



**Positionspapier
Cyber Resilience Act und technischen Richtlinie (BSI-TR-03183)
über horizontale Cybersicherheitsanforderungen für Produkte
mit digitalen Elementen (Cyberresilienz-Verordnung)**

PMeV – Positionspapier

Erstellt vom
Arbeitskreis Cybersicherheit des PMeV
Version 1.0 / Stand 25.09.2026

Inhalt

1. Einleitung	3
2. Ziel dieses Dokumentes	3
3. Spannungsfelder CRA.....	3
3.1. CRA - Artikel 13 Pflichten der Hersteller (Dokumentenverwahrung).....	3
3.2. CRA - Artikel 14 Meldepflichten der Hersteller	4
3.3. CRA - Artikel 24 Pflichten der Verwalter quelloffener Software und 25 Sicherheitsbescheinigung für freie und quelloffene Software	6
3.4. CRA - Artikel 33 Unterstützungsmaßnahmen für Kleinstunternehmen sowie kleine und mittlere Unternehmen, einschließlich Start-up-Unternehmen	7
3.5. CRA – Kapitel IV NOTIFIZIERUNG VON KONFORMITÄTSBEWERTUNGSSTELLEN	8
4. Spannungsfelder BSI-TR-03183	8
4.1. BSI-TR-03183 – Sprache des Dokumentes	Fehler! Textmarke nicht definiert.
4.2. BSI-TR-03183-2 – SBOM – als Beispiel rechtsverbindlicher Aussagen	8
5. Fazit und Ausblick.....	9

Hinweis zu dieser Veröffentlichung

Technische, organisatorische und wirtschaftliche Faktoren können dazu führen, dass die in diesem Positionspapier getroffenen Einschätzungen künftig einer Anpassung bedürfen.

Der PMeV betont, dass die dargestellten Positionen einem fortlaufenden Diskurs unterliegen und bei veränderten Rahmenbedingungen angepasst bzw. aktualisiert werden können.

Der PMeV lädt Stakeholder aus Industrie, Politik und öffentlicher Verwaltung herzlich ein, sich im Wege einer Mitgliedschaft im Verband an der Arbeit und den Entscheidungsprozessen im Arbeitskreis Cybersicherheit zu beteiligen.

1. Einleitung

Die zunehmende geopolitische Dynamik hat den Gesetzgeber auf Bundes- und EU-Ebene dazu veranlasst, Cybersicherheit als zentralen Erfolgsfaktor für die Volkswirtschaft zu stärken. Die Schaffung eines effizienteren Rechtsrahmens für mehr Cybersicherheit begrüßt der Arbeitskreis Cybersicherheit des PMeV ausdrücklich. Der CRA bietet die große Chance, europaweit einen kohärenten Ansatz zu etablieren, regulatorische Lücken in der digitalen Wertschöpfungskette zu schließen und widersprüchliche Vorgaben abzubauen.

Dabei eröffnet dieser regulatorische Rahmen gleichzeitig enorme Chancen, das Vertrauen in digitale Infrastrukturen nachhaltig zu festigen und die Wettbewerbsfähigkeit des europäischen Standorts durch vorbildliche Sicherheitsstandards international auszubauen. In der praktischen Umsetzung zeigt sich zugleich, dass angesichts der hohen Innovationsgeschwindigkeit der IT-Branche sowie der Vielfalt bestehender technischer Standards eine flexible und praxisnahe Ausgestaltung der Regelungen von besonderer Bedeutung ist und sich hieraus für die Praxis entsprechende Herausforderungen im Sinne von Spannungsfeldern ergeben können. Mit dem nötigen Augenmaß gelingt es hierbei, gesetzliche Anforderungen und unternehmerische Innovationskraft erfolgreich miteinander zu verzahnen.

.

2. Ziel dieses Dokumentes

Dieses Dokument will anhand einer Auseinandersetzung mit dem aktuellen Cyber Resilience Act und der daraus in Deutschland entwickelten technischen Richtlinie (BSI-TR-03183) dazu beitragen, sinnvolle Umsetzungsstrategien zu beleuchten. Die Strategien sollen die Bedürfnisse der Industrie nach vollziehbaren Maßnahmen und minimierter Bürokratie berücksichtigen.

Im Einzelnen:

3. Spannungsfelder CRA

Nachstehend werden in der gebotenen Kürze die aus Sicht des PMeV bestehenden Spannungsfelder dargelegt.

3.1. CRA - Artikel 13 Pflichten der Hersteller (Dokumentenverwahrung)

Im Gesetz wurde anlehnend an andere Industrien (z.B.: Dokumentenverwahrung in der Betriebswirtschaft) eine Verwahrungspflicht für alle möglichen Objekte von 10 Jahren eingebaut.

z.B. **Artikel 13 Abs. 9:**

„(9) Die Hersteller gewährleisten, dass jede Sicherheitsaktualisierung gemäß Anhang I Teil II Nummer 8, die den Nutzern während des Unterstützungszeitraums zur Verfügung gestellt wurde, nach ihrer Bereitstellung für mindestens zehn Jahre oder für die verbleibende Dauer des Unterstützungszeitraums, je nachdem, welcher Zeitraum länger ist, verfügbar bleibt.“

Eine Bereitstellung von Sicherheitsupdates über einen so langen Zeitraum von 10 Jahren wirft in der Praxis einige Fragen auf. Ein solcher Zeitraum führt leicht dazu, dass Nutzer deutlich länger als ratsam auf einer bereits veralteten Softwareversion verbleiben, anstatt rechtzeitig auf aktuelle

Versionen zu aktualisieren. Aus Sicherheits- und Produktsicht wäre es daher sogar kontraproduktiv, den Betrieb veralteter Versionen über Jahre hinweg offiziell zu unterstützen. Um hier zu einer wirklich praktikablen und zeitgemäßen Einordnung zu gelangen, lohnt sich ein Blick auf bewährte Standards und Lebenszyklen in anderen IT-Bereichen.

Beispiele sind:

- Bei aktuellen AfA Tabellen bezüglich Software und Hardware findet im Gegensatz zum obigen Ansatz eine gegenläufige Entwicklung statt. Die Abschreibungszeiträume (also der Zeitraum des Wertverlustes auf „0“-Wert der Hardware und Software) sind von drei Jahren auf ein Jahr reduziert worden.
- Security Support für den sogenannten Long Term Support (LTS) freier Linux Betriebssysteme ist auf fünf Jahre beschränkt (z.B. ubuntu oder Debian).
- Im Bezahlbereich von Linux-Betriebssystemen (z.B. RedHat oder SUSE) bieten Anbieter längere Laufzeiten 10-13 Jahre an.
- VMWare bietet als Beispiel für einen Hypervisor für die jeweilige Version 5 Jahre LTS und einen zweijährigen low level Support ohne echte Security Patches an.
- Zuallerletzt diskutiert die Politik aktuell auch die Verwahrungspflichten für Rechnungen von zehn auf sieben Jahre zu reduzieren., um den damit verbundenen Verwaltungsaufwand zu reduzieren.

Vor dem Hintergrund dieser etablierten IT-Praktiken erscheint der Zeitraum von zehn Jahren daher als deutlich zu lang bemessen. Es empfiehlt sich hier, die Fristen noch einmal passgenau an die realen Gegebenheiten des Marktes anzupassen.

Fazit Kapitel Verwahrungsdauer:

Die geplanten Verwahrungszeiten sollten noch einmal auf den Prüfstand. Sie entsprechen weder den aktuellen Entwicklungen der Verwahrungspflichten in anderen Bereichen noch den meisten gelebten Lebenszyklen in der IT. Dabei sollte zusätzlich berücksichtigt werden, dass die Verwahrungszeiten auch einen erheblichen zusätzlichen Energieverbrauch darstellen, da die betroffenen Softwaremodule und Dokumente auf Servern und in Backups dauerhaft aktiv gespeichert werden müssen.

3.2. CRA - Artikel 14 Meldepflichten der Hersteller

In Artikel 14 Abs. 1 heisst es:

*„(1) Ein Hersteller meldet jede aktiv ausgenutzte Schwachstelle, die in dem Produkt mit digitalen Elementen enthalten ist und von der er Kenntnis erlangt, gleichzeitig dem gemäß Absatz 7 als Koordinator benannten CSIRT **und** der ENISA.“*

Die ENISA (European Network and Information Security Agency) wird somit als weitere Meldebehörde bei Cybersicherheitsvorfällen genannt. Deren Single Reporting Platform (SRP) ist im September 2026 an den Start gegangen (siehe <https://digital-strategy.ec.europa.eu/en/policies/cra-reporting> war jedoch bis dato häufig offline). Mit dem 11.

September 2026 werden die neuen Meldepflichten verbindlich, weshalb sich Hersteller ab diesem Zeitpunkt intensiv mit der Meldung von Schwachstellen und Sicherheitsvorfällen auseinandersetzen müssen. Hilfreich zu wissen ist, dass die ENISA als zentrale Instanz vielen Akteuren in der Industrie bisher noch kaum ein Begriff ist, was eine gezielte Aufklärung und Begleitung erfordert.

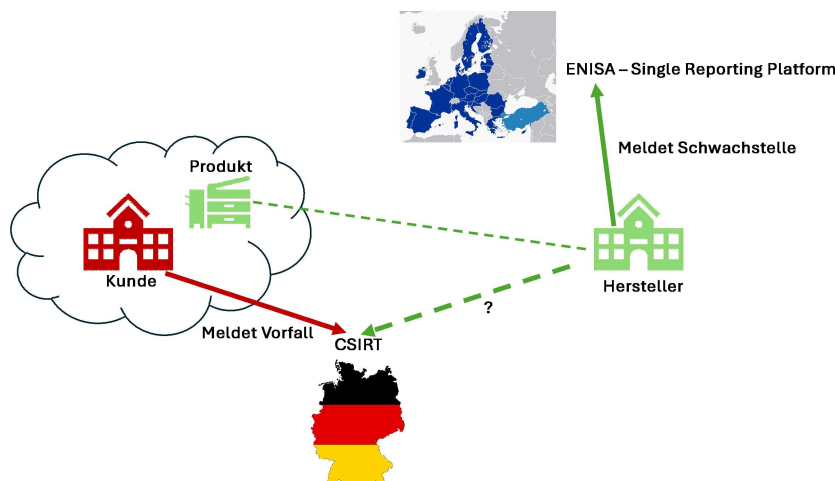


Abbildung 1 Meldevorgänge nach CRA und IT-Sicherheitsgesetz

Wie der Abbildung zu entnehmen ist, sind die CSIRTs entsprechend der einzelnen EU-Länder organisiert, da sie sich mit Angriffen auf KRITIS-Organisationen im eigenen Land auseinandersetzen sollen.

Aus sicherheitstechnischer Sicht ist eine bundeseigene Anlaufstelle zwingend notwendig, da sich Sicherheitsvorfälle in der Regel nicht auf eine einzige Komponente beschränken, sondern Angriffe sich über die betroffene Organisation ausbreiten und die Abwehr der Angriffe unterschiedlichste Maßnahmen erfordern.

Wenn man jetzt den nicht unwahrscheinlichen Fall berücksichtigt, dass der Hersteller von einer Schwachstelle seines Produktes erst durch einen erfolgreichen Hackerangriff auf einen seiner Kunden erfährt, dann stellt sich die Frage, ob der Hersteller oder besser der Kunde das CSIRT unterrichten sollte. Sonst besteht die Gefahr, dass aus dem identischen Vorfall mehrere unabhängige Vorgänge entstehen.

In Deutschland ergibt sich die Herausforderung, dass das aktuell in Deutschland benannte CSIRT das BSI-CERT ist (siehe BSI-TR-03183-3_v1_0_0 Seite 5: „In Germany, the expected designated national CSIRT is the Computer Emergency Response Team for Germany's federal authorities (CERT-Bund)“).

Das CERT beschäftigt sich aber in der derzeitigen Ausprägung fast ausschließlich mit Vorfällen bei Behörden („Die Dienstleistungen von CERT-Bund stehen in erster Linie den Bundesbehörden zur Verfügung“ – siehe

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html).

Geplante Melde-Portale sind noch nicht umgesetzt, bzw. deren Status ist für Außenstehende ungewiss.

Siehe <https://wid.cert-bund.de/portal/wid/fragenundantworten>

„Warum kann ich mich nicht registrieren?“

In einer strategischen Entscheidung hat sich das Bundesamt für Sicherheit in der Informationstechnik (BSI) dazu entschieden, den Betrieb des ehemals auf Basis von individueller Entwicklung realisierten Warn- und Informationsdienst künftig an einen externen Dienstleister zu übergeben. Hiermit gehen verschiedene Änderungen der Rahmenbedingungen einher, weshalb der Zugriff auf den passwortgeschützten Bereich der Webseite derzeit nur Mitarbeitenden der Bundesverwaltung gestattet ist. Das BSI ist dennoch an der Resonanz aller Zielgruppen interessiert und wird die Rückmeldungen bei den weiteren Entscheidungen zur zukünftigen Ausrichtung dieses Portals berücksichtigen.“

Somit haben Hersteller von Hard- und Software für Meldungen im Rahmen des CRA aktuell keine offizielle Anlaufstelle in Deutschland. oder auf europäischer Ebene.

Komplizierend kommt hinzu, dass entgegen der Interpretation im aktuellen BSI-TR-03183-3_v1_0_0 („Commonly, the notifications are sent by the manufacturer to one of the national CSIRTs **or** to the European Union Agency for Cybersecurity (ENISA)¹⁴ and are non-public.“) das Gesetz eindeutig aussagt, dass Hersteller beide Organisationen (lokales CSIRT **und** die ENISA) gleichzeitig informieren müssen (siehe Anfang des Kapitels).

Fazit Kapitel Meldepflichten:

Um den betroffenen Unternehmen – also allen Betrieben, die Software entwickeln oder in Verkehr bringen – eine gute Orientierung und Rechtssicherheit zu geben, wäre es sehr hilfreich, die Prozessvorgaben und die zuständigen Stellen in Deutschland (insbesondere das CSIRT) noch klarer zu definieren. Da die Meldepflichten am 11. September 2026 angelaufen sind und die EU-Plattform zu diesem Zeitpunkt bereitgestellt wurde, wäre es nun ein wichtiger Schritt, auch für Deutschland zeitnah alle notwendigen Informationen bereitzustellen, um einen reibungslosen Übergang für alle Beteiligten zu unterstützen.

3.3. CRA - Artikel 24 Pflichten der Verwalter quelloffener Software und 25 Sicherheitsbescheinigung für freie und quelloffene Software

In diesen Paragraphen wird versucht, Open Source-Projekte unter die allgemeinen gesetzlichen Vorgaben zu stellen. Dabei unterscheidet sich Open Source-Software grundlegend von Modellen in anderen Industrien: Sie wird in der Regel kostenfrei bereitgestellt, und gängige Lizenzen (ob Copyleft oder permissiv) schließen jegliche Haftung von vornherein aus, weshalb die Nutzung in der Verantwortung des Anwenders liegt. Zudem zeichnen sich Open Source-Projekte durch eine enorme Vielfalt aus – das Spektrum reicht von engagierten Einzelpersonen bis hin zu großen Organisationen mit Tausenden Beteiligten, entsprechend unterschiedlich fallen auch die Sicherheitsstrukturen aus. Ein weiterer wichtiger Aspekt ist, dass viele große Projekte außerhalb Europas beheimatet sind und sich daher nur sehr eingeschränkt direkt über EU-Vorgaben regulieren lassen.

Aus den aktuellen Formulierungen geht leider nicht hervor, warum Open Source-Entwickler den Aufwand der EU-Regulierung auf sich nehmen sollten, anstatt im Zweifel schlicht die Distribution ihrer Software im EU-Raum einzustellen – ein Schritt, der für den europäischen Innovationsstandort einen enormen Verlust bedeuten würde.

Hinzu kommt ein wichtiger Punkt bezüglich der Vergangenheit: Viele frühere EU-Forschungsprojekte waren sogar ausdrücklich an die Bedingung geknüpft, die Ergebnisse als Open Source bereitzustellen. Damals lag der Fokus dieser Projekte meist auf der Funktionalität und nicht auf maximaler Enterprise-Security. Ein Großteil dieser Software steht daher zwar als Open Source zur Verfügung, wird aber schon lange nicht mehr aktiv gepflegt, da diese Projekte beendet sind und jegliche Mittel für die Weiterentwicklung fehlen. Für diese Software gibt es weder Verantwortliche noch Ansprechpartner, sodass die neuen Anforderungen bei dieser Art von Open Source-Software kaum umgesetzt werden können.

Fazit Kapitel quelloffene Software:

Die Konsequenzen der Regulierungen im Open Source-Bereich werfen in der Praxis noch einige Fragen auf. Reine Open Source-Projekte erzielen keine Einnahmen durch die Bereitstellung ihrer Software und könnten ihre Angebote für den EU-Raum daher ohne wirtschaftliche Nachteile einschränken oder einstellen. Ein solcher Schritt würde den aktuellen Bestrebungen zur Stärkung unserer digitalen Souveränität – wie sie beispielsweise mit openDesk (<https://www.opendesk.eu/de>) vorangetrieben werden – vor große Herausforderungen stellen.

Um das gemeinsame Ziel des Gesetzes optimal zu erreichen, wäre ein partnerschaftlicher Ansatz denkbar: Wichtigste Open Source-Projekte könnten gezielt motiviert und unterstützt werden. Eine solche Unterstützung muss dabei keineswegs zwingend in finanziellen Zuwendungen bestehen; sie lässt sich auch durch praktische Hilfe bei der Weiterentwicklung realisieren – etwa durch Bereitstellung von Serverkapazitäten, Entwicklungsressourcen oder auch durch tatkräftige, unentgeltliche Unterstützung bei Sicherheitsmaßnahmen und Zertifizierungsprozessen.

3.4. CRA - Artikel 33 Unterstützungsmaßnahmen für Kleinunternehmen sowie kleine und mittlere Unternehmen, einschließlich Start-up-Unternehmen

Nach dem aktuellen Stand erhalten KMUs und Startups leider noch keine spürbaren Erleichterungen bei den eigentlichen Auflagen; die vorgesehenen Maßnahmen beschränken sich bislang vor allem auf Hilfe bei der Dokumentation und Zertifizierung. Um gerade kleinere Unternehmen und innovative Gründer effektiv zu unterstützen, wäre hier eine noch passgenauere Entlastung bei den inhaltlichen Vorgaben ein echter Gewinn.

Fazit Kapitel KMU und Startups:

Für KMUs sowie Startups stellen die neuen regulatorischen Anforderungen eine hohe Hürde dar – sowohl in finanzieller und prozessualer Hinsicht als auch beim erforderlichen Fachwissen. Insbesondere die notwendigen Security-Prüfungen erfordern in der Praxis fast immer den Einsatz von kostenpflichtigen Spezialwerkzeugen, was für Gründer eine erhebliche Dauerinvestition bedeuten kann. Ohne eine beträchtliche Starthilfe wird es für

junge Unternehmen dadurch schwierig, ihr Geschäftsmodell überhaupt erst auf den Markt zu bringen.

Daher schlagen wir vor, für KMUs und Startups pragmatische und konkrete Erleichterungen zu schaffen: Dies betrifft insbesondere technische Vereinfachungen bei den Nachweisen im Anforderungsmanagement, bei Build-Systemen, Security-Checks und Aufbewahrungsfristen. Ein Lösungsansatz wäre hier beispielsweise, dass die Marktüberwachungsbehörden Open Source-Komponenten für eine Build-Chain gezielt unterstützen und zertifizieren, um kleinere Akteure spürbar zu entlasten.

3.5. CRA – Kapitel IV NOTIFIZIERUNG VON KONFORMITÄTBEWERTUNGSSTELLEN

Gemäß der Vorgaben müssen bis 11. Dezember 2026 eine ausreichende Anzahl an notifizierten Stellen in der EU vorhanden sein. In Deutschland ist derzeit geplant, dass das BSI als zentrale Marktüberwachungsbehörde agieren wird und dementsprechend die notifizierten Stellen ernennt.

Fazit Kapitel Notifizierung:

Da es derzeit noch keine benannten Stellen und keine offiziell etablierte Marktüberwachungsbehörde gibt, lassen sich die künftigen Zertifizierungskosten leider noch nicht verlässlich einschätzen. Abgesehen von den festgelegten Strafandrohungen fehlt Herstellern damit momentan die nötige finanzielle und zeitliche Planungssicherheit.

Anders als bei klassischen CE-Zertifizierungen – wo es seit Jahren etablierte und klar messbare Vorgaben (etwa für elektromagnetische Abstrahlungen) gibt – ist im IT-Security-Bereich ein deutlich größerer, individueller Spielraum zu erwarten. Da Kriterien stark von der Programmiersprache, den Produktspezifikationen und der Betriebsumgebung abhängen, lassen sie sich oft nur schwer objektiv in feste Messvorgaben gießen. Auch die Erfahrung mit bisherigen Sicherheits-Zertifizierungen (wie dem Evaluation Assurance Level) zeigt, dass diese im realen Betrieb leider oft nicht zu dem gewünschten spürbaren Sicherheitsplus geführt haben.

Damit dieser wichtige Prozess nicht zu unnötigen Reibungsverlusten für alle Beteiligten führt, könnte die Durchführung eines praxisnahen Piloten angedacht werden. Ein solcher Testlauf – gemeinsam getragen von der künftigen Marktüberwachungsbehörde und starken Industrievertretern und Verbänden – bietet die Chance, ein schlankes und funktionierendes Verfahren zu entwickeln. Auf diese Weise könnte gemeinsam sichergestellt werden, dass der Ansatz am Ende effizient ist und auch für KMUs finanziell gut gestemmt werden kann.

4. Spannungsfelder BSI-TR-03183

4.1. BSI-TR-03183-2 – SBOM

Das BSI-TR-03183 definiert selbst, dass sie nur als Richtlinie zu verstehen ist und eine Einhaltung der Richtlinie nicht gleichzeitig Konformität zu oder Einhaltung des Gesetzes bedeutet:

- „This document can be used as*
- a collection of information for manufacturers about the CRA;*

- *a platform for feedback for the CRA implementation and to support CRA standardisation;*
- *an entry into the CRA and a guideline to prepare for manufacturers without sufficiently structured security-by-design and vulnerability handling processes.*

This document does NOT

- **establish any obligations on manufacturers;**
- **grant presumption of conformity for essential cybersecurity requirements of the CRA when applied;**
- always reflect the current state of standardisation contents;
- describe the only way to be address the CRA.”

Trotzdem werden in dem Dokument technisch verbindliche Forderungen (MUST) aufgestellt. Siehe hier:

“A newly generated or updated SBOM **MUST** be in JSON- or XML-format and a valid SBOM according to one of the following specifications in one of the specified versions:

- CycloneDX9, version 1.6 or higher
- System Package Data Exchange (SPDX)10, version 3.0.1 or higher

Only officially released versions of these specifications MUST be used.”

Diese Vorgehensweise konterkariert die Aussage, dass die TR nicht als verbindliche Vorgabe dient, bzw. eine Einhaltung der technischen Richtlinie eine rechtssichere Umsetzung darstellt.

Die Nutzung von MUST in einem englischsprachigen Dokument oder Vertrag bezeichnet Themen, die als zwingend notwendig ohne Alternative einzuhalten sind.

Fazit Kapitel SBOM:

Im Gegensatz zur ursprünglichen Definition enthält die Technische Richtlinie an einigen Stellen sehr konkrete und verbindliche Vorgaben – unter anderem bei technischen Details wie den SBOM-Formatspezifikationen. Da sich dieser Bereich technologisch rasant und kontinuierlich weiterentwickelt, empfiehlt sich hier ein etwas flexiblerer und offenerer Ansatz (beispielsweise durch den Einsatz von „SHOULD“ anstelle von starren „SHALL“-Regelungen). Andernfalls besteht das Risiko, dass die Einhaltung der Richtlinie nicht mehr dynamisch an den eigentlichen Stand der Technik gekoppelt ist, sondern stattdessen unnötig starr vom zeitlichen Änderungsdienst der Richtlinie abhängt.

5. Fazit und Ausblick

Grundsätzlich werden aus Sicht des PMeV Arbeitskreises Cybersicherheit die Ziele des Cyber Resilience Act voll und ganz unterstützt. Uns kommt es nun vor allem darauf an, die Vorgaben gemeinsam so praxisnah wie möglich umzusetzen und offene Fragen schnell zu klären. Ein enger, vertrauensvoller Dialog zwischen Gesetzgeber, Behörden und Industrie hilft dabei, für die Spannungsfelder maßgeschneiderte Lösungen zu finden. So gelingt es uns verlässlich, die Cybersicherheit effektiv zu stärken und gleichzeitig die Innovations- und Wettbewerbsfähigkeit der europäischen IT-Industrie zu unterstützen.