

Holger Reibold

Cyber Resilience Act in der Praxis

Anforderungen verstehen –
Umsetzung strukturieren –
Compliance erreichen

BRAIN-MEDIA.DE

Alle Rechte vorbehalten. Ohne ausdrückliche, schriftliche Genehmigung des Verlags ist es nicht gestattet, das Buch oder Teile daraus in irgendeiner Form durch Fotokopien oder ein anderes Verfahren zu vervielfältigen oder zu verbreiten. Dasselbe gilt auch für das Recht der öffentlichen Wiedergabe. Der Verlag macht darauf aufmerksam, dass die genannten Firmen- und Markennamen sowie Produktbezeichnungen in der Regel marken-, patent- oder warenrechtlichem Schutz unterliegen.

Verlag und Autor übernehmen keine Gewähr für die Funktionsfähigkeit beschriebener Verfahren und Standards.

© 2026 Brain-Media.de

ISBN: 978-3-95444-333-8

Cover: Freepik

Brain-Media.de

Dr. Holger Reibold – Hubert-Müller-Str. 52c – 66111 Saarbrücken

info@brain-media.de – www.brain-media.de

Inhaltsverzeichnis

Inhaltsverzeichnis	I
Vorwort	1
1 Einführung in den Cyber Resilience Act.....	5
1.1 Motivation und Hintergrund	6
1.2 Ziele des Cyber Resilience Act.....	8
1.3 Einordnung in die europäische Regulierung.....	12
1.4 Zeitplan und Übergangsfristen.....	14
1.5 Bedeutung für Unternehmen.....	17
1.6 Management Summary	21
2 Geltungsbereich	23
2.1 Definition digitaler Produkte im CRA	24
2.2 Software, Hardware und vernetzte Produkte	27
2.3 Produkte mit digitalen Elementen.....	30
2.4 Ausnahmen und Sonderregelungen.....	32
2.5 Beispiele aus der Praxis	35
2.6 Management Summary	38
3 Rollen und Verantwortlichkeiten	39
3.1 Hersteller.....	40

3.2	Importeure.....	43
3.3	Händler und Distributoren	46
3.4	OS-Komponenten und Drittanbieter	48
3.5	Verantwortung entlang der Lieferkette.....	51
3.6	Management Summary	54
4	Klassifizierung und Risikobewertung	55
4.1	Risikobasierter Ansatz des CRA.....	56
4.2	Kritische Produktkategorien.....	59
4.3	Kriterien zur Einstufung digitaler Produkte	61
4.4	Durchführung einer Risikobewertung.....	64
4.5	Dokumentation der Klassifizierung	68
4.6	Management Summary	71
5	Security by Design vs. Security by Default.....	73
5.1	Grundprinzipien	74
5.2	Bedrohung und Risikoanalyse.....	78
5.3	Architektur und Designentscheidungen	81
5.4	Sichere Standardkonfigurationen	84
5.5	Integration in Entwicklungsprozesse	87
5.6	Management Summary	90
6	Sichere Softwareentwicklung	91
6.1	Secure Development Lifecycle	93

6.2	Sichere Programmierpraktiken.....	95
6.3	Code Reviews und Sicherheitsprüfungen	98
6.4	Automatisierte Sicherheitstests	101
6.5	Externe Softwarekomponenten.....	104
6.6	Management Summary	108
7	Schwachstellenmanagement.....	109
7.1	Vulnerability Management Prozesse	110
7.2	Coordinated Vulnerability Disclosure	114
7.3	Patch- und Update-Management	117
7.4	Umgang mit Zero-Day-Schwachstellen.....	120
7.5	Updates über den Produktlebenszyklus	123
7.6	Management Summary	126
8	Dokumentation und Konformität.....	127
8.1	Technische Dokumentation	128
8.2	Anforderungen an Sicherheitsnachweise	132
8.3	Konformitätsbewertungsverfahren.....	135
8.4	CE-Kennzeichnung und Marktüberwachung.....	139
8.5	Vorbereitung auf Audits	142
8.6	Management Summary	145
9	Incident Reporting und Kommunikation.....	147
9.1	Definition eines Sicherheitsvorfalls	148

9.2	Meldepflichten nach CRA.....	151
9.3	Zusammenarbeit mit Behörden	156
9.4	Kommunikation mit Kunden und Partnern	158
9.5	Integration in Incident-Response-Prozesse	162
9.6	Management Summary	165
10	Umsetzung im Unternehmen.....	167
10.1	Governance und Organisatorisches	168
10.2	Integration in Managementsysteme.....	172
10.3	CRA-Implementierungsprojekt.....	175
10.4	Schulung und Sensibilisierung	178
10.5	Verbesserung der Produktsicherheit	180
10.6	Management Summary	184
11	CRA-Implementierungsrahmen	185
11.1	Reifegradmodell für CRA-Compliance	186
11.2	Integration	188
11.3	CRA-Artefakte und Werkzeuge.....	189
11.4	Fortschrittsmessung und Metriken.....	191
11.4	Management Summary	192
	Zum Schluss	193
	Anhang.....	197
	CRA-Compliance-Checkliste	197

Beispiel einer CRA-Implementierungsroadmap.....	202
Struktur einer technischen Dokumentation	207
Glossar	212
Abkürzungsverzeichnis.....	219
Literatur- und Quellenverzeichnis	221
Stichwortverzeichnis	223
Mehr von Brain-Media.de	227

Vorwort

Die digitale Transformation hat in den vergangenen Jahren nahezu alle Branchen grundlegend verändert. Produkte, die früher rein mechanisch oder elektrisch funktionierten, sind heute zunehmend softwarebasiert, vernetzt und Teil komplexer digitaler Ökosysteme. Von industriellen Steuerungssystemen über intelligente Haushaltsgeräte bis hin zu medizinischen Geräten und Fahrzeugen – digitale Komponenten sind inzwischen ein zentraler Bestandteil moderner Produkte. Mit dieser Entwicklung wachsen jedoch auch die Risiken. Schwachstellen in Software, unsichere Kommunikationsschnittstellen oder mangelnde Update-Mechanismen können gravierende Sicherheitslücken verursachen.

Cyberangriffe auf vernetzte Produkte sind längst keine theoretische Bedrohung mehr. Immer häufiger werden Sicherheitslücken in Geräten und Anwendungen ausgenutzt, um Daten zu stehlen, Systeme zu manipulieren oder ganze Infrastrukturen lahmzulegen. Besonders kritisch wird dies, wenn Produkte Teil sensibler Umgebungen sind, etwa in der Industrie, im Gesundheitswesen oder in der Energieversorgung. Gleichzeitig zeigt sich, dass viele Sicherheitsprobleme nicht erst im Betrieb entstehen, sondern bereits in der Entwicklungsphase angelegt sind.

Vor diesem Hintergrund hat die Europäische Union mit dem Cyber Resilience Act (CRA) einen neuen regulatorischen Rahmen geschaffen. Ziel dieser Verordnung ist es, ein einheitliches Mindestniveau an Cybersicherheit für Produkte mit digitalen Elementen sicherzustellen. Hersteller sollen verpflichtet werden, Sicherheitsaspekte bereits bei der Entwicklung zu berücksichtigen, Schwachstellen systematisch zu behandeln und ihre Produkte während des gesamten Lebenszyklus angemessen zu unterstützen. Damit verfolgt der CRA einen grundlegenden Paradigmenwechsel: Sicherheit wird nicht länger ausschließlich als betriebliche Aufgabe betrachtet, sondern als integraler Bestandteil der Produktverantwortung.

Für viele Unternehmen bedeutet diese Regulierung eine erhebliche Veränderung ihrer bisherigen Prozesse. Entwicklungsabteilungen müssen Sicherheitsanforderungen stärker berücksichtigen, Produktmanager müssen Lebenszyklen und Update-Strategien planen, und Compliance-Verantwortliche müssen neue Dokumentations- und Meldepflichten erfüllen. Gleichzeitig bietet der CRA auch Chancen. Unternehmen, die Sicherheit strukturiert in ihre Produkte integrieren, stärken nicht nur ihre regulatorische Position, sondern auch das Vertrauen ihrer Kunden und Partner.

Dieses Buch richtet sich an Verantwortliche in Unternehmen, die digitale Produkte entwickeln, herstellen oder vertreiben. Es richtet sich ebenso an Produktmanager, Entwicklerinnen und Entwickler, Sicherheitsverantwortliche sowie an Entscheiderinnen und Entscheider im Management. Ziel ist es, die Anforderungen des Cyber Resilience Act

verständlich zu erläutern und konkrete Wege zur praktischen Umsetzung aufzuzeigen.

Der Schwerpunkt liegt dabei bewusst auf der Praxis. Neben der Einordnung der regulatorischen Anforderungen werden typische Herausforderungen in Entwicklungsprozessen, im Schwachstellenmanagement und in der technischen Dokumentation behandelt. Zahlreiche Beispiele, Strukturvorschläge und Checklisten sollen dabei helfen, die Anforderungen des CRA systematisch in bestehende Prozesse zu integrieren.

Das Buch folgt dabei einer klaren Struktur. Zunächst werden die Grundlagen des Cyber Resilience Act sowie dessen Geltungsbereich erläutert. Anschließend werden Rollen, Verantwortlichkeiten und Risikoklassifizierungen behandelt. In den folgenden Kapiteln liegt der Fokus auf der sicheren Produktentwicklung, dem Umgang mit Schwachstellen und dem Management des gesamten Produktlebenszyklus. Weitere Kapitel widmen sich der technischen Dokumentation, der Konformitätsbewertung sowie den Anforderungen an Incident Reporting und Behördenkommunikation. Abschließend wird dargestellt, wie Unternehmen ein strukturiertes Implementierungsprojekt zur Umsetzung der CRA-Anforderungen aufsetzen können.

Der Cyber Resilience Act wird die Entwicklung digitaler Produkte in Europa nachhaltig prägen. Unternehmen, die sich frühzeitig mit den Anforderungen auseinandersetzen und ihre Prozesse entsprechend anpassen, können nicht nur regulatorische Risiken reduzieren, sondern auch ihre Wettbewerbsfähigkeit stärken. Produktsicherheit wird

zunehmend zu einem Qualitätsmerkmal und zu einem entscheidenden Faktor für Vertrauen in digitale Technologien.

Dieses Buch soll einen Beitrag dazu leisten, die Anforderungen des Cyber Resilience Act verständlich, strukturiert und praxisnah zugänglich zu machen – und Unternehmen dabei unterstützen, Cybersicherheit als festen Bestandteil ihrer Produktstrategie zu etablieren.

Dabei wünsche ich Ihnen viel Erfolg!

Herzlichst

Holger Reibold

1 Einführung in den Cyber Resilience Act

Digitale Produkte sind zunehmend Angriffsziel – der Cyber Resilience Act schafft erstmals verbindliche Sicherheitsregeln für den europäischen Markt.

Digitale Produkte sind heute in nahezu allen Lebens- und Wirtschaftsbereichen präsent. Software, vernetzte Geräte und cloudbasierte Dienste bilden die Grundlage moderner Geschäftsmodelle, industrieller Prozesse und alltäglicher Anwendungen. Gleichzeitig nimmt jedoch die Zahl der Sicherheitsvorfälle zu, die auf Schwachstellen in solchen Produkten zurückzuführen sind. Unsichere Standardkonfigurationen, fehlende Updates oder unzureichend geprüfte Softwarekomponenten können dazu führen, dass Produkte bereits bei ihrer Markteinführung Sicherheitsrisiken enthalten.

Der Cyber Resilience Act der Europäischen Union adressiert genau dieses Problem. Ziel der Regulierung ist es, verbindliche Mindestanforderungen an die Cybersicherheit von Produkten mit digitalen Elementen festzulegen. Hersteller werden verpflichtet, Sicherheitsaspekte bereits in der Entwicklungsphase zu berücksichtigen, Schwachstellen systematisch zu behandeln und ihre Produkte während des gesamten Lebenszyklus zu unterstützen.

Dieses Kapitel führt in die grundlegenden Ziele und Hintergründe des Cyber Resilience Act ein. Es erläutert die Motivation für die Regulierung, ordnet den CRA in den Kontext der europäischen Cybersecurity-Strategie ein und gibt einen Überblick über Zeitplan, Übergangsfristen sowie die praktischen Auswirkungen für Unternehmen und Produktentwicklung.

1.1 Motivation und Hintergrund

Die zunehmende Digitalisierung von Produkten und Dienstleistungen hat in den letzten Jahren zu einer tiefgreifenden Veränderung vieler Wirtschaftsbereiche geführt. Software, vernetzte Geräte und digitale Plattformen sind heute fester Bestandteil industrieller Produktionsprozesse, moderner Infrastrukturen und des alltäglichen Lebens. Gleichzeitig entstehen durch diese Vernetzung neue Angriffsflächen für Cyberangriffe. Sicherheitslücken in Software oder unsichere Systemarchitekturen können dazu führen, dass Produkte bereits bei ihrer Markteinführung ein erhebliches Risiko darstellen.

In der Vergangenheit zeigte sich immer wieder, dass viele digitale Produkte ohne ausreichende Sicherheitsmaßnahmen entwickelt wurden. Häufig standen Markteinführungszeiten, Funktionsumfang oder Kostenoptimierung im Vordergrund, während Sicherheitsaspekte nur eine untergeordnete Rolle spielten. Typische Probleme waren etwa voreingestellte Standardpasswörter, fehlende Update-Mechanismen oder die Integration unsicherer Softwarekomponenten aus

Drittquellen. Sobald solche Produkte in großem Maßstab eingesetzt werden, können einzelne Schwachstellen weitreichende Auswirkungen haben.

Mehrere öffentlich bekannt gewordene Sicherheitsvorfälle haben deutlich gemacht, welche Folgen mangelnde Produktsicherheit haben kann. Angriffe auf vernetzte Geräte, industrielle Steuerungssysteme oder cloudbasierte Plattformen haben gezeigt, dass Schwachstellen nicht nur einzelne Unternehmen betreffen, sondern auch kritische Infrastrukturen und ganze Lieferketten gefährden können. Gleichzeitig wird es für Nutzerinnen und Nutzer immer schwieriger zu beurteilen, ob ein digitales Produkt angemessene Sicherheitsstandards erfüllt.

Die Europäische Union verfolgt daher das Ziel, ein einheitliches Mindestniveau an Cybersicherheit für Produkte mit digitalen Elementen zu etablieren. Während frühere Regulierungen vor allem Betreiber von IT-Systemen oder kritischen Infrastrukturen adressierten, setzt der Cyber Resilience Act deutlich früher an – nämlich bei der Entwicklung und Herstellung der Produkte selbst. Sicherheit soll nicht erst im Betrieb nachgerüstet werden, sondern von Anfang an Bestandteil des Produktdesigns sein.

Ein weiterer wichtiger Hintergrund für die Regulierung ist die zunehmende Komplexität moderner Software. Viele Produkte bestehen heute aus einer Vielzahl externer Bibliotheken, Open-Source-Komponenten und Cloud-Diensten. Diese Abhängigkeiten erhöhen das Risiko, dass Schwachstellen unbemerkt in Produkte integriert werden.

Ohne strukturierte Prozesse für das Management solcher Komponenten kann es für Hersteller schwierig werden, Sicherheitslücken schnell zu identifizieren und zu beheben.

Der Cyber Resilience Act reagiert auf diese Entwicklungen, indem er klare Anforderungen an Hersteller digitaler Produkte definiert. Dazu gehören unter anderem Verpflichtungen zur sicheren Produktentwicklung, zum Schwachstellenmanagement sowie zur Bereitstellung von Sicherheitsupdates während des gesamten Produktlebenszyklus. Gleichzeitig sollen transparente Dokumentations- und Meldepflichten sicherstellen, dass Sicherheitsvorfälle schneller erkannt und koordiniert behandelt werden können.

Damit verfolgt die Regulierung nicht nur ein sicherheitspolitisches Ziel, sondern auch ein wirtschaftliches. Einheitliche Sicherheitsanforderungen sollen gleiche Wettbewerbsbedingungen im europäischen Binnenmarkt schaffen und das Vertrauen in digitale Produkte stärken. Hersteller, die Sicherheitsstandards konsequent umsetzen, können dadurch ihre Marktposition verbessern und langfristig von stabileren und zuverlässigeren Produkten profitieren.

1.2 Ziele des Cyber Resilience Act

Der Cyber Resilience Act verfolgt das übergeordnete Ziel, die Cybersicherheit von Produkten mit digitalen Elementen innerhalb der Europäischen Union systematisch zu verbessern. Digitale Produkte sind heute häufig Bestandteil kritischer Prozesse in Wirtschaft und

Gesellschaft. Gleichzeitig werden Sicherheitsanforderungen bei der Entwicklung solcher Produkte nicht immer ausreichend berücksichtigt. Der CRA soll daher sicherstellen, dass grundlegende Sicherheitsprinzipien verbindlicher Bestandteil von Produktentwicklung, Vermarktung und Betrieb werden.

Ein zentrales Ziel der Regulierung besteht darin, ein einheitliches Mindestniveau an Cybersicherheit im europäischen Binnenmarkt zu etablieren. Hersteller, die digitale Produkte in der EU bereitstellen, sollen künftig klar definierte Sicherheitsanforderungen erfüllen. Dadurch soll verhindert werden, dass unsichere Produkte auf den Markt gelangen und potenziell erhebliche Risiken für Nutzerinnen und Nutzer, Unternehmen oder kritische Infrastrukturen verursachen. Gleichzeitig wird durch harmonisierte Regeln vermieden, dass unterschiedliche nationale Anforderungen entstehen, die den freien Warenverkehr im Binnenmarkt erschweren könnten.

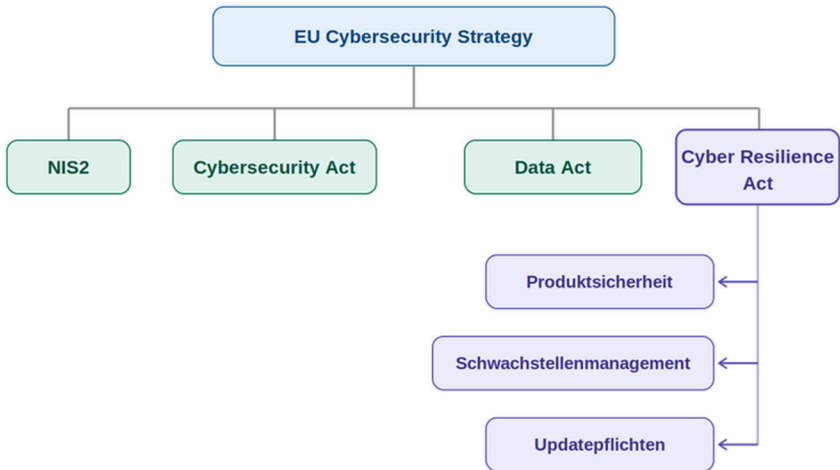
Ein weiterer wichtiger Aspekt des Cyber Resilience Act ist die Verlagerung von Verantwortung hin zu den Herstellern digitaler Produkte. Während Cybersicherheit bislang häufig als Aufgabe der Betreiber von IT-Systemen betrachtet wurde, adressiert der CRA ausdrücklich die Phase der Produktentwicklung. Hersteller sollen verpflichtet werden, Sicherheitsaspekte bereits im Design und in der Architektur ihrer Produkte zu berücksichtigen. Dieses Prinzip wird häufig als „Security by Design“ bezeichnet und umfasst unter anderem sichere Standardkonfigurationen, robuste Authentifizierungsmechanismen sowie eine systematische Analyse potenzieller Bedrohungen.

Darüber hinaus legt der CRA großen Wert auf den sicheren Umgang mit Schwachstellen. Digitale Produkte enthalten häufig komplexe Softwarekomponenten, deren Sicherheitsstatus sich im Laufe der Zeit verändern kann. Neue Schwachstellen werden regelmäßig entdeckt, und Hersteller müssen in der Lage sein, schnell darauf zu reagieren. Der Cyber Resilience Act fordert deshalb strukturierte Prozesse für das Schwachstellenmanagement sowie klare Mechanismen für Sicherheitsupdates. Produkte sollen während ihres vorgesehenen Lebenszyklus aktiv gepflegt und gegen neu entdeckte Risiken abgesichert werden.

Ein weiteres Ziel der Regulierung ist die Verbesserung der Transparenz im Umgang mit Sicherheitsvorfällen. Der CRA verpflichtet Hersteller dazu, bestimmte Sicherheitsvorfälle und aktiv ausgenutzte Schwachstellen an zuständige Behörden zu melden. Dadurch soll eine bessere Übersicht über aktuelle Bedrohungen entstehen und eine koordinierte Reaktion auf größere Sicherheitsprobleme ermöglicht werden. Gleichzeitig können Informationen über Schwachstellen schneller an betroffene Nutzer weitergegeben werden.

Neben sicherheitstechnischen Aspekten verfolgt der Cyber Resilience Act auch wirtschaftspolitische Ziele. Einheitliche Sicherheitsstandards können dazu beitragen, das Vertrauen in digitale Produkte zu stärken und damit die Akzeptanz digitaler Technologien zu erhöhen. Für Hersteller bedeutet dies langfristig auch einen Wettbewerbsvorteil, da Produkte mit klar definierten Sicherheitsmerkmalen zunehmend zu einem wichtigen Qualitätskriterium werden.

Insgesamt zielt der Cyber Resilience Act darauf ab, Cybersicherheit stärker als integralen Bestandteil moderner Produktentwicklung zu verankern. Sicherheit soll nicht als nachträgliche Ergänzung verstanden werden, sondern als grundlegende Eigenschaft digitaler Produkte. Durch klare Anforderungen, transparente Prozesse und verbindliche Verantwortlichkeiten soll ein nachhaltiger Beitrag zur Stabilität und Sicherheit digitaler Infrastrukturen in Europa geleistet werden.



Die EU Cybersecurity Regulatory Landscape: Der Cyber Resilience Act ist Teil einer umfassenden europäischen Cybersecurity-Strategie. Gemeinsam mit Regelwerken wie NIS-2, dem Cybersecurity Act und weiteren Initiativen bildet er einen regulatorischen Rahmen zur Verbesserung digitaler Sicherheit.

1.3 Einordnung in die europäische Regulierung

Der Cyber Resilience Act ist Teil einer umfassenden europäischen Strategie zur Stärkung der Cybersicherheit. In den vergangenen Jahren hat die Europäische Union mehrere regulatorische Initiativen verabschiedet, um den Schutz digitaler Infrastrukturen, Dienstleistungen und Produkte systematisch zu verbessern. Während einige dieser Regelwerke primär Betreiber kritischer Systeme adressieren, konzentriert sich der Cyber Resilience Act auf die Sicherheit der Produkte selbst.

Ein wichtiger Baustein dieser regulatorischen Landschaft ist die NIS2-Richtlinie. Sie verpflichtet Betreiber kritischer Infrastrukturen sowie zahlreiche weitere Organisationen dazu, angemessene Maßnahmen zum Schutz ihrer Netz- und Informationssysteme umzusetzen. Dazu gehören unter anderem Risikomanagement, Incident Response und Meldepflichten bei Sicherheitsvorfällen. Der Fokus liegt dabei jedoch auf Organisationen und deren IT-Betrieb. Der Cyber Resilience Act ergänzt diesen Ansatz, indem er bereits bei der Entwicklung und Bereitstellung digitaler Produkte ansetzt.

Eine weitere relevante Regelung ist der europäische Cybersecurity Act. Mit diesem Rechtsrahmen wurde ein europäisches Zertifizierungssystem für IT-Sicherheitsprodukte und -dienste geschaffen. Ziel ist es, standardisierte Zertifizierungen zu ermöglichen, die Vertrauen in digitale Technologien schaffen. Während der Cybersecurity Act freiwillige Zertifizierungsmechanismen etabliert, verfolgt der Cyber

Resilience Act einen stärker verpflichtenden Ansatz. Hersteller müssen bestimmte Sicherheitsanforderungen erfüllen, um ihre Produkte im europäischen Markt bereitstellen zu dürfen.

Auch bestehende Regelwerke aus dem Bereich der Produktsicherheit spielen eine Rolle im regulatorischen Kontext des CRA. Traditionelle Produktsicherheitsvorschriften konzentrierten sich bislang vor allem auf physische Risiken, etwa elektrische Sicherheit oder mechanische Gefährdungen. Mit der zunehmenden Digitalisierung von Produkten wird jedoch deutlich, dass auch Software und digitale Schnittstellen sicherheitsrelevant sind. Der Cyber Resilience Act erweitert daher den klassischen Produktsicherheitsansatz um Anforderungen an Cybersicherheit.

Darüber hinaus bestehen Überschneidungen mit weiteren europäischen Initiativen wie dem Datenschutzrecht oder der Regulierung digitaler Dienste. Obwohl diese Regelwerke unterschiedliche Zielsetzungen verfolgen, adressieren sie teilweise ähnliche Themenbereiche, etwa den Umgang mit Sicherheitsvorfällen oder den Schutz sensibler Informationen. Unternehmen müssen daher häufig mehrere regulatorische Anforderungen parallel berücksichtigen.

Der Cyber Resilience Act nimmt innerhalb dieses regulatorischen Rahmens eine besondere Rolle ein. Während viele bestehende Vorschriften auf organisatorische Sicherheitsmaßnahmen oder auf bestimmte Sektoren abzielen, konzentriert sich der CRA auf Produkte mit digitalen Elementen und deren gesamten Lebenszyklus. Hersteller werden verpflichtet, Sicherheitsanforderungen bereits während

der Entwicklung zu berücksichtigen und ihre Produkte über einen definierten Zeitraum hinweg zu unterstützen.

Durch diese Position innerhalb der europäischen Cybersecurity-Strategie ergänzt der Cyber Resilience Act bestehende Regelwerke und schließt eine wichtige Lücke: die systematische Absicherung digitaler Produkte bereits vor ihrem Einsatz in realen Umgebungen. Unternehmen müssen daher zunehmend sowohl organisatorische Sicherheitsanforderungen als auch produktbezogene Cybersicherheitsvorgaben berücksichtigen, um regulatorische Compliance sicherzustellen.

1.4 Zeitplan und Übergangsfristen

Der Cyber Resilience Act wird nach seiner endgültigen Verabschiedung schrittweise innerhalb der Europäischen Union wirksam. Wie bei vielen europäischen Verordnungen ist eine Übergangsphase vorgesehen, damit Unternehmen ausreichend Zeit erhalten, ihre Prozesse, Produkte und organisatorischen Strukturen an die neuen Anforderungen anzupassen. Dennoch sollten Hersteller digitaler Produkte frühzeitig mit der Vorbereitung beginnen, da die Umsetzung der Vorgaben in der Praxis häufig umfassende Veränderungen in Entwicklungs- und Sicherheitsprozessen erfordert.

Nach Inkrafttreten der Verordnung gilt der Cyber Resilience Act grundsätzlich unmittelbar in allen Mitgliedstaaten der Europäischen Union. Anders als bei Richtlinien ist keine separate nationale Umsetzung erforderlich. Dies führt zu einheitlichen Regeln im europäischen

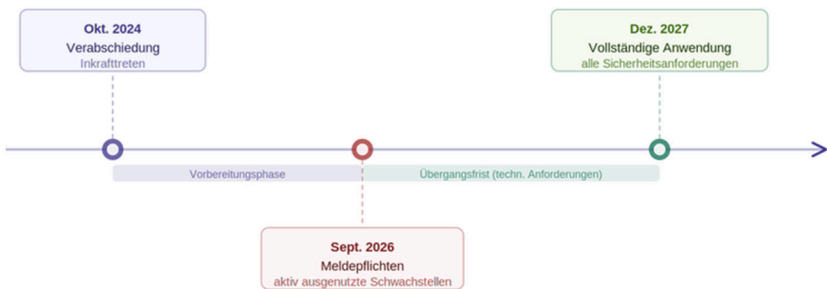
Binnenmarkt und schafft klare Rahmenbedingungen für Hersteller, die ihre Produkte in mehreren Mitgliedstaaten vertreiben.

Der Zeitplan der Regulierung sieht mehrere wichtige Meilensteine vor. Zunächst tritt die Verordnung formell in Kraft, wodurch die grundlegenden rechtlichen Rahmenbedingungen geschaffen werden. In der darauffolgenden Übergangsphase haben Unternehmen Zeit, ihre internen Prozesse zu überprüfen und gegebenenfalls anzupassen. Dazu gehören insbesondere Maßnahmen zur sicheren Produktentwicklung, zum Schwachstellenmanagement sowie zur technischen Dokumentation.

Ein zentraler Bestandteil des Zeitplans betrifft die Einführung von Meldepflichten für Sicherheitsvorfälle und aktiv ausgenutzte Schwachstellen. Hersteller müssen künftig bestimmte Sicherheitsvorfälle innerhalb definierter Fristen an zuständige Behörden melden. Diese Verpflichtungen treten früher in Kraft als einige der weitergehenden Produkthanforderungen, da sie eine zentrale Rolle für die koordinierte Behandlung von Sicherheitsproblemen spielen.

Die vollständige Anwendung der technischen und organisatorischen Anforderungen erfolgt in der Regel erst nach Ablauf einer längeren Übergangsfrist. Diese Phase soll es Unternehmen ermöglichen, bestehende Produkte zu überprüfen, Entwicklungsprozesse anzupassen und notwendige Dokumentationsstrukturen aufzubauen. Besonders für Organisationen mit komplexen Produktportfolios oder langen Entwicklungszyklen kann dies einen erheblichen Anpassungsaufwand bedeuten.

Für Hersteller bedeutet der Zeitplan des Cyber Resilience Act, dass strategische Vorbereitungen frühzeitig beginnen sollten. Viele Anforderungen betreffen grundlegende Entwicklungsprozesse, etwa die Integration von Sicherheitsanalysen, die Verwaltung von Softwarekomponenten oder die Planung von Update-Mechanismen über den gesamten Produktlebenszyklus hinweg. Solche Veränderungen lassen sich in der Regel nicht kurzfristig umsetzen, sondern erfordern eine systematische Anpassung bestehender Strukturen.



Der Cyber Resilience Act wird schrittweise eingeführt. Während einige Meldepflichten bereits früh gelten, erhalten Unternehmen für die vollständige Umsetzung der Sicherheitsanforderungen eine längere Übergangsfrist.

Darüber hinaus sollten Unternehmen die Übergangsfristen nutzen, um ihre organisatorischen Zuständigkeiten zu klären. Fragen der Produktsicherheit betreffen häufig mehrere Bereiche eines Unternehmens, darunter Entwicklung, Qualitätssicherung, IT-Sicherheit,

Abkürzungsverzeichnis

Abkürzung	Bedeutung
API	Application Programming Interface
CERT	Computer Emergency Response Team
CI/CD	Continuous Integration / Continuous Deployment
CRA	Cyber Resilience Act
CVD	Coordinated Vulnerability Disclosure
DoS	Denial of Service
ENISA	European Union Agency for Cybersecurity
EU	Europäische Union
GPL	General Public License
HSM	Hardware Security Module
ICT	Information and Communication Technology
IoT	Internet of Things

Abkürzung	Bedeutung
IT	Information Technology
MIT	Massachusetts Institute of Technology License
NIS2	Network and Information Security Directive 2
OWASP	Open Web Application Security Project
SBOM	Software Bill of Materials
SDL	Secure Development Lifecycle
SIEM	Security Information and Event Management
SOC	Security Operations Center
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UI	User Interface
UX	User Experience
VAPT	Vulnerability Assessment and Penetration Testing
VPN	Virtual Private Network

Literatur- und Quellenverzeichnis

- Bitkom (2025). Leitfaden zur Umsetzung des CRA in KMU: Praktische Checklisten für die Industrie.
- BMDV (2024). Referentenentwurf zur Anpassung des Produktsicherheitsgesetzes (ProdSG) an den Cyber Resilience Act.
- BSI (2025). Anforderungen an Konformitätsbewertungsstellen (KBS) im Rahmen des Cyber Resilience Act. Bundesamt für Sicherheit in der Informationstechnik.
- Bundesnetzagentur (2025). Leitfaden für Wirtschaftsakteure: Marktüberwachungsverfahren nach dem CRA in Deutschland.
- Burri, M., & Zihlmann, Z. (2023). The EU Cyber Resilience Act—an appraisal and contextualization. *Zeitschrift für Europarecht (EuZ)*, 2(2023), B1-B45.
- CEN/CENELEC JTC 13 (2024). Standardization Request M/596 to the European Standardisation Organisations in support of Regulation (EU) 2024/2847.
- CEN/CENELEC (2025). EN 18062: Cybersecurity requirements for products with digital elements.
- Chiara, P. G. (2022). The Cyber Resilience Act: the EU Commission’s proposal for a horizontal regulation on cybersecurity for products with digital elements: An introduction. *International Cybersecurity Law Review*, 3(2), 255-272.
- DigitalEurope (2024). CRA Compliance Handbook: Navigating the transition period.
- ENISA (2025). Technical Guidance on Vulnerability Reporting: Standards and Formats for the CRA Central Repository.

- Europäische Kommission (2024). Leitfaden zur Abgrenzung zwischen dem Cyber Resilience Act und der Funkanlagenrichtlinie (Delegierte Verordnung 2022/30/EU).
- Europäische Kommission (2025). Durchführungsverordnung (EU) 2025/XXX zur Festlegung technischer Spezifikationen für die Software-Stückliste (SBOM) gemäß Verordnung (EU) 2024/2847.
- Europäische Union (2024). Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 10. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Cyber Resilience Act). Amtsblatt der Europäischen Union, L-Serie.
- Heise Online (2024). Cyber Resilience Act final verabschiedet: Was Hersteller jetzt tun müssen.
- ISO/IEC (2024). ISO/IEC 5259-1: Data quality for AI and ML – Part 1: Overview and terminology.
- Meagher, H., & Dhirani, L. L. (2023). Cyber-resilience, principles, and practices. In *Cybersecurity vigilance and security engineering of internet of everything* (pp. 57-74). Cham: Springer Nature Switzerland.
- Mueck, M., Roberts, T., Du Boispéan, S., & Gaie, C. (2025). Introduction to the european cyber resilience act. In *European Digital Regulations* (pp. 91-110). Cham: Springer Nature Switzerland.
- Noerr, White & Case (2025). Joint Analysis: Liability Risks under the Cyber Resilience Act.
- Open Source Initiative (OSI). (2024). The Impact of the Final CRA on Open Source Development – A Summary for Maintainers.
- Schmittner, C., Veledar, O., Faschang, T., Macher, G., & Brenner, E. (2024, September). Fostering cyber resilience in Europe: an in-depth exploration of the cyber resilience act. In *European Conference on Software Process Improvement* (pp. 390-404). Cham: Springer Nature Switzerland.

Stichwortverzeichnis

A

Abhängigkeit.....	7
Angriffsfläche.....	75
Architektur.....	81
Audit.....	142
Ausnahme.....	32
Authentifizierung.....	75
Autorisierung.....	75

B

Bedrohung.....	10
Bedrohungsmodellierung.....	78
Behörde.....	156
Benutzerfreundlichkeit.....	118
Betriebssystem.....	24
Binnenmarkt.....	9

C

CE-Kennzeichnung.....	129, 137
Cloud.....	7, 30
Code Review.....	98
Codeanalyse.....	76
Compliance.....	18, 131

Continuous-Integration-System.....	103
Coordinated Vulnerability Disclosure.....	114
CRA.....	2
CVD.....	114
CVSS.....	67
Cyber Resilience Act.....	2
Cyberangriff.....	1
Cybersecurity-Strategie.....	6
Cybersicherheit.....	8

D

Denial-of-Service.....	149
Designentscheidung.....	84
Digitale Transformation.....	1
Digitales Produkt.....	24
Distributor.....	46
Dokumentation.....	69, 127
Dokumentationspflicht.....	8

E

Einsatzbereich.....	62
Einstufung digitaler Produkte...	63

Entwicklungsphase	88
EU Cybersecurity Regulatory Landscape	11
Europäische Union	5

F

Firewall	37
Firmware	24
Fortschrittsmessung.....	191
Funktionsumfang.....	6
Fuzzing.....	102

G

Gap-Analyse.....	175
Geltungsbereich.....	23
Gesellschaft.....	9
Governance	168

H

Händler	46
Hardwareprodukt.....	28
Hersteller	40
Herstellerverantwortung	41
Hybrides Produkt	37

I

IEC 62443.....	188
----------------	-----

Implementierung	175, 185
Importeur	43
Incident Response	155
Incident-Response-Prozess.....	162
Informationssicherheit.....	18
Inkrafttreten.....	14
Internet of Things	28
IoT.....	28
ISO 27001	188
IT-System	7

K

Kennzahl.....	191
Klassifizierung.....	55, 68
KMU.....	17
Kommunikation	30, 121
Kommunikationsstruktur	170
Komplexität.....	63
Konformitätsbewertung..	127, 135
Kontinuierliche Verbesserung ..	76
Kostenoptimierung.....	6

L

Lebenszyklus.....	31
Lieferkette	51

M

Management.....	170
Managementsystem.....	172
Marktüberwachung	140
Meldepflicht	8, 151
Meldung	42

N

Netzwerkverbindung	28
NIS-2	11, 188

O

Ökosystem.....	1
Open Source	7, 48

P

Patch-Management	117
Penetrationstest.....	133
Plattform.....	7
Produktarchitektur	38
Produkteinstufung	60
Produktentwicklung.....	74
Produktkategorie.....	61
Produktlebenszyklus.....	123
Produktsicherheit.....	53, 180
Produktverantwortung	17
Programmierpraktik.....	95

Q

Qualifikation.....	97
Qualitätsmanagement.....	18, 173
Qualitätssiegel	140

R

Regulierung.....	2
Reifegradmodell	186
Risikoanalyse	58, 80
Risikobewertung.....	64
Risikopotenzial.....	55
Rolle.....	39
Router.....	37

S

SBOM	49
Schulung	178
Schwachstelle	30
Schwachstellenmanagement	8, 41, 66, 109
SDL	93
Secure Development Lifecycle	88, 93
Security by Default.....	73
Security by Design	73
Sensibilisierung	180
Sicherheitslücke.....	50, 119

Sicherheitsnachweis.....	133
Sicherheitspolitik	8
Sicherheitsproblem	1
Sicherheitsprüfung	101
Sicherheitsscan.....	133
Sicherheitstest	76, 101
Sicherheitsvorfall.....	147
Simulation	180
Software	24
Software Bill of Materials.....	49
Softwareentwicklung.....	48, 91
Softwareprodukt.....	27
Sonderregelung	34
Standardkonfiguration	84
Systemarchitektur.....	76

T

Transparenz.....	11, 52
------------------	--------

U

Umsetzung	167
Unternehmensnetzwerk.....	35
Update.....	6, 57
Update-Management	117

V

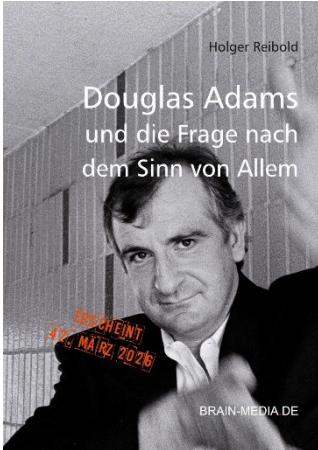
Vernetzung	30, 62
Vulnerability Management	110

W

Wirtschaft.....	8
-----------------	---

Z

Zeitplan	15
Zero-Day-Schwachstelle	120



42 – Douglas Adams und die Frage nach dem Sinn von Allem

Am 11. Mai 2026 ist Douglas Adams 25 Jahre tot. Der Kultautor hat der Welt wunderbar, skurrile Werke geschenkt. Jetzt ist es an der Zeit, den Autor kennenzulernen.

Umfang: 140 Seiten

Preis: 14,99 EUR

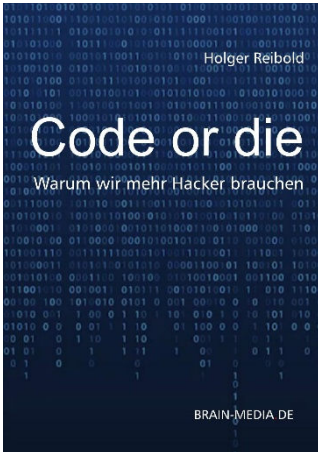
Erscheint: 42. März 2026



Towelday, das ultimative Handtuch für alle Fans

An seinem Todestag, dem Towelday, erinnern sich Fans an Douglas Adams und huldigen dem Kultautor.

100 % intergalaktisch geprüfte Baumwolle, nachhaltig Produktion zum Preis von 42 EUR.



Code or die – Warum wir mehr Hacker brauchen

Ein Manifest für mehr digitale Selbstbestimmung, Neugierde und Eigenverantwortung. Medienkompetenzen alleine genügen nicht; die Gesellschaft von morgen braucht Digitalkompetenzen.

Umfang: 120 Seiten

Preis: 14,99 EUR

Erscheint Frühjahr 2026



Lokale KI – Sichere Architektur, Betrieb und Governance von GenAI- und RAG-Systemen

RAG- und LLM-Plattformen mit klarer Architektur, Guardrails, Monitoring und Governance kontrolliert und resilient betreiben.

Umfang: 270 Seiten

Preis: 24,99 EUR



Brain-Media KaaS

Individual

Business

Enterprise

– die E-Book-Flatrate –

Brain-Media.de ist ein **Pionier** in Sachen E-Book-Flatrates. Bereits 2014 wurden mit Plus+ E-Books als attraktives und preisgünstiges Abo angeboten. Im April 2026 erlebt Plus+ eine Renaissance.

Abonnenten erhalten **1 Jahr Zugriff auf alle E-Books**, die bereits erschienen sind, und auf alle Neuerscheinungen des Abozeitraums. Sie können über 30 verfügbare E-Books herunterladen – dazu editierbare Checklisten, Vorlagen, Beispiele etc. Sie können die E-Books ausdrucken und auf mehreren Lesegeräten verwenden. Die Inhalte werden kontinuierlich an die Dynamik der Entwicklung angepasst.

Und das alles zum **unschlagbaren Sonderpreis!**