfällen zu ermöglichen.

10. Internationale Cyberoperationen

Cyberangriffe sind häufig grenzüberschreitend organisiert und betreffen international vernetzte Infrastrukturen. Angriffsstrukturen, Schadsoftware und Steuerungssysteme sind oftmals über mehrere Staaten verteilt, sodass eine wirksame Bekämpfung solcher Aktivitäten nur im Rahmen internationaler Zusammenarbeit erfolgen kann.

Der Referentenentwurf sieht daher eine stärkere Rolle des Bundeskriminalamtes (BKA) bei der internationalen Zusammenarbeit zur Abwehr von Cyberangriffen vor, etwa im Rahmen der neuen Aufgabe nach § 3a BKAG-RefE. Damit soll das BKA künftig auch in Fällen tätig werden können, in denen Cyberangriffe aufgrund ihres internationalen Charakters oder ihrer außen- und sicherheitspolitischen Bedeutung eine koordinierte Zusammenarbeit mit ausländischen Behörden oder internationalen Organisationen erfordern.

Aus Sicht der Automobilindustrie ist eine enge internationale Zusammenarbeit bei der Bekämpfung von Cyberkriminalität grundsätzlich zu begrüßen. Allerdings sollte darauf geachtet werden, dass entsprechende Maßnahmen transparent ausgestaltet sind und die Interessen betroffener Unternehmen angemessen berücksichtigt werden. Gerade bei international koordinierten Maßnahmen kann eine frühzeitige Information betroffener Betreiber dazu beitragen, mögliche Auswirkungen auf industrielle Systeme zu minimieren und notwendige technische Gegenmaßnahmen einzuleiten.

Bei Maßnahmen, die Mitwirkungs- oder Auskunftspflichten von Unternehmen betreffen, sollte zudem klargestellt werden, dass entsprechende Verpflichtungen grundsätzlich auf informationstechnische Systeme im Hoheitsgebiet der Bundesrepublik Deutschland beschränkt bleiben.

Viele Unternehmen der Automobilindustrie betreiben weltweit verteilte IT-Infrastrukturen, etwa für Entwicklung, Produktion oder digitale Dienste. Verpflichtungen, auf Systeme außerhalb Deutschlands zuzugreifen oder dort technische Maßnahmen umzusetzen, könnten Unternehmen in Konflikt mit ausländischen Rechtsordnungen bringen.

Der gesetzliche Rahmen sollte daher sicherstellen, dass staatliche Maßnahmen nicht zu Rechtskonflikten in Drittstaaten führen und Unternehmen dadurch zusätzlichen rechtlichen Risiken ausgesetzt werden

11. Bußgelder und Sanktionen

Der Referentenentwurf enthält zudem Bußgeldregelungen für Verstöße gegen Mitwirkungs- und Auskunftspflichten sowie gegen Offenbarungsverbote im Zusammenhang mit Maßnahmen der Cyberabwehr. Entsprechende Regelungen finden sich unter anderem in § 104 Absatz 1 BPolG-RefE, § 87a BKAG-RefE sowie § 65 Absatz 2 Nummer 3a BSIG-RefE.

Aus Sicht der Automobilindustrie ist es wichtig, dass solche Sanktionsregelungen verhältnismäßig ausgestaltet sind und Unternehmen ausreichende Rechtssicherheit hinsichtlich ihrer Verpflichtungen erhalten. Voraussetzung hierfür ist insbesondere, dass Mitwirkungs- und Informationspflichten klar definiert sind und Unternehmen nachvollziehen können, welche Anforderungen im Einzelfall zu erfüllen sind.

Darüber hinaus sollte berücksichtigt werden, dass Unternehmen bereits heute umfangreiche Maßnahmen zur Sicherung ihrer informationstechnischen Systeme umsetzen und mit staatlichen Stellen zusammenarbeiten. Sanktionsregelungen sollten daher so ausgestaltet sein, dass sie die Kooperation zwischen Wirtschaft und Behörden nicht erschweren, sondern vielmehr einen klaren und verlässlichen Rahmen für die Zusammenarbeit im Bereich der Cybersicherheit schaffen.

Ansprechpartner

Dr. Marcus Bollig
Geschäftsführer
marcus.bollig@vda.de

Martin Lorenz
Abteilungsleiter Security, Daten & Digitalisierung
martin.lorenz@vda.de

Arlina Benson
Referentin Cybersecurity & Wirtschaftsschutz
arlina.benson@vda.de

Der Verband der Automobilindustrie (VDA) vereint mehr als 620 Hersteller und Zulieferer unter einem Dach. Die Mitglieder entwickeln und produzieren Pkw und Lkw, Software, Anhänger, Aufbauten, Busse, Teile und Zubehör sowie immer neue Mobilitätsangebote.

Wir sind die Interessenvertretung der Automobilindustrie und stehen für eine moderne, zukunftsorientierte multimodale Mobilität auf dem Weg zur Klimaneutralität. Der VDA vertritt die Interessen seiner Mitglieder gegenüber Politik, Medien und gesellschaftlichen Gruppen.

Wir arbeiten für Elektromobilität, klimaneutrale Antriebe, die Umsetzung der Klimaziele, Rohstoffsicherung, Digitalisierung und Vernetzung sowie German Engineering. Wir setzen uns dabei für einen wettbewerbsfähigen Wirtschafts- und Innovationsstandort ein. Unsere Industrie sichert Wohlstand in Deutschland: Mehr als 780.000 Menschen sind, direkt in der deutschen Automobilindustrie beschäftigt.

Der VDA ist Veranstalter der größten internationalen Mobilitätsplattform IAA MOBILITY und der IAA TRANSPORTATION, der weltweit wichtigsten Plattform für die Zukunft der Nutzfahrzeugindustrie.

Herausgeber
Verband der Automobilindustrie e. V. (VDA)
Behrenstraße 35,10117 Berlin
www.vda.de

Deutscher Bundestag Lobbyregister-Nr.:
R001243 EU-Transparenz-Register-Nr.:
9557 4664 768-90

Version
März 2026

VDA