

# Evaluierung der Cybersicherheitsstrategie

Die derzeit geltende "Cybersicherheitsstrategie für Deutschland 2021" wurde am 8. September 2021 vom Bundeskabinett beschlossen und veröffentlicht. Sie bildet den strategischen Rahmen für das Handeln der Bundesregierung im Bereich der Cybersicherheit und ist wichtigstes Instrument zur Festlegung und Umsetzung von Maßnahmen zur Cybersicherheit. Nach spätestens vier Jahren ist vorgesehen, dass eine Evaluierung erfolgen soll (s. [Ziffer 9.4 der Cybersicherheitsstrategie](#)). Das Dienstleistungszentrum der Bundesregierung für Bessere Rechtsetzung im Statistischen Bundesamt unterstützt das BMI bei der Durchführung dieser Evaluierung.

Unter Zuhilfenahme von verschiedenen Fragebögen, welche die unterschiedlichen Akteure (Bundesressorts, Länder, Wirtschaft, Wissenschaft und Zivilgesellschaft) adressieren, sollen die Maßnahmen der Strategie nun evaluiert werden.

Im Nachfolgenden finden Sie den für Sie relevanten Fragebogen.  
Wir danken Ihnen für Ihre Teilnahme und aktive Unterstützung bei der Evaluierung!

## Ausfüllhinweise

Die nachstehend von Ihnen zu bewertenden Aussagen beziehen sich alle auf die in der Cybersicherheitsstrategie 2021 angelegten Kriterien zur Überprüfung der Zielerreichung (vgl. dort [Ziffer 8.1.1 bis Ziffer 8.4.7](#)). Es wurden dabei jedoch nur jene Kriterien ausgewählt, die für Sie einschlägig sind. Auf jeder Seite ist die entsprechende Fundstelle des Ziels in der Cybersicherheitsstrategie verlinkt.

Bitte geben Sie zu jeder der Aussagen den Grad Ihrer Zustimmung auf der vorgegebenen mehrstufigen Antwortskala (von „trifft zu“ bis „trifft nicht zu“) an. Sollten Sie eine Frage nicht beantworten können, wählen Sie bitte „Kann ich nicht bewerten“. Bitte beachten Sie, dass zu jeder Aussage eine der vorgegebenen Bewertungen ausgewählt werden muss, um zur nächsten Aussage zu gelangen. Ergänzend haben Sie jeweils die Möglichkeit, Kommentare abzugeben, etwa um die Gründe Ihrer Zustimmung/Ablehnung näher zu erläutern.

Sie müssen nicht alle Aussagen in einem Durchgang bewerten. Vielmehr können Sie jeweils am Ende jeder Seite auf „Beantwortung später fortsetzen“ klicken. In diesem Falle speichern Sie den dann angegebenen Link bitte ab, um die Beantwortung zu einem späteren Zeitpunkt fortzusetzen.

Bitte füllen Sie den Fragebogen bis zum Ende aus, damit Ihre Antworten verwendet und ausgewertet werden. Mit einem Klick auf den Button „Beenden“ auf der letzten Seite der Befragung schließen Sie diese ab. Eine Änderung Ihrer Antworten ist dann nicht mehr möglich. Nach dem Beenden der Befragung haben Sie die Möglichkeit, Ihre Antworten auszudrucken oder als PDF zu speichern.

Ihre Antworten werden nach den gesetzlichen Bestimmungen des Datenschut-

zes ausschließlich für den o. g. Zweck verarbeitet. Sie werden streng vertraulich behandelt und in anonymisierter Form ausgewertet, so dass Rückschlüsse auf Ihre Angaben nicht möglich sind. Weitere Datenschutzhinweise finden Sie [hier](#)



Kontakt:

- inhaltliche Fragen: [CI1@bmi.bund.de](mailto:CI1@bmi.bund.de)
- technische Fragen: [evaluierung@destatis.de](mailto:evaluierung@destatis.de)

## Staatliche Angebote

### [Ziel 8.1.3:](#)

Staatliche Angebote des digitalen Verbraucherschutzes ausbauen

# Inwieweit stimmen Sie den folgenden Aussagen zu?\*

Bitte wählen Sie pro Aussage eine Option aus. Sollten Sie die Aussage nicht bewerten können, wählen Sie "Kann ich nicht bewerten" aus.

	Trifft zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft nicht zu	Kann ich nicht bewerten
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat für die grundsätzliche Beratung, Erfassung, Koordinierung, Beantwortung und Dokumentation von Anfragen der Zielgruppen Staat, Wirtschaft und Gesellschaft ein zentrales Service-Center eingerichtet (Multichannel First-Level-Support).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

## Haben Sie noch weitere Anmerkungen zu diesem Thema?

Die deutsche Industrie schätzt die vertrauensvolle und enge Zusammenarbeit mit dem BSI grundsätzlich sehr. Das BSI verfügt über sehr engagierte Mitarbeitende. Allerdings fehlt es weiterhin an einer zentralen Anlaufstelle für Unternehmen sowie an einem einheitlichen Vorfallsmeldewesen inkl. Rückkanal in die Wirtschaft. Das BSI sollte hierfür die notwendigen Ressourcen erhalten / diese Aufgaben priorisieren.

---

## Sichere Identitäten

### Ziel 8.1.5:

Sichere elektronische Identitäten gewährleisten.

## Inwieweit stimmen Sie den folgenden Aussagen zu?\*

Bitte wählen Sie pro Aussage eine Option aus. Sollten Sie die Aussage nicht bewerten können, wählen Sie "Kann ich nicht bewerten" aus.

	Trifft zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft nicht zu	Kann ich nicht bewerten
Ein Identitätsökosystem mit der Wirtschaft wurde pilotiert.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

## Haben Sie noch weitere Anmerkungen zu diesem Thema?

Digitale Identitäten wirken als Vertrauensanker in einer zunehmend digitalisierten Gesellschaft. Der Aufbau eines echten Ökosystems digitaler Identitäten ist damit ein wichtiger Hebel, um digitale Prozesse sicher und leistungsfähig zu implementieren.

---



## Verantwortungsvoller Umgang

### Ziel 8.1.8:

Verantwortungsvoller Umgang mit Schwachstellen – Coordinated Vulnerability Disclosure fördern.

## Inwieweit stimmen Sie den folgenden Aussagen zu?\*

Bitte wählen Sie pro Aussage eine Option aus. Sollten Sie die Aussage nicht bewerten können, wählen Sie "Kann ich nicht bewerten" aus.

	Trifft zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft nicht zu	Kann ich nicht bewerten
Anreizstrukturen für Hersteller und Dienstleister, gemeldete Lücken in einem angemessenen Zeitraum zu schließen, wurden gestärkt.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

## Haben Sie noch weitere Anmerkungen zu diesem Thema?

Der CRA wird viele Hersteller dazu verpflichtet, Schwachstellen in Produkten in einem angemessenen Zeitraum zu schließen. Dies muss auch eine Harmonisierung mit anderen entweder bestehenden (z.B. CSA) oder in Kürze ebenfalls in Kraft tretenden Gesetze (z.B. NIS2UmzuCG) beinhalten, da es ansonsten zu Doppelarbeit und Überlappungen unweigerlich kommt. Die Bundesregierung sollte sich für eine praxisnahe Implementierung der CRA-Anforderungen einsetzen.

---

# Verschlüsselung

## [Ziel 8.1.9:](#)

Verschlüsselung als Voraussetzung eines souveränen und selbstbestimmten Handelns flächendeckend einsetzen.

## Inwieweit stimmen Sie den folgenden Aussagen zu?\*

Bitte wählen Sie pro Aussage eine Option aus. Sollten Sie die Aussage nicht bewerten können, wählen Sie "Kann ich nicht bewerten" aus.

	Trifft zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft nicht zu	Kann ich nicht bewerten
Es wurden Initiativen zur Förderung von Verschlüsselung in Wissenschaft, Wirtschaft, Gesellschaft sowie in internationale Gremien, die diesen Zweck verfolgen, eingebracht.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Haben Sie noch weitere Anmerkungen zu diesem Thema?

---

# Koordinierungsfunktion

## [Ziel 8.2.1:](#)

Den Nationalen Cyber-Sicherheitsrat (NCSR) in seiner Koordinierungsfunktion für die Cybersicherheitslandschaft stärken.

## Inwiefern stimmen Sie den folgenden Aussagen zu?\*

Bitte wählen Sie pro Aussage eine Option aus. Sollten Sie die Aussage nicht bewerten können, wählen Sie "Kann ich nicht bewerten" aus.

	Trifft zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft nicht zu	Kann ich nicht bewerten
Das in der Bundesregierung und mit NCSR abgestimmte Konzeptpapier zeigt Maßnahmen auf, mit denen ein zielorientierter Beratungsprozess der Bundesregierung durch den NCSR ermöglicht wird.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

## Haben Sie noch weitere Anmerkungen zu diesem Thema?

Der NCSR kommt seiner Koordinierungsfunktion in großen teilen nicht da. In Gesetzgebungsverfahren sollte er stärker als Forum des zielgerichteten Austauschs zwischen Bund, Ländern und der Wirtschaft dienen, um ein gegenseitiges Verständnis für die jeweiligen Positionen herbeizuführen und idealerweise ein gemeinsames Verständnis der Position Deutschlands in EU-Gesetzgebungsverfahren zu befördern. National sollte er die Umsetzung der Nationalen Cyber-Sicherheitsstrategie monitoren.

---

## Zusammenarbeit

### [Ziel 8.2.2:](#)

Die Zusammenarbeit von Staat, Wirtschaft, Wissenschaft und Zivilgesellschaft im Bereich der Cybersicherheit verbessern.

# Inwieweit stimmen Sie den folgenden Aussagen zu?\*

Bitte wählen Sie pro Aussage eine Option aus. Sollten Sie die Aussage nicht bewerten können, wählen Sie "Kann ich nicht bewerten" aus.

	Trifft zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft nicht zu	Kann ich nicht bewerten
Die Anzahl der Mitgliedschaften in der Allianz für Cybersicherheit ist gestiegen.	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Staatliche Unterstützungsangebote, unter anderem in Form verschiedener Kooperationsmodelle sowie über Social Media und Newsletter, sind erweitert und die Anzahl der Nutzerinnen und Nutzer der Angebote ist gestiegen.	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Diese Unterstützungsangebote werden in meinem Kreis im Vergleich zu vor 2021 vermehrt genutzt bzw. zu Rate gezogen.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Anteil großer Schadprogrammwellen, die mittels technischer Sensoren entdeckt werden, ist im Vergleich zu vor 2021 gestiegen.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Die Anzahl der Angebote der Initiative Wirtschaftsschutz für Unternehmen,	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>



Forschungseinrichtungen und Kommunen ist im Vergleich zu vor 2021 gestiegen.

Das Mittelstand-Digital-Netzwerk des BMWi ist bekannt und seine Angebote zur IT-Sicherheit werden von der Wirtschaft und insbesondere von kleinen und mittleren Unternehmen (KMU) genutzt.

<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Haben Sie noch weitere Anmerkungen zu diesem Thema?

---

# Kooperationsplattform

## [Ziel 8.2.3:](#)

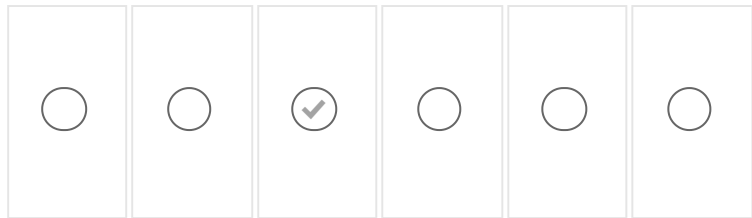
Eine kooperative Kommunikationsplattform zu Cyberangriffen zwischen Staat, Wirtschaft, Wissenschaft und Gesellschaft aufbauen.

# Inwieweit stimmen Sie den folgenden Aussagen zu?\*

Bitte wählen Sie pro Aussage eine Option aus. Sollten Sie die Aussage nicht bewerten können, wählen Sie "Kann ich nicht bewerten" aus.

	Trifft zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft nicht zu	Kann ich nicht bewerten
Die neue kooperative Plattform „Information Sharing Portal“ für den freiwilligen Austausch von Informationen zu Cyberangriffen ist mir bekannt.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich habe die neue kooperative Plattform „Information Sharing Portal“ bereits genutzt.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Anreize für die Teilnahme am Informationsaustausch und für das Teilen von Informationen wurden im Vergleich zu vor 2021 gestärkt.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Die Anzahl der zwischen den betroffenen Organisationen ausgetauschten allgemeinen Informationen und technischen Merkmalen zu Cyberangriffen hat zugenommen.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Der Schutz vor Schäden durch Cyberangriffe wurde im Vergleich zur vor 2021 deutlich verbessert.



## Haben Sie noch weitere Anmerkungen zu diesem Thema?

Die deutsche Industrie erachtet die Etablierung des Information Sharing Portals als wichtigen Schritt, damit aus den beim BSI vorliegenden Informationen zu aktuellen Cyber-Angriffsvektoren sowie Schwachstellen ein tagesaktuelles Lagebild entstehen kann. Die neuerliche Verzögerung des Go-ing-lives des Portals sehen wir sehr kritisch. BMI und BSI sollten rasch sicherstellen, dass alle unter die NIS-2-Richtlinie fallenden Einrichtungen ab In-Kraft-Treten des NIS2UmsuCG das Portal nutzen können. Ein verlässlicher Zeitplan sollte kommuniziert werden.

---

# Unternehmen schützen

## [Ziel 8.2.4:](#)

Unternehmen in Deutschland schützen.

# Inwieweit stimmen Sie den folgenden Aussagen zu?\*

Bitte wählen Sie pro Aussage eine Option aus. Sollten Sie die Aussage nicht bewerten können, wählen Sie "Kann ich nicht bewerten" aus.

	Trifft zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft nicht zu	Kann ich nicht bewerten
Die Angebote der Mittelstand-Digital-Zentren werden durch die Wirtschaft angenommen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Die Transferstelle IT-Sicherheit im Mittelstand (TISiM) ist insbesondere bei KMU und Handwerk bekannt.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Die Angebote der TISiM werden nachgefragt.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Förderprogramme, die auch auf Unterstützung der IT-Sicherheit von KMU, einschließlich Handwerk und freie Berufe, abzielen (insbesondere „go-digital“ und „Digital Jetzt“), sind bekannt.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Förderprogramme, die auch auf Unterstützung der IT-Sicherheit von KMU, einschließlich Handwerk und freie Berufe, abzielen (insbesondere „go-digital“ und „Digital Jetzt“), werden nachgefragt.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Die Anzahl der Mitglieder in der Allianz für Cybersicherheit ist gestiegen.



Die Anzahl der Angebote der Allianz für Cybersicherheit ist gestiegen.



Die Anzahl der Nutzenden der Unterstützungsangebote des BSI bei mir/ uns ist nachweislich im Vergleich zu vor 2021 gestiegen.



Die Umsetzung empfohlener Cybersicherheitsvorkehrungen ist im Vergleich zu vor 2021 gestiegen.



Der prozentuale Anteil betroffener Unternehmen, die nach BSI-Warnungen reagiert und ihre Sicherheitslücken geschlossen haben, ist im Vergleich zu vor 2021 gestiegen.



Die „Initiative Wirtschaftsschutz“ hat Projekte zum ganzheitlichen Schutz der Wertschöpfungskette vor Know-how- und Informationsabfluss etabliert.



Haben Sie noch weitere Anmerkungen zu diesem Thema?

Programme wie „TISiM“ und „go-digital“ sind etabliert, aber nicht flächendeckend bekannt oder genutzt.

---



# Digitale Wirtschaft

## [Ziel 8.2.5:](#)

Die deutsche digitale Wirtschaft stärken.

# Inwieweit stimmen Sie den folgenden Aussagen zu?\*

Bitte wählen Sie pro Aussage eine Option aus. Sollten Sie die Aussage nicht bewerten können, wählen Sie "Kann ich nicht bewerten" aus.

	Trifft zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft nicht zu	Kann ich nicht bewerten
Die Datenübertragung von und zu Mobilitätsdatenräumen sowie autonome Fahrfunktionen wurden abgesichert.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Die Resistenz gegen Angriffe auf die Sensorik von Fahrzeugen wurde gesteigert und entsprechende Technische Richtlinien wurden veröffentlicht.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Die (Typ-)Genehmigung und Marktbeobachtung von Kraftfahrzeugen und Kraftfahrzeugteilen zur Gewährleistung der Cybersicherheit wurde vom BSI in Zusammenarbeit mit dem Kraftfahrtbundesamt gestaltet.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Die Smart-Metering-PKI, eine zentrale Infrastrukturkomponente für die Digitalisierung der Energiewende, wird erfolgreich und mit wachsender Nutzerzahl betrieben. Die BMWi-BSI-Roadmap zur	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Entwicklung technischer Eckpunkte für die Einsatzbereiche Smart Grid (Steuerbare Verbrauchs- und Erzeugungsanlagen), Smart Mobility (Integration der Ladesäuleninfrastruktur von Elektromobilen) und Smart beziehungsweise Sub Metering (Spartenübergreifende Verbrauchsmessung wie Strom, Gas, Wasser, Heizen beziehungsweise Wärme) wurde im Rahmen mehrerer Standardisierungsprojekte umgesetzt. Im Bereich Smart Home beziehungsweise Consumer-IoT wurden Standards, Normen, Technische Richtlinien und Prüfkriterien (zum Beispiel Prüfspezifikation Router-TR) unter anderem für die Anwendung in Verbindung mit nationalen und internationalen Labeling- und Zertifizierungsverfahren (zum Beispiel im Rahmen des Cybersecurity Act) in Zusammenarbeit mit erforderlichen Stakeholdern aus Staat, Wirtschaft und Gesellschaft entwickelt.

Die BMWi-BSI-Roadmap zur Entwicklung technischer Eckpunkte für die Einsatzbereiche Smart Grid (Steuerbare Verbrauchs- und Erzeugungsanlagen), Smart Mobility (Integration der Ladesäuleninfrastruktur von Elektromobilen) und Smart be-



ziehungsweise Sub Metering (Spartenübergreifende Verbrauchsmessung wie Strom, Gas, Wasser, Heizen beziehungsweise Wärme) wurde im Rahmen mehrerer Standardisierungsprojekte umgesetzt.

Im Bereich Smart Cities wurden bestehende kommunale IoT-Infrastrukturen analysiert, Handlungsempfehlungen für deren sicheren Aufbau und Betrieb erstellt, Technische Richtlinien und Standards für Schlüsseltechnologien und Plattformen in Kooperation mit erforderlichen Stakeholdern aus Staat, Wirtschaft und Gesellschaft erarbeitet.

Es wurden rechtliche Rahmenbedingungen für eine verbindliche Umsetzungsverpflichtung der Maßnahmen zur Verbesserung der IT-Sicherheit in kritischen Einsatzbereichen geschaffen.

Im Bereich Industrie 4.0 wurde im internationalen Rahmen ein Konzept von Vertrauensinfrastrukturen für den Aufbau digitaler Wertschöpfungsnetze abgestimmt.

Es wurden Handlungsempfehlungen (Best Practices) für KMU zur Umsetzung wichtiger Komponen-

<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

ten von Vertrauensinfrastrukturen erstellt.

Im Finanzwesen wurden die Sicherheitsanalysen von Online-Bezahlvorgängen kommuniziert und fortgeschrieben.

Die Sicherheitsanforderungen an Biometrie-Anwendungen für die Zwei-Faktor-Authentisierung wurden etabliert.

<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## Haben Sie noch weitere Anmerkungen zu diesem Thema?

In Summe wurde eher zu viel Regulierung geschaffen, was zu zu viel Bürokratie bei den Unternehmen führt. Thema Smart-Meter ist im Vergleich zu anderen europäischen Mitgliedsstaaten in Deutschland vollkommen überreguliert. So manch gut gemeintes Papier des BSI (z.B. "Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung", oder "Auditstandards mit Maturityleveln") werden von manchen Stakeholder als regulatorische Vorgabe gesehen (z.B. als Zertifizierungsgrundlage bei der Umsetzung der IT-Sicherheitsregulierung im Energiesektor).

Die Bundesregierung sollte zur Stärkung der Cyberresilienz Deutschlands die EU-Vorgaben 1:1 umsetzen und von darüber hinausgehenden Anforderungen absehen. Aktuell sehen sich Unternehmen mit widerstreitenden Anforderungen konfrontiert, die zu einem erheblichen Mehraufwand bei der Umsetzung führen.

# Europäischer Regulierungsrahmen

## [Ziel 8.2.6:](#)

Einen einheitlichen europäischen Regulierungsrahmen für Unternehmen schaffen.

# Inwieweit stimmen Sie den folgenden Aussagen zu?\*

Bitte wählen Sie pro Aussage eine Option aus. Sollten Sie die Aussage nicht bewerten können, wählen Sie "Kann ich nicht bewerten" aus.

	Trifft zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft nicht zu	Kann ich nicht bewerten
Doppelregulierungen für Unternehmen sind im Vergleich zu vor 2021 minimiert worden.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Die Anzahl der beteiligten Stakeholder und Technologiefelder im interministeriellen Ausschuss IKT-Standardisierung für die Cybersicherheit ist gestiegen.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## Haben Sie noch weitere Anmerkungen zu diesem Thema?

Im Rahmen des für das vierte Quartal angekündigten Digital Simplification Packages der EU sollte sich die Bundesregierung dringend für eine Vereinfachung der Cyberregulierung einsetzen. Überlappungsfreie Anforderungen sind essenziell, um die Umsetzbarkeit von Regulatorik zu gewährleisten und die Wettbewerbsfähigkeit der europäischen Wirtschaft zu stärken. Bürokratie durch überbordende Meldepflichten stärkt nicht die Cyberresilienz, sondern schwächt diese eher, da Unternehmen ihre personellen und finanziellen Ressourcen nicht für Prävention und Mitigation einsetzen können.

---

Die überlappende Regulierung ist im Cybersicherheitsbereich eklatant, siehe CRA und RED DA. Gleichzeitig werden unrealistische Forderungen an die beteiligten Stakeholder zur Umsetzung gestellt. Standards müssen unter hohem Zeitdruck entwickelt werden, Hersteller haben wenig bis keine ausreichende Entwicklungszeit auf Basis der Standards. Die Bundesregierung sollte sich für wirtschaftsfreundlichere Übergangsszenarien einsetzen, insbesondere bezüglich des CRA.



# Forschung und Entwicklung

## [Ziel 8.2.7:](#)

Forschung und Entwicklung resilienter, sicherer IT-Produkte, Dienstleistungen und Systeme für den EU-Binnenmarkt fördern.

# Inwieweit stimmen Sie den folgenden Aussagen zu?\*

Bitte wählen Sie pro Aussage eine Option aus. Sollten Sie die Aussage nicht bewerten können, wählen Sie "Kann ich nicht bewerten" aus.

	Trifft zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft nicht zu	Kann ich nicht bewerten
Die Anzahl an Projekten und Unternehmen in der Forschung ist gestiegen.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Umfang der Förderung des Forschungsrahmenprogramms der Bundesregierung ist gestiegen.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Innovationen aus der IT-Sicherheitsforschung werden vermehrt durch Unternehmen (inkl. Startups) umgesetzt beziehungsweise kommerzialisiert.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Haben Sie noch weitere Anmerkungen zu diesem Thema?

---

# Technologiesicherheit

## [Ziel 8.2.8:](#)

Sicherheit von Zukunfts- und Schlüsseltechnologien im Sinne eines Security-by-Design-Ansatzes stärken.

# Inwieweit stimmen Sie der folgenden Aussage zu?\*

Bitte wählen Sie pro Aussage eine Option aus. Sollten Sie die Aussage nicht bewerten können, wählen Sie "Kann ich nicht bewerten" aus.

	Trifft zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft nicht zu	Kann ich nicht bewerten
Entlang der Wertschöpfungskette vertrauenswürdiger IT-Systeme ist eine Organisations-, Qualitäts-sicherungs- und Kommunikationsinfrastruktur gegründet.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Im Rahmen des Netzwerkes zu vertrauenswürdiger IT, das die wirtschaftlichen Akteure gebildet haben, werden Projekte zu verschiedenen Technologiefeldern bearbeitet.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Haben Sie noch weitere Anmerkungen zu diesem Thema?

---

# IT-Sicherheit

## [Ziel 8.2.9:](#)

IT-Sicherheit durch Quantentechnologie gewährleisten.

# Inwieweit stimmen Sie der folgenden Aussage zu?\*

Bitte wählen Sie pro Aussage eine Option aus. Sollten Sie die Aussage nicht bewerten können, wählen Sie "Kann ich nicht bewerten" aus.

	Trifft zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft nicht zu	Kann ich nicht bewerten
Technologien und Lösungen der Quantenkommunikation von Anbietern aus Deutschland und Europa stehen für Staat, Wirtschaft und Gesellschaft zur Verfügung.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
In der Wirtschaft ist die Dringlichkeit des Wechsels zu quantensicherer Kryptografie akzeptiert und in kritischen Bereichen eingeleitet.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Pilot-Infrastrukturen binden Partner hierbei aus den verschiedenen Bereichen ein.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



# Haben Sie noch weitere Anmerkungen zu diesem Thema?

Das Wissen um die Relevanz von PQC ist stark abhängig von der Branche sowie der Größe der Unternehmen. Im Rahmen der ACS sollte eine Informationskampagne zu PQC initiiert werden.

---

# Prüf- und Abnahmeverfahren

## [Ziel 8.2.10:](#)

Prüf- und Abnahmeverfahren mit Innovationszyklen harmonisieren (Time-to-Market).

## Inwieweit stimmen Sie der folgenden Aussage zu?\*

Bitte wählen Sie pro Aussage eine Option aus. Sollten Sie die Aussage nicht bewerten können, wählen Sie "Kann ich nicht bewerten" aus.

	Trifft zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft nicht zu	Kann ich nicht bewerten
Standards, Technische Richtlinien und Prüfspezifikationen im Bereich Smart Home beziehungsweise Consumer-IoT wurden in den letzten fünf Jahren geschaffen.	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## Haben Sie noch weitere Anmerkungen zu diesem Thema?

Nationale Zertifizierungen oder Kennzeichnungsinitiativen sind für die Industrie nicht geeignet. Hier sind mindestens europäische Verfahren anzustreben. Nationale Initiativen, wie das deutsche IT-Sicherheitskennzeichen, sollten eingestellt werden und die Ressourcen zur Unterstützung europäischer Verfahren genutzt werden.

---

# Kritische Infrastruktur

## [Ziel 8.2.11:](#)

Schutz Kritischer Infrastrukturen weiter verbessern.

## Inwieweit stimmen Sie der folgenden Aussage zu?\*

Bitte wählen Sie pro Aussage eine Option aus. Sollten Sie die Aussage nicht bewerten können, wählen Sie "Kann ich nicht bewerten" aus.

	Trifft zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft nicht zu	Kann ich nicht bewerten
Die Betreiber kritischer Infrastruktur (KRITIS) können über einen nationalen Informationsaustausch zu Cyberangriffen ihre jeweilige Abwehr stärken.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## Haben Sie noch weitere Anmerkungen zu diesem Thema?

Der Informationsaustausch ist schon erheblich besser geworden. Es könnte aber noch schneller "actionabel" Informationen zur Verfügung gestellt werden (auch Informationen, die aus anderen Ländern bei den Behörden vorliegen), damit Betreiber Kritischer Infrastrukturen in Deutschland ihre eigene Betroffenheit zeitnah überprüfen und bei Bedarf Maßnahmen zum Schutz der kritischen Infrastruktur ergreifen.

---

# Cybersicherheitszertifizierung

[Ziel 8.2.12:](#)

Cybersicherheitszertifizierung

# Inwieweit stimmen Sie der folgenden Aussage zu?\*

Bitte wählen Sie pro Aussage eine Option aus. Sollten Sie die Aussage nicht bewerten können, wählen Sie "Kann ich nicht bewerten" aus.

	Trifft zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft nicht zu	Kann ich nicht bewerten
Die Anzahl zertifizierter Produkte unter der Aufsicht der Nationalen Behörde für die Cybersicherheitszertifizierung ist gestiegen.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Die Anzahl von Unternehmen und Organisationen, die IT-Grundschutz anwenden, ist gestiegen.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

# Haben Sie noch weitere Anmerkungen zu diesem Thema?

Die deutsche Industrie spricht sich gegen den zwingende Einsatz zertifizierter Produkte aus. Als zusätzliche Möglichkeit die Vertrauenswürdigkeit eines Produktes zu überprüfen, ist eine Sicherheitszertifizierung hilfreich. Die Verfahren für den Grundschatz sollten den europäischen NIS2-Anforderungen angepasst werden, sodass ein für KMU geeignetes Basislevel im Rahmen des IT-Grundschatzes zur Erfüllung der Anforderungen ermöglicht wird.

---



# Telekommunikationsinfrastrukturen

## [Ziel 8.2.13:](#)

Telekommunikationsinfrastrukturen der Zukunft sichern.

# Inwieweit stimmen Sie der folgenden Aussage zu?\*

Bitte wählen Sie pro Aussage eine Option aus. Sollten Sie die Aussage nicht bewerten können, wählen Sie "Kann ich nicht bewerten" aus.

	Trifft zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft nicht zu	Kann ich nicht bewerten
Die Verfügbarkeit der Telekommunikationsnetze und deren Widerstandsfähigkeit gegenüber Störungen und Angriffen wurde im Vergleich zu vor 2021 erhöht.	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Software und Hardware der kritischen Komponenten wird vor ihrem Einsatz einer Überprüfung unterzogen, mit der Schwachstellen erkannt und beseitigt werden.	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Deutsche und europäische Unternehmen sind in den betreffenden Standardisierungsgremien präsent und prägen maßgeblich die Standardisierung zukünftiger Telekommunikationssysteme mit einer gesteigerten Anzahl von Standardisierungsbeiträgen.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Der Anteil deutscher und europäischer Netzkompo-	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

nenten in Telekommunikationsnetzen ist gestiegen.

--	--	--	--	--	--

## Haben Sie noch weitere Anmerkungen zu diesem Thema?

Die Widerstandsfähigkeit der Telekommunikationsnetze wird nicht durch Gesetze erhöht, sondern durch die Eigeninitiative der Betreiber und Hersteller sowie derer Innovation an neuen Funktionen und Produkten. Der Einsatz vertrauenswürdiger Hersteller muss forciert werden.

Europäische Firmen tragen seit Jahren mit konstanter Anzahl von Experten und Beiträgen zur Standardisierung bei. Asiatische Firmen haben die Anzahl ihrer Experten und Beiträge in den letzten Jahren massiv gesteigert.

Vor allem in IETF und ITU besetzen asiatische Firmen inzwischen sehr viele

---

Führungspositionen und bringen sehr viele Forschungsergebnisse in die Standardisierung ein. Europäische Firmen und da vor allem auch jene, die bereits mit mehr als 20 Expertinnen und Experten in der Standardisierung aktiv sind, brauchen stärkere Unterstützung durch staatliche Einrichtungen, sei es nun durch Geld oder durch Mitarbeitende. In fast allen Standardisierungsgremien braucht es für eine Firma mindestens 10 Expertinnen / Experten, um Themen voranzubringen. Durch die Verzahnung der einzelnen Organisationen, wie zum Beispiel 3GPP mit IETF, ITU und GSMA müssen mehrere Gremien von derselben Firma bespielt werden. 20 ist da schon das Minimum, um Themen zu treiben. Auch staatliche Organisation können in der Standardisierung mit guten Expertinnen / Experten viel bewegen.

# Sicherheit durch Verschlüsselung

## [Ziel 8.3.9:](#)

Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung gewährleisten.

# Inwieweit stimmen Sie der folgenden Aussage zu?\*

Bitte wählen Sie pro Aussage eine Option aus. Sollten Sie die Aussage nicht bewerten können, wählen Sie "Kann ich nicht bewerten" aus.

	Trifft zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft nicht zu	Kann ich nicht bewerten
Technische und operative Lösungen für den rechtmäßigen Zugang zu Inhalten aus verschlüsselter Kommunikation sind in enger Abstimmung mit allen betroffenen Unternehmen, Interessensträgern und zuständigen Behörden auf europäischer Ebene entwickelt.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

# Haben Sie noch weitere Anmerkungen zu diesem Thema?

Die aktuell auf EU-Ebene diskutierten Ansätze zur Aufweichung von Ende-zu-Ende-Verschlüsselung sieht die deutsche Industrie sehr kritisch.

---

# Völkerrecht

## [Ziel 8.4.3:](#)

Völkerrecht und den normativen Rahmen für den Cyberraum stärken und auf verantwortliches Staatenverhalten hinwirken.

# Inwieweit stimmen Sie der folgenden Aussage zu?\*

Bitte wählen Sie pro Aussage eine Option aus. Sollten Sie die Aussage nicht bewerten können, wählen Sie "Kann ich nicht bewerten" aus.

	Trifft zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft nicht zu	Kann ich nicht bewerten
Die Bundesregierung beteiligt sich bilateral, multilateral und im Austausch mit der Zivilgesellschaft auf Grundlage des im März 2021 veröffentlichten Positionspapiers an Diskussionen zur Anwendbarkeit des Völkerrechts im Cyberraum sowie zur Implementierung von Selbstverpflichtungen zu verantwortlichem Staatenverhalten.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



Haben Sie noch weitere Anmerkungen zu diesem Thema?

---

## Endseite

Wir danken Ihnen herzlich für Ihre Teilnahme! Bitte klicken Sie auf "Beenden", wenn Sie mit der Bearbeitung fertig sind.

Ihre Antworten werden durch das BMI und das Statistische Bundesamt ausgewertet.

Über das Ergebnis werden wir Sie anschließend informieren.

Sie können Ihre Angaben hier drucken: 

