

## Beschlussempfehlung und Bericht

des Innenausschusses (4. Ausschuss)

zu dem Gesetzentwurf der Bundesregierung

– Drucksachen 21/6134, 21/6512 –

**Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2024/2847  
über horizontale Cybersicherheitsanforderungen für Produkte mit  
digitalen Elementen  
(Cyberresilienz-Verordnung)**

### A. Problem

Am 10. Dezember 2024 ist die Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung) in Kraft getreten. Die Verordnung (EU) 2024/2847 stellt verpflichtende Anforderungen an die Cybersicherheit von Produkten mit digitalen Elementen auf und erweitert das CE-Kennzeichen um den Aspekt der Cybersicherheit.

Der vorliegende Gesetzentwurf dient der Durchführung der Verordnung (EU) 2024/2847. Geschaffen wird eine Rechtsgrundlage, damit das Bundesamt für Sicherheit in der Informationstechnik (BSI) als Marktüberwachungsbehörde und als notifizierende Behörde unter der Verordnung (EU) 2024/2847 tätig werden kann. Zusätzlich sollen Unterstützungsmaßnahmen für die von der Verordnung (EU) 2024/2847 betroffenen Wirtschaftsakteure ergriffen und Vorschriften für ein Bußgeldverfahren erlassen werden.

### B. Lösung

Der Innenausschuss empfiehlt mit dieser Beschlussempfehlung, den Gesetzentwurf mit einer Maßgabe zu den Inkrafttretensbestimmungen abzuändern.

**Annahme des Gesetzentwurfs in geänderter Fassung mit den Stimmen der Fraktionen CDU/CSU, SPD und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktion der AfD bei Stimmenthaltung der Fraktion Die Linke.**

*Vorabfassung – wird durch die lektorierte Fassung ersetzt.*

**Annahme einer Entschließung mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktion der AfD bei Stimmenthaltung der Fraktionen BÜNDNIS 90/DIE GRÜNEN und Die Linke.**

### **C. Alternativen**

Keine.

### **D. Haushaltsausgaben ohne Erfüllungsaufwand**

Durch das gestaffelte Wirksamwerden der Verpflichtungen aus der Verordnung (EU) 2024/2847 kommen auf das BSI aufgrund dieses Gesetzes laufend neue Fachaufgaben hinzu. Außerdem werden jedes Jahr neue Produkte mit digitalen Elementen in den Verkehr gebracht, wodurch die Anzahl der Produkte, die das BSI als Marktüberwachungsbehörde auf ihre Konformität hin überprüft, stetig ansteigt. Aus diesem Grund werden die Haushaltsausgaben für das BSI bis 2029 sukzessive ansteigen.

Der Personalmehrbedarf beim BSI für die Wahrnehmung der nach diesem Gesetz zugewiesenen Aufgaben beläuft sich bis zum Jahr 2029 dauerhaft auf insgesamt 141 Planstellen/Stellen. Davon entfallen 68 Stellen auf die Wertigkeit des höheren Dienstes, 54 Stellen auf die Wertigkeit des gehobenen Dienstes und 19 Stellen auf die Wertigkeit des mittleren Dienstes.

Zusätzlich entstehen einmalige Sachkosten in Höhe von 10 Millionen Euro. Diese entstehen insbesondere für die Einrichtung eines Reallabors. Laufende jährliche Sachkosten in Höhe von 8,1 Millionen Euro entstehen insbesondere für die Beauftragung externer Dienstleister, die im Rahmen der Marktüberwachung tätig werden sollen.

Der Mehrbedarf an Sach- und Personalmitteln sowie an Planstellen und Stellen für BSI soll im Einzelplan 06 ausgeglichen werden.

### **E. Erfüllungsaufwand**

Die Verpflichtungen für die Wirtschaft und die Bürgerinnen und Bürger ergeben sich aus der unmittelbar geltenden Verordnung (EU) 2024/2847. Mit diesem Durchführungsgesetz werden keine neuen Verpflichtungen geschaffen, sondern lediglich die zuständigen Behörden benannt und deren Zusammenarbeit geregelt. Ein Erfüllungsaufwand für Bürgerinnen und Bürger und die Wirtschaft ergibt sich daher aus diesem Gesetz nicht.

#### **E.1 Erfüllungsaufwand für Bürgerinnen und Bürger**

Siehe Ausführungen unter Abschnitt E.

#### **E.2 Erfüllungsaufwand für die Wirtschaft**

Siehe Ausführungen unter Abschnitt E.

*Vorabfassung – wird durch die lektorierte Fassung ersetzt.*

### E.3 Erfüllungsaufwand der Verwaltung

Für die Verwaltung entsteht durch die gesetzliche Änderung ein laufender Erfüllungsaufwand in Höhe von ca. 20,5 Millionen Euro und ein einmaliger Erfüllungsaufwand in Höhe von ca. 10 Millionen Euro auf Ebene der Bundesverwaltung.

### F. Weitere Kosten

Keine.

*Vorabfassung – wird durch die lektorierte Fassung ersetzt.*

**Beschlussempfehlung**

Der Bundestag wolle beschließen,

- a) den Gesetzentwurf auf Drucksachen 21/6134, 21/6512 mit folgenden Maßgaben, im Übrigen unverändert anzunehmen:

Artikel 4 wird wie folgt geändert:

1. Die Absätze 1 bis 3 werden durch den folgenden Absatz 1 ersetzt:  
„(1) In Artikel 1 treten § 3 Absatz 1 Satz 2 Nummer 30 und 31, § 5 Absatz 3 Satz 2 Nummer 5 und 6 und § 66 des BSI-Gesetzes sowie die Artikel 2 und 3 treten am Tag nach der Verkündung in Kraft.“
2. Der bisherige Absatz 4 wird Absatz 2;

- b) folgende EntschlieÙung anzunehmen:

„I. Der Deutsche Bundestag stellt fest:

Die aktuelle geopolitische Bedrohungslage durch Cyberangriffe, Sabotage und Spionage verdeutlicht den dringenden Bedarf, unsere kritische Infrastruktur resilienter und sicherer aufzustellen. Die Sicherheit unserer Mobilfunknetze im GroÙen genau wie die Sicherheit jedes einzelnen digitalen Produkts im Kleinen muss oberste Priorität in einer Zeit haben, in der sich Deutschland verstärkt hybriden Angriffen ausgesetzt sieht. Digitale und technologische Souveränität bedeuten dabei keine internationale Abschottung, sondern lediglich die Möglichkeit, tatsächliche Alternativen nutzen zu können und nicht in Abhängigkeiten zu verharren.

Mit dem NIS-2-Umsetzungsgesetz, dem KRITIS-Dachgesetz sowie dem europäischen Cyber Resilience Act und dem vorliegenden Durchführungsgesetz wurden bereits wichtige Schritte dieses Weges hin zu mehr Cybersicherheit und weniger Abhängigkeiten ermöglicht.

Dennoch sind die deutsche Wirtschaft, Verwaltung und Infrastrukturen weiterhin in hohem Maße von einzelnen Herstellern und Lieferketten abhängig. Geopolitische Eskalationen, Lieferkettenunterbrechungen, Sicherheitsvorfälle, fehlende Softwareupdates oder Ersatzteile können zu systemischen Risiken führen. Staaten wie China verpflichten in ihrem Land ansässige Hersteller zudem zur Zusammenarbeit mit ihren Geheimdiensten. Die Verwendung kritischer Komponenten nicht vertrauenswürdiger Anbieter birgt erhebliche Gefahren für die IT-Sicherheit, die nationale Sicherheit und die wirtschaftliche Stabilität. Wenn Systeme von Herstellern abhängen, die unmittelbar oder mittelbar unter dem Einfluss eines Drittstaates stehen, macht uns dies verwundbar. Durch das BSIG wird der Einsatz von kritischen Komponenten eines nicht vertrauenswürdigen Herstellers gegenüber Betreibern kritischer Anlagen (KRITIS) bereits reguliert und kann durch das Bundesministerium des Innern untersagt werden. Jedoch bestehen die genannten Gefahren nicht nur für KRITIS-Anlagen, sondern in jedem einzelnen Haushalt, in dem systemkritische Komponenten, beispielsweise Router im Telekommunikationsbereich und Wechselrichter im Bereich Energie, zum Einsatz kommen. In solchen Komponenten können versteckte Hintertüren eingebaut sein, die es ermöglichen können, den Datenverkehr unbemerkt zu überwachen oder abzufangen. Außerdem besteht die Gefahr, dass auf solche Komponenten aus der Ferne zugegriffen werden kann. Sind solche Kompo-

nennten erst einmal tief in einem System verbaut, wäre ihr Austausch nicht nur technisch herausfordernd, sondern vor allem teuer. Daher muss der Markt möglichst effektiv überwacht werden.

Digitale Souveränität und technologische Diversifizierung sind daher wesentliche Voraussetzungen für die Resilienz kritischer Infrastrukturen.

II. Der Deutsche Bundestag fordert die Bundesregierung der 21. Wahlperiode auf:

Im Rahmen der Marktüberwachung nach der Cyberresilienz-Verordnung durch das BSI als Marktüberwachungsbehörde, die Prüfung von Routern vorrangig durchzuführen und den bestehenden Rechtsrahmen auszuschöpfen;

den bisherigen, erfolgreichen Weg weiter zu verfolgen und sich auf europäischer Ebene sowie im Rahmen anstehender Gesetzesvorhaben mit Nachdruck für die Reduzierung der Abhängigkeit kritischer Infrastrukturen von nicht vertrauenswürdigen Herstellern zu einzusetzen und die Diversifizierung kritischer Lieferketten zu stärken;

sich auf Europäischer Ebene im Rahmen der Verhandlungen zum Cybersecurity Act 2 für eine stärkere Regulierung von netz- beziehungsweise systemkritischen Komponenten nicht vertrauenswürdiger Anbieter auf dem EU-Binnenmarkt einzusetzen;

sich auf europäischer Ebene für einen gemeinsamen risikobasierten Ansatz zur Sicherheit kritischer IKT-Lieferketten und zur Stärkung der digitalen Souveränität einzusetzen und diesen Weg gemeinsam mit den europäischen Partnern konsequent weiterzugehen;

bei Beschaffungsaufträgen kritischer digitaler Komponenten neben technischen Sicherheitsanforderungen insbesondere Herstellerabhängigkeiten, Lieferketten, Update- und Wartungsmöglichkeiten sowie die Substituierbarkeit von Komponenten zu berücksichtigen;

durch den Abbau von Abhängigkeiten in der kritischen Infrastruktur gleichzeitig auch deutsche und europäische Hersteller zu stärken, zum Beispiel in den Bereichen Heimrouter und Energieanlagen.“

*Vorabfassung – wird durch die lektorierte Fassung ersetzt.*

Berlin, den 14. Oktober 2026

**Der Innenausschuss**

**Josef Oster**  
Amtierender Vorsitzender

**Marc Henrichmann**  
Berichterstatter

**Steffen Janich**  
Berichterstatter

**Johannes Schätzl**  
Berichterstatter

**Jeanne Dillschneider**  
Berichterstatterin

**Jan Krampe**  
Berichterstatter

*Vorabfassung – wird durch die lektorierte Fassung ersetzt.*

## Bericht der Abgeordneten Marc Henrichmann, Steffen Janich, Johannes Schätzl, Jeanne Dillschneider und Jan Krampe

### I. Überweisung

Der Gesetzentwurf auf **Drucksache 21/6134** wurde in der 83. Sitzung des Deutschen Bundestages am 11. Juni 2026 an den Innenausschuss federführend sowie an den Ausschuss für Recht und Verbraucherschutz, den Haushaltsausschuss und den Ausschuss für Digitales und Staatsmodernisierung zur Mitberatung überwiesen. Dem Haushaltsausschuss wurde der Gesetzentwurf gemäß § 96 der Geschäftsordnung überwiesen. Die Unterrichtung durch die Bundesregierung zur Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung lag auf **Drucksache 21/6512** vor. Der Parlamentarische Beirat für nachhaltige Entwicklung und Zukunftsfragen beteiligte sich gutachtlich (Ausschussdrucksache 21(26)53-12).

### II. Stellungnahmen der mitberatenden Ausschüsse

Der **Ausschuss für Recht und Verbraucherschutz** hat in seiner 55. Sitzung am 14. Oktober 2026 mit den Stimmen der Fraktionen CDU/CSU, SPD und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktion der AfD bei Stimmenthaltung der Fraktion Die Linke die Annahme des Gesetzentwurfs auf Drucksachen 21/6134, 21/6512 in geänderter Fassung empfohlen.

Der **Haushaltsausschuss** hat in seiner 50. Sitzung am 14. Oktober 2026 mit den Stimmen der Fraktionen CDU/CSU, SPD und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktion der AfD bei Stimmenthaltung der Fraktion Die Linke die Annahme des Gesetzentwurfs auf Drucksachen 21/6134, 21/6512 in geänderter Fassung empfohlen. Seinen Bericht gemäß § 96 der Geschäftsordnung wird er gesondert abgeben.

Der **Ausschuss für Digitales und Staatsmodernisierung** hat in seiner 35. Sitzung am 14. Oktober 2026 mit den Stimmen der Fraktionen CDU/CSU, SPD und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktion der AfD bei Stimmenthaltung der Fraktion Die Linke die Annahme des Gesetzentwurfs auf Drucksachen 21/6134, 21/6512 in geänderter Fassung empfohlen.

### III. Beratungsverlauf und Beratungsergebnisse im federführenden Ausschuss

Der **Innenausschuss** hat den Gesetzentwurf auf Drucksachen 21/6134, 21/6512 in seiner 47. Sitzung am 14. Oktober 2026 abschließend beraten und empfiehlt die Annahme des Gesetzentwurfs in der aus der Beschlussempfehlung ersichtlichen Fassung mit den Stimmen der Fraktionen CDU/CSU, SPD und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktion der AfD bei Stimmenthaltung der Fraktion Die Linke.

Die Änderungen entsprechen dem Änderungsantrag der Fraktionen der CDU/CSU und SPD auf Ausschussdrucksache 21(4)239, der zuvor mit den Stimmen der Fraktionen CDU/CSU, SPD und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktion der AfD bei Stimmenthaltung der Fraktion Die Linke angenommen wurde.

Zudem hat der Innenausschuss die Entschließung der Fraktionen der CDU/CSU und SPD auf Ausschussdrucksache 21(4)240 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktion der AfD bei Stimmenthaltung der Fraktionen BÜNDNIS 90/DIE GRÜNEN und Die Linke angenommen.

### IV. Begründung

#### 1. Begründung zum Änderungsantrag

#### Zu Artikel 4 Nummer 1 und Nummer 2

Vorabfassung – wird durch die lektorierte Fassung ersetzt.

Die Änderung ist aufgrund des zeitlichen Fortgangs des Gesetzgebungsverfahrens erforderlich. Die bislang vorgesehene Anknüpfung an den 11. Juni bzw. 11. September 2026 ist durch Zeitablauf gegenstandslos geworden. Die Regelungen finden damit ab ihrem Inkrafttreten Anwendung.

## 2. Begründung der Fraktionen im Ausschuss

Die **Fraktion der CDU/CSU** erklärt, dass mit der Umsetzung des Cyber Resilience Acts erstmals europaweit Produkte mit digitalen Elementen in den Blick genommen und verbindliche Cyber-Sicherheitsanforderungen für solche Produkte definiert würden. Das BSI werde durch die Verordnung zur Marktüberwachungsbehörde aufgewertet. Es sei als notifizierende Behörde für Konformitätsbewertungen und für die Verhängung von Bußgeldern zuständig. So könne Einfluss auf den Markt genommen werden. Die Cyber-Sicherheit von entsprechenden Komponenten sei wichtig, wobei die Wirtschaft eine entscheidende Rolle spiele. Sie begrüßt die Implementierung eines Reallabors für Cyber-Resilienz, in dem Hersteller von Produkten mit digitalen Elementen einen Raum fänden, diese vor der Marktzulassung zu erproben. Gemeinsam mit Verbänden und Unternehmen könne man gute Lösungen erzielen und zur Stärkung der Cyber-Resilienz bei den Komponenten beitragen. Die vorzunehmenden Änderungen beträfen im Wesentlichen Fristen. Mit der Entschließung würden erstmals systemkritische Komponenten ergänzend in den Blick genommen und ein risikobasierter Ansatz betont. Dies beziehe sich insbesondere auf Komponenten wie Router oder Wechselrichter. Es gehe um die Diversifizierung von Lieferketten. Es gehe um die Frage des Umgangs mit nicht vertrauenswürdigen Herstellern. Relevant sei auch die Stärkung der digitalen Souveränität, ebenso wie mit Herstellerabhängigkeiten, mit Software-Updates, Software-Verfügbarkeit oder Wartungsmöglichkeiten umzugehen sei. Zu klären seien auch die Optionen für eine Stärkung europäischer Hersteller.

Der **Fraktion der AfD** sei bekannt, dass durch den Gesetzesentwurf unionsrechtliche Vorgaben umgesetzt werden sollten, um kein Vertragsverletzungsverfahren zu riskieren. Dennoch unterstütze sie das Umsetzungsgesetz nicht. Sie habe in der ersten Lesung darauf hingewiesen, dass die sieben größten US-amerikanischen Tech-Unternehmen mit einer Marktkapitalisierung von 22 Billionen US-Dollar neunmal so viel wert seien wie alle deutschen Unternehmen in den Indizes DAX, MDAX und SDAX zusammen. Durch die zugrunde liegende Verordnung werde die Marktmacht dieser wirtschaftlichen Oligopole weiter zementiert. Die Verordnung schaffe für alle Produkte, die eine Datenverbindung benutzten, also auch für jede Software und jedes vernetzte Küchengerät, umfassende neue bürokratische Pflichten wie ein Schwachstellenmanagement, Produktupdates, technische Dokumentation oder eine externe Bewertung. Diese Bürokratiepflichten überlasteten jeden europäischen Hersteller von technischen Geräten und Software. Sie sei der Auffassung, die Bundesregierung hätte diese Verordnung auf EU-Ebene verhindern müssen. Aufgrund der Verordnung würden Produkte für Verbraucher weniger bezahlbar. 141 neue BSI-Mitarbeiter seien schwer zu rekrutieren. 30 Millionen Euro an Mehrkosten seien in Zeiten knapper Kassen ebenfalls nicht erklärbar. Deshalb sei das Gesetz inklusive des Änderungs- und Entschließungsantrags abzulehnen.

Die **Fraktion der SPD** weist darauf hin, dass der Cyber Resilience Act auch für US-amerikanische Produkte gelte und dadurch die Menschen in Europa schütze. Diesen Grundgedanken des Cyber Resilience Acts begrüße sie ausdrücklich. Die Umsetzung sei daher folgerichtig. Ziel sei gewesen, durch die Umsetzungsverordnung keine weitere Bürokratie zu schaffen. Im Rahmen der Entschließung habe man sich dazu entschieden, einen Fokus auf die Produktkette, vor allen Dingen der Router zu legen. Hierbei handele es sich um ein Produkt, welches in jedem Haushalt teilweise mehrfach vertreten sei, und welches Millionen von Anfragen pro Sekunde verarbeiten könne. Deshalb sei ein verstärktes Augenmerk auf das Thema Router von nicht sicheren Herstellern zu richten. Die Entschließung sehe vor, die Bundesregierung bei den Verhandlungen für den Cyber Security Act 2 zu unterstützen. Hier werde es explizit um die Frage gehen, wie mit chinesischen Hardwarekomponenten in sicherheitsrelevanten Infrastrukturen umzugehen sei.

Die **Fraktion BÜNDNIS 90/DIE GRÜNEN** begrüßt den Gesetzesentwurf zur Umsetzung und Durchführung des Cyber Resilience Acts, um ein einheitliches Niveau von Cybersicherheit in Europa zu schaffen, insbesondere für Produkte mit digitalen Elementen. Damit werde zugleich die Grundlage geschaffen, dass das BSI die Aufgaben nach der Cyberresilienz-Verordnung wahrnehmen könne. Wichtig sei auch, dass die Aufgaben beim BSI als Marktüberwachungsbehörde, notifizierende Behörde und Meldestelle gebündelt würden, um die Fachkompetenz zusammenzuführen. Die vorgesehene Unterstützung kleiner und mittlerer Unternehmen sei von besonderer Bedeutung, denn mit der Verordnung gehe ein großer Aufwand für die Wirtschaft einher. Positiv hervorzuheben sei

Vorabfassung – wird durch die lektorierte Fassung ersetzt.

zudem das Reallabor für Cyberresilienz, in dem Hersteller die Möglichkeiten erhielten, neue Produkte zu testen. Sie äußert Kritik an der fehlenden Möglichkeit zur Verhängung von Bußgeldern gegen öffentliche Stellen, dies sei nur gegen die Privatwirtschaft möglich. Auch komme die Verordnung insgesamt zu spät. Sie vertritt die Auffassung, dass zusammen mit der NIS-2-Richtlinie wichtige Möglichkeiten geschaffen würden, um die Cybersicherheit insgesamt zu stärken. Hinsichtlich der Entschließung erklärt sie, sich enthalten zu wollen. Sie begrüße zwar einige Punkte der Entschließung, insbesondere zu den Risiken durch Abhängigkeiten von nicht vertrauenswürdigen Herstellern, diese bleibe jedoch insgesamt zu vage. Es fehlten insbesondere Aussagen zur substanziellen Stärkung des BSI, indem man es zur Zentralstelle ausbaute und zu einem gesetzlich verankerten Schwachstellenmanagement. Dem Gesetzesentwurf und auch dem Änderungsantrag sei zuzustimmen.

Die **Fraktion Die Linke** weist darauf hin, dass der Gesetzesentwurf darauf abziele, die Aufgaben der Marktaufsicht, der Notifizierung, der Unterstützung von kleinen und mittelständischen Unternehmen zur Stärkung ihrer Cyber-Resilienz und der Beschwerdestelle für Bürgerinnen und Bürger auf das Bundesamt für Sicherheit in der Informationstechnik zu übertragen, um eine Zersplitterung auf zahlreiche Landesbehörden zu vermeiden. Dies erachtet sie für sachgerecht, befürchtet jedoch durch die Bündelung aller Aufgaben die Entstehung von Rollenkonflikten für das BSI. Das BSI nehme die Produktprüfung nicht selbst vor, sondern sei lediglich Notifizierungsstelle für die Unternehmen, welche die Cyber-Resilienz-Act-Konformität von IT-Produkten prüften und zertifizierten. Allerdings könne eine Konformitätsbewertungsstelle auch ohne formale Akkreditierung zugelassen werden, wenn dies im sogenannten öffentlichen Interesse liege. Damit sei zu befürchten, dass Unternehmen aufgrund eines Mangels an Konformitätsbewertungsstellen ohne ausreichende fachliche Prüfung zugelassen würden. Sie äußert vor diesem Hintergrund Bedenken an der effizienten Umsetzung der Cyber-Resilienz-Act-Verordnung, die aufgrund der geringen personellen Ausstattung des BSI für die Umsetzung des Gesetzes noch verstärkt würden. Der Entschließungsantrag betone zu Recht die Relevanz von sicheren und europäischen Lieferketten zur Stärkung der Resilienz der Informations- und Kommunikationstechnik und des Energiesektors gegen digitale Angriffe. Allerdings gebe er der Bundesregierung keinerlei Maßgaben zur operativen Umsetzung dieser Forderung. Sie vertritt die Auffassung, die Entschließung zielen vielmehr darauf ab, chinesische Hersteller als generell unzuverlässig einzustufen und infolgedessen vom deutschen Markt auszuschließen. Dies reduziere jedoch allenfalls den Kreis der Informationstechnik-Anbieter, zu denen eine Abhängigkeit bestehe.

Berlin, den 14. Oktober 2026

**Marc Henrichmann**  
Berichtersteller

**Steffen Janich**  
Berichtersteller

**Johannes Schätzl**  
Berichtersteller

**Jeanne Dillschneider**  
Berichterstellerin

**Jan Krampe**  
Berichtersteller

Vorabfassung – wird durch die lektorierte Fassung ersetzt.