



Stellungnahme

des Deutschen Anwaltvereins durch den Ausschuss Informationsrecht

zur Öffentlichen Konsultation der Europäischen Kommission zu einem Gesetz über Cyberresilienz - neue Cybersicherheitsvorschriften für digitale Produkte und Nebendienstleistungen

Stellungnahme Nr.: 29/2022

Brüssel, im Mai 2022

Mitglieder des Ausschusses

- Rechtsanwalt Dr. Helmut Redeker, Bonn (Vorsitzender)
- Rechtsanwalt Dr. Simon Assion, Frankfurt am Main
- Rechtsanwältin Dr. Christiane Bierehoven, Düsseldorf
- Rechtsanwältin Isabell Conrad, München
- Rechtsanwalt Dr. Malte Grützmaker, LL.M., Hamburg
- Rechtsanwalt Prof. Niko Härting, Berlin
- Rechtsanwalt Peter Huppertz, LL.M, Düsseldorf
- Rechtsanwältin Birgit Roth-Neuschild, Karlsruhe
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München
(Berichterstatter)

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwältin Nicole Narewski

Ansprechpartnerin in Brüssel:

- Hannah Adzakpa, LL.M.

Deutscher Anwaltverein

Littenstraße 11, 10179 Berlin

Tel.: +49 30 726152-0

Fax: +49 30 726152-190

E-Mail: dav@anwaltverein.de

Büro Brüssel

Rue Joseph II 40, Boîte 7B

1000 Brüssel, Belgien

Tel.: +32 2 28028-12

Fax: +32 2 28028-13

E-Mail: bruessel@eu.anwaltverein.de

EU-Transparenz-Registernummer:

87980341522-66

www.anwaltverein.de

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV versammelt mehr als 61.000 Rechtsanwältinnen und Rechtsanwälte sowie Anwaltsnotarinnen und Anwaltsnotare, die in 253 lokalen Anwaltvereinen im In- und Ausland organisiert sind. Er vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene. Der DAV ist im Lobbyregister für die Interessenvertretung gegenüber dem Deutschen Bundestag und der Bundesregierung zur Registernummer R000952 eingetragen.

Die folgenden Fragen wurden im Rahmen der Öffentlichen Konsultation beantwortet:

FRAGE 9: Inwieweit können Ihrer Meinung nach die folgenden Maßnahmen dazu beitragen, die Cybersicherheit digitaler Produkte, die in der Union auf den Markt gebracht werden, zu erhöhen (auf einer Skala von 1 bis 5, wobei 5 bedeutet, dass eine Maßnahme sehr wirksam wäre)?

	1	2	3	4	5	Weiß nicht /keine Meinung
Leitlinien oder Empfehlungen für die Entwicklung sicherer digitaler Produkte auf EU-Ebene, die sich an Hersteller richten	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Weiteres freiwilliges europäisches Programm für die Cybersicherheitszertifizierung digitaler Produkte und Services	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
EU-Leitlinien für die öffentliche Auftragsvergabe unter Berücksichtigung der Cybersicherheitsanforderungen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Änderung bestehender Rechtsvorschriften zur Regelung bestimmter Produkte mit digitalem Bezug (z. B. die Rechtsvorschriften für Aufzüge oder Gasverbrauchseinrichtungen)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Einführung verbindlicher horizontaler Cybersicherheitsanforderungen für Hardwareprodukte	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Einführung verbindlicher horizontaler Cybersicherheitsanforderungen für Softwareprodukte	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Bitte erläutern Sie Ihre Antwort.

höchstens 1000 Zeichen

Bloße Leitlinien (Punkt 1), die keinen rechtlich verbindlichen Charakter haben, werden erfahrungsgemäß nur wenig Wirkung zeigen, v.a. wenn sie mit (Entwicklungs-/ Umsetzung-/Kosten-) Aufwand verbunden sind. Gleiches gilt für Punkt 2 – ein nur freiwilliges Programm.

Dagegen haben Vorgaben mit rechtsverbindlichem Charakter naturgemäß deutlich höhere Wirkung, v.a. in Verbindung mit Sanktionsnormen, seien es denkbare zivilrechtliche Folgen (Schadensersatz o.Ä.) oder öffentlich-rechtliche Sanktion wie im deutschen Recht Bußgeldvorschriften nach dem Ordnungswidrigkeitengesetz („administrative fines“).

Die höchste Wirkung werden gesetzliche Normen entfalten, v.a., wenn sie spezifisch bestimmte Vorgaben enthalten (Punkt 4). Vorgaben, die bei einer öffentlichen Auftragsvergabe zwingend zu berücksichtigen sind, werden ebenfalls als wirksam angesehen.

FRAGE 10: Wie würden Sie die Auswirkungen der folgenden Maßnahmen auf das Niveau der Cybersicherheit digitaler Produkte und der Verbraucherinnen und Verbraucher/Organisationen bewerten, die solche Produkte nutzen (auf einer Skala von 1 bis 5, wobei 5 bedeutet, dass eine Maßnahme eine sehr große Auswirkung haben würde)?

	1	2	3	4	5	Weiß nicht /keine Meinung
Verpflichtung der Anbieter, Informationen und Anleitungen für die sichere Installation, den Betrieb und die Verwendung des betreffenden Produkts zur Verfügung zu stellen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Verpflichtung der Anbieter, entsprechende Korrekturmaßnahmen zu ergreifen (z. B. Patches, Rückruf oder Rücknahme eines Produkts), wenn sich herausstellt, dass ein Produkt nicht sicher ist	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

FRAGE 13: Inwieweit stimmen Sie den folgenden Aussagen darüber zu, wie die Cybersicherheit in den bestehenden EU-Rechtsvorschriften behandelt wird (z. B. in der [Richtlinie über die allgemeine Produktsicherheit](#) und der [Maschinenrichtlinie](#), die beide derzeit überarbeitet werden, sowie in der [Delegierten Verordnung vom 29. Oktober 2021 zur Funkanlagenrichtlinie](#)) (auf einer Skala von 1 bis 5, wobei 5 bedeutet, dass Sie der Aussage voll zustimmen)?

	1	2	3	4	5	Weiß nicht /keine Meinung

In den geltenden EU-Verordnungen wird die Cybersicherheit von materiellen digitalen Produkten (Hardware) während ihres gesamten Lebenszyklus angemessen berücksichtigt.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
In den geltenden EU-Verordnungen wird die Cybersicherheit von immateriellen digitalen Produkten (Software) während ihres gesamten Lebenszyklus angemessen berücksichtigt.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
In den geltenden EU-Verordnungen werden alle relevanten Cybersicherheitsrisiken (materielle und immaterielle Schäden) im Zusammenhang mit der Nutzung oder dem Missbrauch eines digitalen Produkts angemessen berücksichtigt.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

FRAGE 14: Wenn es auf europäischer Ebene keine horizontalen Cybersicherheitsanforderungen gibt, könnten die Mitgliedstaaten nationale Gesetze erlassen, um den Anbietern bestimmte Anforderungen aufzuerlegen. Inwieweit stimmen Sie zu, dass ohne eine EU-Initiative das Risiko steigender Kosten und Rechtsunsicherheit für die Marktteilnehmer besteht (auf einer Skala von 1 bis 5, wobei 5 bedeutet, dass Sie der Aussage voll zustimmen)?

- 1
- 2
- 3
- 4
- 5
- Weiß nicht/keine Meinung

Bitte erläutern Sie Ihre Antwort.

höchstens 1000 Zeichen

Die Erfahrung zeigt, dass selbst bei EU-Verordnungen dort, wo ausnahmsweise nationaler Spielraum besteht (wie im Rahmen der Öffnungsklauseln etwa bei der DSGVO) es trotz des klaren vollharmonisierenden Charakters aufgrund nationaler Alleingänge zu einem Auseinanderfallen kommt. Dies gilt – so zeigt die Vergangenheit – erst recht bei Richtlinien. Soweit es überhaupt keine europarechtlichen verbindlichen Vorgaben gäbe, ist nicht davon auszugehen, dass die Mitgliedstaaten zu einem auch nur ansatzweise harmonisierten Ansatz kommen.

FRAGE 16: Sollten Hardwarehersteller und Softwareentwickler für den gesamten Lebenszyklus eines digitalen Produkts verantwortlich sein (z. B. indem sie verpflichtet werden, Updates bereitzustellen)?

- Ja
- Nein
- Weiß nicht/keine Meinung

FRAGE 16a: Wenn Sie der Meinung sind, dass Hardwarehersteller und Softwareentwickler verpflichtet werden sollten, Sicherheitsupdates zur Verfügung zu stellen, für wie viele Jahre sollten sie dazu verpflichtet werden?

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- Weiß nicht/keine Meinung
- Sonstige (bitte unten angeben)

Bitte erläutern Sie Ihre Antwort.

höchstens 1000 Zeichen

Zu Frage 16: Nur die Hersteller sind typischerweise in der Lage, ausreichend Einfluss auf deren Produkte zu nehmen und diese up-to-date zu halten, Dritten ist dies nicht oder nur begrenzt möglich. Daher kommen nur die Hersteller in Frage.

Zwingend muss aber die Frage der Vergütung geklärt werden, also zu welcher Vergütung die Herstellung diese Pflicht tragen sollen.

Ferner wäre zu klären, was genau mit „Lebenszyklus“ gemeint ist, eine Definition ist essentiell, da von ihr die Dauer der Pflicht abhängt.

Zu Frage 16a: 3 bis 5 Jahre. Auch bei hoch innovativen Produkten ist eine Produktlebenszeit von 3 Jahren realistisch, auch im Sinne der Nachhaltigkeit. Zugleich ist eine Zeit von länger als 5 Jahren meist technisch nicht realistisch, zu sehr hat sich dann das technische Umfeld geändert.

FRAGE 18: Im Rahmen dieser Initiative müssten Hardwarehersteller und Softwareentwickler nachweisen, dass sie die Anforderungen an die Cybersicherheit erfüllen. Sollten digitale Produkte mit einem höheren Risiko einem strengeren Verfahren zum Nachweis der Konformität mit diesen Anforderungen unterliegen?

- Ja
- Nein
- Weiß nicht/keine Meinung

FRAGE 18a: Die Art und Weise, wie Hardwarehersteller und Softwareentwickler ihre Konformität mit den Cybersicherheitsanforderungen nachweisen müssen, könnte von dem mit einem bestimmten Produkt verbundenen Risiko abhängig gemacht werden. Welche Risikokategorien sollten bei einer solchen risikobasierten Methodik berücksichtigt werden? *(Mehrfachantworten sind möglich.)*

- Der Funktionsumfang eines Produkts (z. B. ob es eine Netzwerkschnittstelle hat oder nicht, oder ob es bestimmte Sicherheitsfunktionen eines digitalen Systems steuert)
- Die gesellschaftliche Bedeutung eines Produkts (z. B. gemessen am Marktanteil oder der Anzahl der Nutzer)
- Die beabsichtigte Verwendung eines Produkts (z. B. für die Erbringung von Dienstleistungen im Gesundheitswesen, als industrielles Steuerungssystem oder in einem Sicherheitskontext)
- Das mit einem Produkt verbundene Sicherheitsrisiko
- Sonstige (bitte unten angeben)
- Weiß nicht/keine Meinung

Bitte erläutern Sie Ihre Antwort.

höchstens 1000 Zeichen

Man benötigt hier möglichst objektive Kriterien, was beim Funktionsumfang sowie dem Sicherheitsrisiko der Fall ist bzw. zumindest im Verhältnis zu den anderen genannten Varianten. Zugleich bestimmt wesentlich der Funktionsumfang den Einsatzbereich und damit wiederum mögliche Risiken – der Punkt „verbundenes Sicherheitsrisiko“ ist im Ergebnisse eine Folge davon.

FRAGE 18b: Wer sollte das mit einem Produkt verbundene Risiko und folglich seine Risikokategorisierung festlegen? *(Mehrfachantworten sind möglich.)*

- Der Hersteller
-

- Eine zuständige Behörde
- Eine unabhängige Stelle, die für die Überprüfung der Erfüllung der Cybersicherheitsanforderungen zuständig ist
- Rechtsvorschriften
- Sonstige (bitte unten angeben)
- Weiß nicht/keine Meinung

Bitte erläutern Sie Ihre Antwort.

höchstens 1000 Zeichen

Das Risiko hängt v.a. auch vom Einsatz und den genutzten Funktionen ab. Der Hersteller ist einerseits zu subjektiv und verfolgt eigene Interessen, kann aber auch den Einzelfall nicht bewerten. Eine Behörde ist zwar neutral(er), kennt aber den Einzelfall ebenfalls nicht – gleiches gilt für eine unabhängige Stelle. Gute Erfahrungen wurden die letzten Jahre mit den Regelungsmechaniken in der DSGVO zu Risikothemen gemacht (Datenschutzfolgenabschätzung in Art. 35 DSGVO, die Regelungen des Art. 25 und 32 DSGVO), man könnte also an ähnlich gesetzliche Mechaniken auch hier denken – ggfls. dann überprüft von einer Behörde im Sinne einer Aufsicht.

FRAGE 19: Wie beurteilen Sie die folgende Aussage zur Selbsterklärung als Möglichkeit für Hardwarehersteller und Softwareentwickler, die Erfüllung der Sicherheitsanforderungen nachzuweisen (auf einer Skala von 1 bis 5, wobei 5 bedeutet, dass Sie voll zustimmen)?

	1	2	3	4	5	Weiß nicht /keine Meinung
Eine Selbsterklärung der Konformität durch einen Hardwarehersteller oder Softwareentwickler gibt ein ausreichendes Vertrauen, dass die Sicherheitsanforderungen erfüllt werden.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>