

Position Paper

Digitale Resilienz Teil 1 / 3

03
26

idw
trend
watch

IDW

Digitale Resilienz

Wie resilient muss und kann Deutschland sein?

Digitale Resilienz wird als zentrale Voraussetzung für Deutschlands Sicherheit, Handlungsfähigkeit und Wettbewerbsfähigkeit beschrieben. Dieses IDW Trendwatch Position Paper analysiert bestehende Fortschritte und Defizite und formuliert Handlungsempfehlungen für eine widerstandsfähige digitale Infrastruktur, Verwaltung und Wirtschaft.

Inhalt

Vorbemerkung	4
1. Einleitung: eine Ära der Resilienz und Verteidigung	5
2. Begriffserklärungen: Was ist Resilienz?	6
3. Resilienz in Deutschland stärken	7
a) Wo digitale Resilienz in Deutschland bereits entsteht und aufgebaut wird	7
b) Das kann Deutschland von anderen Ländern lernen	9
c) Darauf sollte Deutschland bei digitaler Resilienz den Fokus setzen	10
4. Fazit und Ausblick	12

Vorbemerkung

Digitale Resilienz ist eine zentrale Voraussetzung für die Sicherheit, Handlungsfähigkeit und Wettbewerbsfähigkeit Deutschlands. Angesichts zunehmender Cyberangriffe, geopolitischer Spannungen und technologischer Abhängigkeiten muss Deutschland seine Widerstandsfähigkeit gegenüber digitalen Störungen konsequent stärken.

Mit diesem Position Paper eröffnet der Ausschuss Trendwatch des IDW seine dreiteilige Reihe „Wie resilient muss und kann Deutschland sein?“. Der Auftakt widmet sich der Stärkung der digitalen Resilienz in Deutschland, da digitale Infrastrukturen heute das Fundament von Wirtschaft, Verwaltung und Gesellschaft bilden. Das Papier fasst wesentliche Erkenntnisse und Empfehlungen zusammen, um die Widerstandsfähigkeit digitaler Infrastrukturen und Systeme im Land nachhaltig zu verbessern. Es hebt die Bedeutung einer ganzheitlichen Strategie hervor, die technologische, organisatorische und gesellschaftliche Aspekte integriert, um den Schwierigkeiten der digitalen Transformation effektiv zu begegnen.

Deutschland hat mit neuen Regulierungen, einer nationalen Resilienz-Strategie und Initiativen zur digitalen Souveränität wichtige Fortschritte erzielt. Dennoch bestehen erhebliche Defizite bei der Koordination, dem Schutzniveau vieler Unternehmen und Behörden sowie bei den verfügbaren Fachkräften. Das Trendwatch Position Paper des IDW empfiehlt daher, digitale Resilienz als strategische Führungsaufgabe zu verankern, bestehende Maßnahmen konsequenter umzusetzen, Mittelstand und Verwaltung gezielt zu unterstützen, den Fachkräftemangel im Bereich Cybersicherheit zu bekämpfen und Investitionen in souveräne digitale Technologien zu stärken. Ein nationaler Chief Resilience Officer im Bundeskanzleramt könnte die hierfür erforderlichen Aktivitäten ressortübergreifend koordinieren.

KAPITEL

01

Einleitung: eine Ära der Resilienz und Verteidigung

Deutschland, seine Unternehmen und seine Bevölkerung müssen wehrhafter und resilienter werden, um sich gegen Bedrohungen und Aggressoren zu wappnen. Dies erfordert erhebliche Mittel, die an anderen Stellen fehlen könnten. Resilienz ist dabei weit mehr als eine rein militärische Frage. Sie muss gesamtstaatlich und gesamtgesellschaftlich betrachtet werden.

Der Staat trägt die Verantwortung, Menschen und Betriebe in Deutschland zu schützen und die Voraussetzungen für ein Leben in Freiheit und Sicherheit zu schaffen. Hierzu gehören insbesondere der Schutz und Ausbau kritischer Infrastrukturen sowie die Stärkung der digitalen Resilienz. Gleichzeitig sind aber auch Unternehmen und Bürgerinnen und Bürger gefordert, etwa beim verantwortungsvollen Umgang mit knappen Ressourcen und der Sicherung wichtiger Rohstoffe. Dabei müssen die Auswirkungen steigender Verteidigungsausgaben auf Wirtschaft, Gesellschaft, Wachstum und Produktivität in Deutschland mitgedacht werden. Die Erkenntnis lautet: Eine moderne und leistungsfähige Verteidigung ist ein zentraler Baustein für Deutschlands Resilienz.

Auch die Gesellschaft selbst muss resilienter werden. Dafür braucht es stärkeren gesellschaftlichen Zusammenhalt sowie gezielte Bildung

und Aufklärung. Ebenso wichtig ist politische Resilienz: Stabile Institutionen und verlässliche Entscheidungsprozesse sind dafür zentral.



Begriffserklärungen: Was ist Resilienz?

Resilienz ist vom lateinischen Wort ‚resilire‘ hergeleitet und bedeutet ‚zurückspringen‘, ‚abprallen‘. Der Begriff umschreibt die Fähigkeit eines Systems, sich gegenüber inneren oder äußeren Einflüssen so zu verhalten, dass es in der Lage ist, wieder in seinen Ursprungszustand zurückzukehren. Es geht also um die Widerstandsfähigkeit, Fehlertoleranz oder Selbstregulation eines Systems¹.

Im fachlichen Kontext, insbesondere im wirtschaftlichen und gesellschaftlichen Bereich, hat sich die Bedeutung dieses Begriffs erweitert. Er beschreibt die Fähigkeit von Organisationen, Gemeinschaften und Gesellschaften, Störungen, Krisen oder unerwartete Herausforderungen zu bewältigen, sich anzupassen und gestärkt daraus hervorzugehen².

Im wirtschaftlichen Bereich bezeichnet Resilienz die Fähigkeit von Unternehmen, Branchen oder Volkswirtschaften, externe Schocks wie Finanzkrisen, Marktveränderungen, technologische Umbrüche oder globale Ereignisse abzufedern und funktionsfähig zu bleiben. Wirtschaftliche Resilienz ist entscheidend für die Stabilität und das nachhaltige Wachstum einer Volkswirtschaft. Dazu gehören Diversifikation, eine flexible Produktion, robuste Lieferketten, finanzielle Stabilität und Innovationsfähigkeit.

Unternehmen, die resilient sind, zeichnen sich durch eine proaktive Risikomanagementstrategie aus, die es ihnen ermöglicht, auf Veränderungen schnell zu reagieren. Zudem spielt die Fähigkeit zur Innovation eine zentrale Rolle, um sich an neue Marktbedingungen anzupassen. Die Förderung wirtschaftlicher Resilienz ist eine zentrale Aufgabe der Wirtschaftspolitik, um die Wettbewerbsfähigkeit und die soziale Stabilität zu sichern³.

Gesellschaftliche Resilienz beschreibt die Fähigkeit einer Gemeinschaft oder Gesellschaft, soziale, kulturelle und ökologische Probleme zu bewältigen. Dazu gehören Naturkatastrophen, soziale Konflikte, demografische Veränderungen oder gesundheitliche Krisen. Eine resiliente Gesellschaft ist in der Lage, Krisen zu antizipieren, angemessen zu reagieren und sich nach der Krise zu erholen, ohne dauerhaft geschwächt zu werden⁴.

Mehr gesellschaftliche Resilienz lässt sich erreichen, indem man soziale Netzwerke ausbaut, Gemeinschaftsstrukturen stärkt, die Infrastruktur verbessert, Bildung fördert und nachhaltige Umweltstrategien entwickelt. Besonders in Zeiten globaler Krisen wie der Covid-19-Pandemie hat die Bedeutung gesellschaftlicher Resilienz

deutlich zugenommen, da sie die Grundlage für eine stabile und widerstandsfähige Gesellschaft bildet⁵. Im wirtschaftlichen wie gesellschaftlichen Kontext gewinnt digitale Resilienz an Bedeutung. Bei dieser Ausprägung geht es um die Widerstandsfähigkeit digitaler Infrastrukturen und Systeme.

Resilienz in Deutschland stärken

Digitale Resilienz bezeichnet die Fähigkeit eines Landes, kritische digitale Systeme auch unter Cyberangriffen oder sonstigen Störungen aufrechtzuerhalten oder schnell wiederherzustellen. Sie ist heute ein zentraler Bestandteil der nationalen Sicherheitsarchitektur, da die Bedrohungen zunehmend hybrid sind: Cyberattacken nehmen in Anzahl und Komplexität stetig zu und sind oft mit physischen Aktionen verzahnt⁶.

a) Wo digitale Resilienz in Deutschland bereits entsteht und aufgebaut wird

Die Angreifer agieren hochprofessionell – „Cybercrime as a Service“ macht Angriffswerkzeuge breit verfügbar, und auch staatliche Akteure verschärfen die Lage erheblich⁷. Die ökonomischen Schäden sind enorm: Rund 267 Milliarden

Euro kostet Cyberkriminalität die deutsche Wirtschaft pro Jahr⁸. Besonders Ausfälle kritischer Infrastrukturen haben unmittelbare Folgen für Sicherheit und Versorgung der Bevölkerung. Zudem können gezielte Desinformationskam-

pagnen das Vertrauen in Gesellschaft und Staat untergraben und so die Sicherheitslage weiter verschärfen. Digitale Resilienz ist folglich essenziell für eine robuste Wirtschaft und einen wehrhaften Staat⁹.

Europas Abhängigkeit von US-amerikanischen Cloud-Diensten ist trotz vermehrter Initiativen zu digitaler Souveränität weiter sehr hoch.¹⁰ Auch die Bundesregierung bewertet technologische Abhängigkeiten – etwa bei Cloud-Diensten, Netzwerktechnik oder Betriebssystemen – als strategisches Risiko für kritische Infrastrukturen, Datenhoheit und politische Handlungsfreiheit. Das Bundesministerium für Digitales und Staatsmodernisierung (BMDS) strebt daher eine strategische Neuausrichtung an: Abhängigkeiten von Anbietern aus Drittstaaten sollen verringert und eigene Schlüsseltechnologien wie KI, Cloud und Cybersicherheit gezielt gefördert werden – unter anderem durch den Ausbau europäischer Cloud-Infrastruktur, offene Standards sowie ein Beschaffungswesen, das den Staat zum Ankerkunden der heimischen Digitalwirtschaft macht.¹¹

Deutschland hat in den vergangenen Jahren diverse Schritte für den Ausbau der digitalen Resilienz angestoßen. 2022 beschloss die Bundesregierung erstmals eine nationale Resilienz-Strategie als Rahmen für einen ganzheitlichen Umgang mit Risiken¹². Zudem entsteht in Darmstadt ein Zentrum für digitale Resilienz, das KRITIS-Betreiber, Behörden, Wirtschaft und Wissenschaft für ein verbessertes Krisenmanagement vernetzt¹³. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wird als zentrale Cyber-Sicherheitsbehörde reformiert; 2023 übernahm eine neue Präsidentin mit dem Ziel, dem BSI mehr Unabhängigkeit und Schlagkraft zu verleihen¹⁴ und das Thema digitale Souveränität klar zu priorisieren¹⁵.

Deshalb wurden ein KRITIS-Dachgesetz nach der EU-Richtlinie zur Resilienz kritischer Einrichtungen (CER) umgesetzt und einheitliche Sicherheitsstandards für alle KRITIS-Sektoren

vorgegeben¹⁶. Das KRITIS-Dachgesetz ist am 17. März 2026 in Kraft getreten¹⁷. Parallel erfolgt die Umsetzung der EU-NIS-2-Richtlinie, wodurch deutlich mehr Unternehmen – auch aus IT, Gesundheit oder Versorgung – Cybersicherheitsauflagen erfüllen müssen¹⁸. Die EU-NIS-2-Richtlinie zur Stärkung der Cybersicherheit ist seit Dezember 2025 in Deutschland durch das NIS-2-Umsetzungsgesetz in nationales Recht in Kraft¹⁹. Die bisherigen Regeln erfassten zunächst nur rund 1.260 registrierte KRITIS-Betreiber – gemessen an den insgesamt rund 30.000 Unternehmen, die künftig unter die erweiterte NIS-2-Regulierung fallen, ein deutlich geringer Anteil von unter 5 Prozent.^{20,21} Im Finanzsektor sorgt die EU-Verordnung DORA für verbindliche Vorgaben, damit Banken und Versicherer ihr IT-Risiko systematischer managen²². Unterstützend wurden Programme wie „Digital Jetzt“ gestartet, um insbesondere den Mittelstand bei Investitionen in digitale Technologien und IT-Sicherheit zu fördern²³.

Zudem investiert Deutschland in digitale Souveränität – etwa mit dem europäischen Cloud-Projekt GAIA-X und dem nationalen Deutschland-Stack für die Verwaltung –, um Abhängigkeiten von fremden Anbietern zu reduzieren²⁴. Mit dem vorgeschlagenen Cloud- und KI-Entwicklungsgesetz (CADA) möchte die Europäische Kommission den digitalen Handlungsspielraum Europas spürbar ausweiten²⁵. Auch auf nationaler Ebene wird digitale Souveränität zunehmend praktisch umgesetzt: Für die Verwaltung hat das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS) mit openDesk eine quell-offene Office- und Kollaborationssuite als Alternative zu US-Software entwickelt.²⁶ Vorreiter ist hier Schleswig-Holstein: Das Land hat rund 80 Prozent der Verwaltungsarbeitsplätze von Microsoft Office auf LibreOffice umgestellt und spart dadurch jährlich über 15 Millionen Euro an Lizenzkosten.²⁷

Das Bundesdigitalministerium entwickelt mit dem „Deutschland-Stack“ eine nationale Technologieplattform, die offene, sichere und



skalierbare IT-Dienste für Bund, Länder und Kommunen bereitstellen soll²⁸. Der Stack basiert auf einem modularen Schichtenmodell – von Infrastruktur über Basisdienste bis zu Fachanwendungen – und soll bis 2028 konkrete Angebote liefern. Ziel ist es, vertrauenswürdige, interoperable und europäisch anschlussfähige Technologien zu fördern. Eine interaktive Landkarte für Standards und Technologien sowie eine breite Konsultation mit Stakeholdern

sollen die Entwicklung begleiten. Bund und Länder haben sich im Juni 2026 auf eine „verbindliche Anbindung und Flächendeckung“ des Deutschland-Stacks verständigt. Der Bund stellt zentrale Basiskomponenten und Standards bereit, während die Umsetzung flächendeckend bis 2028 erfolgen soll. Ziel ist es, den digitalen Flickenteppich der Verwaltung zu beenden und Behördengänge – beispielsweise eine digitale Ummeldung – drastisch zu verkürzen²⁹.

b) Das kann Deutschland von anderen Ländern lernen

Dennoch bestehen Schwächen. Gerade kleine und mittlere Unternehmen und viele Behörden sind weiterhin unzureichend geschützt – rund 61 % der KMU haben laut Umfragen kein angemessenes Schutzniveau³⁰. Es mangelt an übergreifender Koordination und Erfolgskontrolle: Diese Lücke könnte ein zentraler Chief Resilience Officer im Kanzleramt schließen³¹. Schließlich verschärft der Fachkräftemangel das Problem – Ende 2024 waren etwa 137.000 IT-Stellen unbesetzt³², was die Umsetzung vieler Vorhaben bremst.

Andere Länder sind Deutschland teils voraus. Estland hat nach den Cyberattacken von 2007 sehr früh eine umfassende Cyberstrategie implementiert und verfolgt seither einen Security-by-Design-Ansatz³³. Dort gehört Cyberaufklärung zur Staatsräson: Alle Beamten durchlaufen Cyberhygiene-Schulungen und öffentliche Kampagnen sensibilisieren die Bevölkerung³⁴ – ein Modell, das zu einer besonders wehrhaften digitalen Gesellschaft geführt hat. Im Juli 2026 unterzeichneten Bonn und der Rhein-Sieg-Kreis

mit der Republik Estland ein Memorandum of Understanding, um die Zusammenarbeit in der IT- und Cybersicherheit weiter voranzutreiben³⁵. Israel wiederum hat Cybersicherheit zur nationalen Priorität erklärt. Dank kontinuierlicher Strategien, enger Vernetzung von Militär, Tech-Industrie und Universitäten sowie konsequenter Talentförderung (u. a. im Militärdienst) gilt Israel heute als führend in der Cyberabwehr³⁶. Beide Länder zeigen, dass frühe, koordinierte Investitionen in Technologie und Bildung zu überdurchschnittlicher Resilienz führen.

Auch größere Staaten haben eine Vorreiterrolle. Frankreich hat mit der frühen Einrichtung einer eigenen Cyber-Sicherheitsbehörde (ANSSI) und einer nationalen Cloud-Strategie (Cloud souveraine) systematisch Kapazitäten aufgebaut. Strikte Vorgaben wie die Zertifizierung SecNumCloud für Cloud-Dienste³⁷ und das 2024 beschlossene Gesetz zur Sicherheit und Regulierung des digitalen Raums (SREN)³⁸ unterstreichen den entschlossenen Kurs. Im November 2025 veranstalteten Frankreich und Deutsch-

land einen Gipfel für mehr digitale Souveränität in Berlin. Sie setzen mit einem gemeinsamen Gipfel ein Zeichen für mehr digitale Unabhängigkeit. „Investitionen in Schlüsseltechnologien und die Stärkung europäischer Lösungen sind der Schlüssel, um im digitalen Raum weniger auf Dritte angewiesen zu sein“, so die Bundesregierung³⁹.

Die USA verfügen dank großer Ressourcen über eine robuste Ausgangslage: Mit der Cybersecurity and Infrastructure Security Agency (CISA) als zentralem Koordinator und regelmäßigen Strategie-Updates setzt die US-Regierung verstärkt auf Resilienz und verpflichtende Mindeststandards. Zugleich treiben amerikanische Tech-Konzerne als Innovationstreiber viele Sicherheitslösungen voran. Diese Beispiele zeigen, dass konsequente Strategien, stringente Umsetzung und der Aufbau souveräner digitaler Strukturen entscheidende Faktoren für Resilienz sind.

c) Darauf sollte Deutschland bei digitaler Resilienz den Fokus setzen

Gezielte Investitionen können die digitale Resilienz deutlich erhöhen. An erster Stelle steht die Modernisierung der Sicherheitsarchitekturen: Überall in Verwaltung und Wirtschaft sollten moderne Konzepte wie das Zero-Trust-Modell und ein wirksames Schwachstellen- sowie Incident-Management etabliert werden. Auch der Einsatz von KI-gestützter Abwehr lohnt sich – etwa durch Frühwarnsysteme, die Anomalien automatisch erkennen, oder automatisierte Response-Plattformen gegen Angriffe. Ebenso essenziell ist die Investition in Bildung und Awareness: Jeder Euro für Aus- und Weiterbildung in Cybersicherheit – von Schulprogrammen bis zu Führungskräfte trainings – verringert langfristig

das menschliche Fehlerrisiko und baut benötigte Fachkompetenzen auf. Schließlich muss die digitale Infrastruktur robuster gestaltet werden, z. B. durch souveräne Cloud-Plattformen und redundante Netze für den Krisenfall.

Bei knappen Mitteln sollte man Maßnahmen priorisieren, die neben Sicherheitsgewinn auch Wertschöpfung bringen. So schafft die Förderung von Cybersecurity-Innovationen und -Start-ups sowohl neue Schutztechnologien als auch Arbeitsplätze. Auch eine besser ausgebildete IT-Fachkräftebasis stärkt neben der Resilienz auch insgesamt die Wettbewerbsfähigkeit der Wirtschaft. Investitionen in digitale Resilienz

sind somit keine Wachstumsbremse. Sie bilden vielmehr die Grundlage für nachhaltiges ökonomisches Gedeihen im digitalen Zeitalter.

Die aktuelle Entwicklung im europäischen Defence-Tech-Sektor zeigt, dass Investitionen in deutsche Start-ups ein zentraler Hebel sind, um militärische Leistungsfähigkeit, digitale Souveränität und volkswirtschaftliche Resilienz gleichzeitig zu stärken. Panzer und andere klassische Hardware stehen längst nicht mehr primär für eine moderne Verteidigungsfähigkeit. Stattdessen sorgen softwaregetriebene Systeme dafür, dass Sensorik, Autonomie und KI in Echtzeit nutzbar werden. Start-ups wie Helsing verbinden Rüstung und digitale Transformation, indem sie KI-Plattformen entwickeln, die bestehende Waffensysteme softwareseitig auf ein völlig neues Leistungsniveau heben. Quantum Systems zeigt mit seinen autonomen Aufklärungsdrohnen, dass vernetzte, datenbasierte Systeme

heute oft effizienter und flexibler einsetzbar sind als schwere militärische Großgeräte. ARX Robotics beweist, dass modulare, KI-gesteuerte Bodenrobotik schneller skalierbar und nachhaltiger anpassbar ist als rein industrielle Hardwareprodukte. Diese Unternehmen schaffen technologische Mehrwerte, die nicht nur militärisch, sondern auch im zivilen Bereich – etwa Krisenmanagement oder Schutz kritischer Infrastrukturen – wirken. Investitionen in solche dual-use-fähigen Technologien erhöhen somit die Resilienz des gesamten Landes. Daher sollte Deutschland eine gezielte Strategie verfolgen, die Defence-Software, autonome Systeme und digitale Plattformtechnologien stärker fördert. Entscheidend ist, Innovationen zu unterstützen, die langfristig nutzbar, updatefähig und skalierbar sind – und damit deutlich nachhaltiger wirken als reine Beschaffungsprogramme für konventionelle Rüstungsgüter.

Konkrete Handlungsempfehlungen:

- **Zentrale Koordination schaffen:** Einrichtung eines nationalen Chief Resilience Officer im Kanzleramt, der alle Aktivitäten zur digitalen Resilienz strategisch bündelt und über Ressortgrenzen hinweg steuert⁴⁰.
- **Strategien konsequent umsetzen:** Schnellere Umsetzung bestehender Strategien und Gesetze (etwa KRITIS-Dachgesetz, NIS-2) mit klaren Fristen und Erfolgskontrollen. Zuständige Behörden (u. a. BSI, BBK) personell und technisch stärken.
- **KMU und Verwaltung unterstützen:** Förderprogramme und Beratungsangebote für Mittelstand und Kommunen ausbauen, um Sicherheitslücken zu schließen – zumal rund 61 % der KMU noch kein adäquates Schutzniveau haben⁴¹.
- **Fachkräfteoffensive starten:** Mehr Cyber-Studienplätze, Weiterbildungen und erleichterte Zuwanderung, um den eklatanten Mangel an IT-Sicherheitsexperten (2024 ca. 137.000 offene Stellen) zu beheben⁴².
- **Cybersicherheit zur Chefsache machen:** Unternehmensleitungen und Aufsichtsräte müssen digitale Risiken aktiv managen. Klare Vorgaben sollen das Problembewusstsein auf Führungsebene erhöhen⁴³.
- **Souveräne Technologien fördern:** Staatliche Unterstützung für innovative Sicherheitslösungen (etwa KI-Tools), europäische Cloud-Infrastrukturen und heimische Verschlüsselungstechnologien, um digitale Unabhängigkeit zu stärken und neue Wachstumsfelder zu erschließen.

Fazit und Ausblick

Die digitale Resilienz ist eine – wenn nicht die – zentrale Voraussetzung für die Wettbewerbsfähigkeit und Sicherheit Deutschlands im digitalen Zeitalter. Die Analyse zeigt, dass aktuelle Schwachstellen vor allem in unzureichender Infrastruktur, mangelnder Cybersicherheitsstrategie und fehlender Sensibilisierung der Bevölkerung bestehen. Um diese Probleme zu bewältigen, sind gezielte Investitionen in moderne Technologien, die Förderung von Fachkräften im Bereich Cybersicherheit sowie die Entwicklung eines robusten rechtlichen Rahmens notwendig.



Es wird weiterhin wesentlich bleiben, kontinuierlich in Innovationen zu investieren und die Zusammenarbeit zwischen öffentlichen Institutionen, Wirtschaft und Wissenschaft zu intensivieren. Da wir uns nicht in einem isolierten Kontext befinden, wird es wichtiger werden, nationale und europäische Initiativen zu stärken, um eine gemeinsame Sicherheitsarchitektur zu schaffen.

Die Sensibilisierung der Gesellschaft für digitale Risiken und die Förderung einer digitalen Kultur wird essenziell bleiben, um die Resilienz auf breiter Basis zu erhöhen. Insgesamt ist die nachhaltige Stärkung der digitalen Resilienz ein dynamischer Prozess, der eine kontinuierliche Anpassung und Weiterentwicklung erfordert, um den sich ständig wandelnden Bedrohungen effektiv begegnen zu können.

Quellen

- <https://difu.de/nachrichten/was-ist-eigentlich-resilienz>
- <https://www.bmz.de/de/service/lexikon/resilienz-70564>
- https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/NW_Oekonomische_Resilienz.pdf
- <https://www.baks.bund.de/de/arbeitspapiere/2016/was-ist-resilienz-unschaerfen-eines-schlüsselbegriffs> und <https://www.bundeswehr.de/de/gesellschaftliche-resilienz-zeitenwende-6041356>
- https://www.tab-beim-bundestag.de/themenfeld-biotechnologie-und-gesundheit_krisenradar-resilienz-von-gesellschaft-politik-und-wirtschaft-durch-krisenvorhersage-staerken.php
- <https://wirtschaftsrat.de/de/presse/wr-intern/digitale-resilienz-ist-kein-luxus-sie-ist-%C3%BCberlebenswichtig/#:~:text=In%20einer%20Welt%2C%20die%20zunehmend,auf%20die%20digitale%20Ebene%20beschr%C3%A4nkt>
- <https://wirtschaftsrat.de/de/presse/wr-intern/digitale-resilienz-ist-kein-luxus-sie-ist-%C3%BCberlebenswichtig/#:~:text=kritische%20Infrastrukturen%20nehmen%20nicht%20nur,zunehmend%20mit%20physischen%20Angriffen%20verzahnt>
- <https://wirtschaftsrat.de/de/presse/wr-intern/digitale-resilienz-ist-kein-luxus-sie-ist-%C3%BCberlebenswichtig/#:~:text=Die%20%C3%B6konomischen%20Folgen%20sind%20verheerend%3A,heute%20durch%20unzureichende%20Cybersicherheit%20entstehen>
- <https://wirtschaftsrat.de/de/presse/wr-intern/digitale-resilienz-ist-kein-luxus-sie-ist-%C3%BCberlebenswichtig/#:~:text=Die%20%C3%B6konomischen%20Folgen%20sind%20verheerend%3A,heute%20durch%20unzureichende%20Cybersicherheit%20entstehen>
- <https://www.heise.de/news/Strafgerichtshof-Microsofts-E-Mail-Sperre-als-Weckruf-fuer-digitale-Souveraenitaet-10387368.html>
- <https://bmds.bund.de/themen/digitale-souveraenitaet>
- <https://www.praeventionstag.de/nano.cms/news/details/9174#:~:text=ver%C3%B6ffentlicht%20www.im%20Umgang%20mit%20Risiken>
- <https://www.security-insider.de/nationales-zentrum-digitale-resilienz-deutschland-a-66ca8d09b00eefcfce9a0e27ecf11a54/#:~:text=Austauschplattform%20f%C3%BCr%20KRITIS>
- https://www.bsi.bund.de/DE/Das-BSI/Organisation-und-Aufbau/Leitung/leitung_node.html#:~:text=Claudia%20Plattner%20ist%20seit%20dem,wurde%201973%20in%20Mainz
- BSI - Presse - Positionierung des BSI zu Digitaler Souveränität in Zeiten von Cyber Dominance und „Schneller zur digitalen Souveränität“ - Atlantik-Brücke e.V.
- <https://www.openkritis.de/it-sicherheitsgesetz/kritis-dachgesetz-sicherheitsgesetz-3-0.html#:~:text=Das%20KRITIS,physische%20Sicherheit%2C%20Personal%20und%20Krisenmanagement>
- Schutz kritischer Infrastruktur gestärkt | Bundesregierung
- <https://www.openkritis.de/it-sicherheitsgesetz/kritis-dachgesetz-sicherheitsgesetz-3-0.html#:~:text=Parallel%20zum%20KRITIS,Anfang%202026%20in%20Kraft%20treten>
- NIS2-Umsetzungsgesetz in Deutschland 2025 – OpenKRITIS
- <https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-in-Zahlen/nis-2-in-zahlen.html>
- <https://wirtschaftsrat.de/de/presse/wr-intern/digitale-resilienz-ist-kein-luxus-sie-ist-%C3%BCberlebenswichtig/#:~:text=Trotz%20bestehender%20gesetzlicher%20Rahmenbedingungen%20wie,Anteil%20angesichts%20der%20realen%20Bedrohungslage>
- <https://www.openkritis.de/it-sicherheitsgesetz/kritis-dachgesetz-sicherheitsgesetz-3-0.html#:~:text=Finanzwesen%20%5E%20DORA,und%20Daten%20%C3%BCbertragung>
- <https://www.bundeswirtschaftsministerium.de/Redaktion/DE/FAQ/Digital-Jetzt/faq-digital-jetzt.html#:~:text=,Dezember%202023%20befristet>
- <https://scs.community/#:~:text=On%20the%20digital%20summit%202019,as%20Gaia%20X%20Lighthouse%20Project> und <https://netzpolitik.org/2025/deutschland-stack-was-ist-drin-im-baukasten-fuer-die-digitale-verwaltung/#:~:text=Was%20ist%20der%20Deutschland>
- Gaia-X zum EU-Cloud- und KI-Entwicklungsgesetz: Ein Überblick - All About Security Das Online-Magazin zu Cybersecurity (Cyber-sicherheit), Ransomware, Phishing, IT-Sicherheit, Netzwerksicherheit, KI, Threats, DDoS, Identity & Access, Plattform-sicherheit

26 <https://www.opendesk.eu/de/ueber>

27 https://www.schleswig-holstein.de/DE/landesregierung/ministerien-behoerden/I/Presse/PI/2025/cds/251204_cds_open-source

28 Deutschland-Stack: So soll die nationale, souveräne Technologieplattform aussehen: <https://www.heise.de/news/Deutschland-Stack-So-soll-die-nationale-souveraene-Technologieplattform-aussehen-10748972.html>

29 <https://bmds.bund.de/themen/digitaler-staat/deutschland-stack>

30 <https://wirtschaftsrat.de/de/presse/wr-intern/digitale-resilienz-ist-kein-luxus-sie-ist-%C3%BCberlebenswichtig/#:~:text=Besonders%20alarmierend%20ist%20die%20Situation,Aufwand%20hohe%20Sch%C3%A4den%20verursachen%20k%C3%B6nnen>

31 <https://www.security-insider.de/deutschland-chief-resilience-officer-a-f526886ab5c088f64d4c8e29ab1785c1/?cflt=rel#:~:text=match%20at%20L460%20Ein%20Chief,politischem%20Mandat%2C%20klarer%20Weisungskompetenz%20und>

32 <https://www.henrichsen4easy.de/news/it-unter-druck-fachkraeftemangel-und-steigende-anforderungen#:~:text=IT%20unter%20Druck%20%E2%80%93%20Fachkr%C3%A4ftemangel,H%C3%B6chststand%2C%20der%20sich%20besonders>

33 <https://e-estonia.com/estonias-cyber-security-model-for-europe/#:~:text=Estonia%E2%80%99s%20unique%20history%20and%20proactive,grow%20in%20sophistication%20and%20scale>

34 <https://e-estonia.com/estonias-cyber-security-model-for-europe/#:~:text=Cyber%20security%20is%20not%20just,These%20initiatives>

35 Cybersicherheit: Von den Besten lernen für mehr digitale Resilienz | Bundesstadt Bonn

36 <https://wirtschaftsrat.de/de/presse/wr-intern/digitale-resilienz-ist-kein-luxus-sie-ist-%C3%BCberlebenswichtig/#:~:text=Langfristig%20kann%20digitale%20Resilienz%20nur,und%20darf%20nicht%20l%C3%A4nger%20z%C3%B6gern>

37 <https://itif.org/publications/2025/05/25/france-cloud-service-restrictions/#:~:text=France%27s%20cloud%20security%20certification%20scheme%2C,protectionist%20digital%20regulations%20in%20Europe>

38 <https://incyber.org/en/article/france-sren-bill-strengthens-position-of-sovereign-cloud-players/#:~:text=France%3A%20SREN%20bill%20strengthens%20position,The%20law%20contains%20several>

39 Gipfel für europäische digitale Souveränität | Bundesregierung

40 <https://www.security-insider.de/deutschland-chief-resilience-officer-a-f526886ab5c088f64d4c8e29ab1785c1/?cflt=rel#:~:text=match%20at%20L460%20Ein%20Chief,politischem%20Mandat%2C%20klarer%20Weisungskompetenz%20und>

41 <https://wirtschaftsrat.de/de/presse/wr-intern/digitale-resilienz-ist-kein-luxus-sie-ist-%C3%BCberlebenswichtig/#:~:text=Besonders%20alarmierend%20ist%20die%20Situation,Aufwand%20hohe%20Sch%C3%A4den%20verursachen%20k%C3%B6nnen>

42 <https://www.henrichsen4easy.de/news/it-unter-druck-fachkraeftemangel-und-steigende-anforderungen#:~:text=IT%20unter%20Druck%20%E2%80%93%20Fachkr%C3%A4ftemangel,H%C3%B6chststand%2C%20der%20sich%20besonders>

43 <https://wirtschaftsrat.de/de/presse/wr-intern/digitale-resilienz-ist-kein-luxus-sie-ist-%C3%BCberlebenswichtig/#:~:text=,Infrastrukturen%2C%20insbesondere%20im%20Bereich%20Energieversorgung>

Bildquellen

Seite 5: ©Adobe-Stock.com/Eduardo
Seite 9: ©Adobe-Stock.com/nfiniteFlow
Seite 12: ©Adobe-Stock.com/Gorodenkoff

Copyright © Institut der Wirtschaftsprüfer in Deutschland e.V., Düsseldorf 2026

Dieses Position Paper wurde vom Ausschuss Trendwatch des IDW erarbeitet.
Wir freuen uns über Ihre Anmerkungen. Sie können diese direkt an das Institut der Wirtschaftsprüfer in Deutschland e.V., Postfach 320580, 20420 Düsseldorf, oder an info@idw.de senden.

watch trend

**Institut der Wirtschaftsprüfer
in Deutschland e.V.**

Roßstraße 74 | 40476 Düsseldorf

 0211 - 4561-0

 info@idw.de

 www.idw.de

IDW