bitkom

# Stellungnahme

November 2024

# BSI TR-03183: Cyber-Resilienz-Anforderungen

## Allgemeiner Teil

Mit der geplanten Technischen Richtlinie (TR) 03183 möchte das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Hersteller dabei unterstützen, sich frühzeitig auf die Anforderungen des Cyber Resilience Act (CRA) vorzubereiten, der am 20. November 2024 in Kraft getreten ist. Bitkom begrüßt den proaktiven Ansatz, Unternehmen in Vorbereitung auf den CRA eine Orientierung bieten zu wollen, und schätzt die Möglichkeit, durch eine Kommentierung zu der Zielsetzung beizutragen.

Die Veröffentlichung einer TR ist grundsätzlich ein hilfreiches Instrument, um Standards auf nationaler Ebene zu setzen. Dennoch wäre es in diesem Fall für den Markt zielführender, wenn das BSI durch die Wahl eines anderen Dokumententyps signalisieren würde, dass dieser Prozess lediglich als unverbindliche Hilfestellung im europäischen Kontext gedacht ist. In Anbetracht der EU-weiten Standardisierung, die derzeit im Rahmen der CEN/CLC/JTC 13/WG 9 und weiteren Technischen Komitees von CEN, CENELEC und ETSI entwickelt wird, scheint die TR stattdessen die bestehenden Bemühungen mit einem nationalen Alleingang ergänzen zu wollen. Der Bitkom betont jedoch die Bedeutung der fortschreitenden Entwicklung von harmonisierten europäischen Normen (hEN) durch CEN, CENELEC und ETSIETSI, da diese langfristig als Grundlage für eine „Presumption of Conformity“ gemäß Artikel 27 des CRA dienen werden.

Für Hersteller stellt sich durch ein weiteres nationales Dokument die Frage, welchem Standard sie folgen sollen, insbesondere da die ETSI EN 303 645 bereits eine gute Grundlage für technische Anforderungen bietet und in vielen Fällen Anwendung findet. Ebenso wird die EN 18031 (RED-DA) als Basis für die harmonisierten CRA-Standards dienen und könnte in bestimmten Fällen verpflichtend sein, etwa bei „internet-connected radio equipment“. In diesem Zusammenhang entsteht das Risiko, dass die TR durch abweichende Anforderungen von den verbindlichen Vorgaben zukünftiger harmonisierter Standards zu zusätzlichem Aufwand für Hersteller führt. Die TR bietet, wie anfangs erwähnt, keine „Presumption of Conformity“ für den CRA

und birgt daher die Gefahr, dass Hersteller ihre Produkte später an die harmonisierten Standards anpassen müssen, um die notwendige Konformität sicherzustellen. Dadurch wird die Rolle der TR als Orientierungshilfe für den Markt geschwächt.

Die TR wirft in ihrer aktuellen Fassung zudem mehrere inhaltliche Fragen auf, auf die wir im weiteren Verlauf dieser Stellungnahme im Detail eingehen werden. Im Hinblick auf die Essential Requirements entsteht der Eindruck, dass ein Assessment nach der TR allein Rechtssicherheit gewährleisten könne, was jedoch nicht zutrifft. Gleichzeitig ist fraglich, ob ein allgemeines Assessment auf einer Ebene formuliert werden kann, die für alle Produktklassen gleichermaßen geeignet ist. Anforderungen wie „Risk assessment“ und „Data minimisation“ verdeutlichen diesen Punkt besonders, da sie einer präzisen und spezifischen Auslegung bedürfen, die sinnvollerweise im Rahmen der Standardisierung erfolgen sollte. Derzeit bietet die TR hier jedoch keine ausreichende Hilfestellung. Eine klare Position des BSI zu diesen Konkretisierungen, die in die Standardisierung eingebracht wird, wäre hilfreich, um den Herstellern verlässliche Orientierung zu bieten.

Eine weitere Schwierigkeit ergibt sich durch die Gefahr einer Übererfüllung der CRA-Vorgaben, die aus den Formulierungen der TR resultiert. Dies betrifft insbesondere Anforderungen wie REQ_ER 5.2 oder die zweiten Assessment-Kriterien. Solche überzogenen Anforderungen könnten die Hersteller unnötig belasten und zu zusätzlichem Aufwand führen, ohne dass dies zur Konformität mit dem CRA notwendig wäre. Um den administrativen und finanziellen Aufwand der Hersteller nicht unverhältnismäßig zu erhöhen, sollte die TR eine sorgfältige Abwägung zwischen den Anforderungen und ihrer Notwendigkeit gewährleisten.

Zudem geht die TR in einigen Bereichen über die eigentlichen Kompetenzen des BSI hinaus. Ein prominentes Beispiel ist die Festlegung des SBOM-Formats, das gemäß Artikel 13 und 24 des CRA der Europäischen Kommission vorbehalten ist. Diese Vorgehensweise wirft die Frage auf, ob die TR zulässige Handlungsspielräume überschreitet und damit eine Abgrenzung der Zuständigkeiten missachtet. Auch die sogenannten „Should“-Anforderungen tragen zur bestehenden Unklarheit bei. Diese Formulierungen erwecken den Eindruck, dass ihre Umsetzung nicht zwingend erforderlich ist, um die Konformität zum CRA zu gewährleisten. Dies könnte bei Herstellern zu Verwirrung führen, da unklar bleibt, wie mit diesen Anforderungen umzugehen ist. In der Praxis könnten solche Anforderungen häufig ohne rechtliches Risiko ignoriert werden, was die Praxistauglichkeit der TR weiter in Frage stellt. Es wäre daher sinnvoll, wenn das BSI hierzu klare Anwendungshinweise bereitstellen würde, um die Unsicherheiten zu reduzieren.

Angesichts der potenziellen Risiken, die durch eine TR entstehen können – wie Verwirrung bei Herstellern, zusätzlicher Aufwand und mögliche Konflikte mit den Vorgaben des CRA –, plädiert der Bitkom dafür, die TR nicht als verpflichtende Vorgabe (Version 1.0) zu veröffentlichen. Stattdessen sollte sie als Best-Practice-Dokument konzipiert werden, das Herstellern eine freiwillige Orientierung bietet, ohne zusätzliche nationale Pflichten aufzuerlegen. Auf Grundlage der vorliegenden Arbeit

kann den Herstellern ein klarer und praxisnaher Leitfaden zur Verfügung gestellt werden. Dieser Leitfaden sollte wesentliche Fragen adressieren, wie etwa:

- Fällt mein Produkt unter den CRA? Welche Kriterien werden dafür angewendet?
- In welche Produktkategorie fällt ein bestimmtes Produkt?
- Welche Methoden zur Konformitätserklärung sind für diese Produktkategorie relevant?
- Wo können akkreditierte Prüflabore für das Assessment der Konformität gefunden werden?
- Welche existierenden Standards können für die Umsetzung des CRA herangezogen werden?
- Welche weiteren Aspekte müssen beachtet werden, um die Konformität mit den Essential Requirements nachzuweisen?
- Wie ist die „remote data processing solution“ aus Anforderungssicht im Kontext des CRA zu behandeln?
- Welchen Spielraum für technische Entscheidungen lässt das Risiko-Assessment im CRA?

Ein solcher Leitfaden würde Herstellern helfen, die Konformität mit dem CRA effizient und rechtssicher zu erreichen, ohne sie mit widersprüchlichen oder übermäßigen Anforderungen zu belasten.

Gleichzeitig möchten wir die Gelegenheit nutzen, konstruktive Anmerkungen zu den Inhalten der vorliegenden TR zu liefern. Unser Ziel ist es, die Inhalte praxisnah auszugestalten und so zu optimieren, dass sie die Anforderungen der Industrie sowie die Vorgaben des CRA bestmöglich vereint. Dabei legen wir besonderen Wert darauf, dass das Dokument den aktuellen Stand der europäischen Standardisierung berücksichtigt und keine unnötigen Abweichungen schafft. Im Folgenden präsentieren wir konkrete Vorschläge, die eine praxisnahe, effektive Grundlage für Hersteller schaffen sollen. Sie sollen nicht nur helfen, die Anforderungen des CRA zu erfüllen, sondern auch die europäische Harmonisierung unterstützen und die Marktzugänglichkeit für Produkte fördern.

# Teil 1 "General Requirements"

## 3.1 Security objectives and scope

Es wird festgelegt, dass die Anforderungen der TR auf alle Produkte mit digitalen Elementen angewendet werden, einschließlich der zugehörigen Remote-Data-Processing-Lösungen. Es wird jedoch darauf hingewiesen, dass eine „remote data processing solution“ gemäß der Definition des CRA ein integraler Bestandteil des Produkts mit digitalen Elementen (PWDE) ist. Eine isolierte Betrachtung des Produkts ohne die Berücksichtigung der Remote-Data-Processing-Lösungen könnte dazu führen, dass Hersteller die spezifischen Anforderungen an diese Lösungen außer Acht lassen, was dazu führen würde, dass das PWDE nicht mehr den Vorgaben des CRA entspricht. Eine ganzheitliche Betrachtung der Produktkomponenten ist daher unerlässlich, um die Konformität mit dem CRA sicherzustellen.

## 4.1 Important Note

Laut der TR ist ein Risiko-Assessment nur für die Implementierungsdetails relevant, nicht jedoch für die Auswahl der umzusetzenden Anforderungen. Diese Einschätzung steht im Widerspruch zum CRA, welcher bei den technischen Produktanforderungen die Formulierung „where applicable“ verwendet, welche in der TR nicht berücksichtigt wird. Ein solches Vorgehen könnte dazu führen, dass Anforderungen aufgestellt werden, die für viele Produkte weder notwendig noch sinnvoll sind. Dies würde nicht nur den praktischen Nutzen der TR infrage stellen, sondern auch Hersteller unnötig belasten, da sie Anforderungen erfüllen müssten, die in ihrem spezifischen Kontext keine Relevanz haben.

## 5.2 Application Guidance

Die Definition und der Umfang dieser beiden Datenarten, nämlich security data und critical security data sind nicht klar festgelegt. Aus der Perspektive der Netzwerksicherheit haben sie jedoch unterschiedliche Auswirkungen auf die Verfügbarkeit, Integrität und Vertraulichkeit. Unklare Definitionen beeinflussen die Art der Daten, die im TOE gespeichert werden sollten.

## 5.3.1.2 REQ_ER 1.2

Es stellt sich die Frage, ob GSMA FS.16 Network Equipment Security Assurance Scheme ebenfalls als Beispiel für Best Practices herangezogen werden könnte.

## 5.3.2 REQ_ER 2

Sollte sichergestellt werden müssen, dass bei der Veröffentlichung keinerlei bekannte Schwachstellen vorhanden sind, einschließlich auch geringfügiger Schwachstellen, wäre dies in der Praxis nahezu unmöglich.

## 5.3.2.1 REQ_ER 2.1

Die Regelung des CRA zielt explizit darauf ab, dass Produkte frei von ausnutzbaren Schwachstellen sein müssen. Der Entwurf des BSI in Abschnitt 5.3.2.1 geht darüber hinaus und fordert die Verwendung der "neuesten verfügbaren Software/Firmware" vor der ersten Nutzung eines Produkts. Dabei wird nicht geprüft, ob durch diese Maßnahme tatsächlich produktrelevante und ausnutzbare Schwachstellen behoben werden.

Es sollte betont werden, dass der CRA bewusst den Fokus auf die Behebung ausnutzbarer Schwachstellen legt. Diese Zielsetzung berücksichtigt die Maßnahmen moderner Sicherheits-Architekturen, die häufig darauf abzielen, Schwachstellen von Unterkomponenten durch Schutzmechanismen oder die Nicht-Nutzung bestimmter Funktionen zu mitigieren. Der Entwurf des BSI hingegen scheint die Funktionsweise solcher Sicherheits-Architekturen zu ignorieren, obwohl sie ein zentraler Bestandteil des aktuellen Stands der Technik sind.

Viele kommerzielle Produkte enthalten Software-Bibliotheken mit allgemeiner Zweckbestimmung, von denen nur ein kleiner Teil des Codes tatsächlich genutzt wird. Funktionen, die von außerhalb des Produkts nicht angesteuert werden können, tragen nicht zur Angreifbarkeit des Produkts bei. Die Forderung des BSI, unabhängig von der Relevanz auf die "neueste verfügbare Version" umzustellen, geht damit an den praktischen Anforderungen und Sicherheitsmechanismen vorbei.

Aus der derzeitigen Formulierung ergeben sich erhebliche Konsequenzen: Hersteller können nicht prüfen, welche Auswirkungen die Nutzung der neuesten Software- oder Firmware-Version auf die Funktionalität und Sicherheit eines Produkts hat. Häufig kann es dazu kommen, dass die aktuelle Software nicht reibungslos mit den verwendeten Applikationen oder Bibliotheken zusammenarbeitet. Insbesondere muss die Interoperabilität in einem Netzsegment gewährleistet werden. Selbst wenn bekannte negative Auswirkungen auftreten, bleibt ihnen in dem derzeitigen Entwurf keine Wahl: Die Nutzung der "letztbekannten brauchbaren Version" wird durch 5.3.2.1 ausgeschlossen.

Um sicherzustellen, dass die Anforderungen des CRA sinnvoll und praktikabel umgesetzt werden, empfehlen wir, die Forderung nach der "neuesten verfügbaren Software/Firmware" in der aktuellen Form zu überdenken. Es können auch ältere Softwareversionen verwendet werden, sofern diese noch supported und die aktuellen Sicherheitspatches verwendet werden. EsEs sollte geprüft werden, ob durch die jeweilige Version tatsächlich sicherheitsrelevante Schwachstellen mit Bezug auf die Nutzung des Produkts behoben werden. Dies würde eine effektivere Balance zwischen Sicherheitsanforderungen und technischer Umsetzbarkeit gewährleisten.

## 5.3.2.2 REQ_ER 2.2

Die im Entwurf des BSI formulierte Anforderung, die sich auf "bekannte, aktiv ausgenutzte Schwachstellen" bezieht, erfordert eine differenziertere Betrachtung. Insbesondere wird nicht spezifiziert, ob diese Schwachstellen die Unterkomponente oder das Produkt selbst betreffen. Es ist jedoch ein grundlegender Aspekt moderner

Sicherheits-Architekturen, dass ein Produkt nicht allein durch die Summe der Schwachstellen seiner Unterkomponenten angreifbar ist. Schutzmechanismen und gezielte Nicht-Nutzung von Teilfunktionen sind hierbei zentrale Elemente, die eine differenzierte Bewertung erfordern.

Ein weiterer kritischer Punkt ist das Fehlen einer klaren Abgrenzung der Testumgebung und der Testszenarien. Die Testbedingungen sollten zwingend mit der vorgesehenen Einsatzumgebung des Produkts abgestimmt werden, um praxisnahe und relevante Ergebnisse sicherzustellen. Die Formulierung im Entwurf lässt jedoch die Gefahr offen, dass Szenarien konstruiert werden, die weit von realistischen Einsatzbedingungen entfernt sind.

Es wird daher empfohlen, die Anforderung dahingehend zu präzisieren, dass sich der Begriff "aktiv ausgenutzte Schwachstellen" ausschließlich auf Schwachstellen bezieht, die in Testergebnissen der vorgesehenen Einsatzumgebung nachgewiesen wurden. Gleichzeitig sollten Tests nur auf die intendierte und vorhersehbare Nutzung des Produkts ausgerichtet sein und keine theoretischen Labor-Szenarien abdecken, die auf unrealistischen Kombinationen von Wissen und Ressourcen beruhen.

Die aktuelle Umsetzung birgt das Risiko, dass auf Basis unrealistischer Szenarien Schwachstellen identifiziert werden, die in der Praxis keine Relevanz besitzen. Dies kann insbesondere durch White-Hat-Hacker genutzt werden, um vermeintliche Sicherheitslücken öffentlichkeitswirksam zu präsentieren. Hersteller wären gezwungen, sich für diese "praktisch unmöglichen" Schwachstellen zu rechtfertigen und unnötige Schutzmaßnahmen umzusetzen, was den Fokus von tatsächlich sicherheitskritischen Maßnahmen ablenkt.

### 5.3.2.3 REC_ER 2.3

Die Empfehlung im Entwurf des BSI, die sich auf "bekannte, ausnutzbare Schwachstellen" konzentriert, bedarf einer präziseren Definition. Es fehlt eine klare Differenzierung, ob die Ausnutzbarkeit durch bekannte oder wahrscheinliche Angriffe die Unterkomponente oder das Produkt selbst betrifft. Wie bereits ausgeführt, reduziert eine wirksame Sicherheits-Architektur die Angreifbarkeit eines Produkts, selbst wenn Schwachstellen in einzelnen Unterkomponenten vorliegen. Diese Differenzierung ist entscheidend, um die tatsächliche Angreifbarkeit des Produkts zu bewerten und den Aufwand für Hersteller realistisch zu halten.

Die Empfehlung sollte klarstellen, dass sich "bekannte, ausnutzbare Schwachstellen" ausschließlich auf Schwachstellen beziehen, die in Bezug auf das Produkt in seiner vorgesehenen Einsatzumgebung relevant sind. Diese Präzisierung würde verhindern, dass Hersteller gezwungen sind, irrelevante oder theoretisch nicht ausnutzbare Schwachstellen zu adressieren.

Die umfangreichen Spezifikationen der BSI TR 03183 in ihrer aktuellen Form bergen die Gefahr einer Über-Allokation von Ressourcen und Maßnahmen. Diese führen dazu, dass Hersteller erhebliche Aufwände in Szenarien investieren müssen, die für die Sicherheit des Produkts in der Praxis keine Rolle spielen. Insbesondere ergeben sich negative Folgen für:

- Kosten: Der erhöhte Aufwand für die Definition, Durchführung und Auswertung von Tests treibt die Entwicklungskosten erheblich in die Höhe.
- Zeit: Die aufwendige Auseinandersetzung mit theoretischen Szenarien verzögert die Markteinführung neuer Produkte.
- Produktqualität und Nutzbarkeit: Eine einseitige Priorisierung von Schutzmaßnahmen zulasten der Funktionalität und Benutzerfreundlichkeit kann zu Einschränkungen in der Bedienbarkeit führen.

## 5.3.3.1 REQ_ER 3.1

Die Anforderung kann beispielsweise nicht auf Telekommunikationsausrüstung angewendet werden, da die Löschung aller lokalen Benutzerdaten katastrophale Folgen für ein Netzwerk haben könnte. Die Formulierung sollte dahingehend geändert werden, dass sie beispielsweise lautet: „Das Netzwerkelement kann in einen stabilen Betriebszustand mit den ursprünglichen Konfigurationswerten zurückversetzt werden."

## 5.3.4.3 REQ_ER 4.3

Die Fähigkeit zur automatischen Aktualisierung vonseiten der Betreiber oder durch vertragliche Vorgaben ist unter anderem bei vielen Telekommunikationsprodukten nicht zulässig. In der Regel kontrollieren die Betreiber, wie und wann Updates durchgeführt werden.

Zudem widerspricht die allgemeine Forderung nach einer standardmäßig aktivierten automatischen Update-Funktion, den im CRA festgelegten Grundsätzen. Der Erwägungsgrund 56 des CRA besagt nämlich Folgendes: "The requirements relating to automatic updates as set out in an annex to this Regulation are not applicable to products with digital elements primarily intended to be integrated as components into other products. They also do not apply to products with digital elements for which users would not reasonably expect automatic updates, including products with digital elements intended to be used in professional ICT networks, and especially in critical and industrial environments where an automatic update could cause interference with operations".

Die im CRA dargelegten Ausnahmen zeigen, dass die generelle Forderung nach einer aktivierten automatischen Update-Funktion nicht für alle Produkte geeignet ist und den spezifischen Anforderungen im Telekommunikationssektor widerspricht. Eine Überarbeitung der Anforderung im Sinne der regulatorischen Vorgaben und der Praxis ist daher notwendig. Dies gilt auch für Anforderung 5.3.4.4.

## 5.3.4.5 REQ_ER 4.5

Im Fall von Telekommunikationsausrüstung ist typischerweise der Betreiber der Nutzer und entscheidet darüber, wann und wie Updates durchgeführt werden. Der Text muss entsprechend angepasst werden, um diesem Umstand Rechnung zu tragen.

## 5.3.7 REQ_ER 7

Die Empfehlungen und Anforderungen scheinen davon auszugehen, dass es sich bei den Produkten um Verbraucherprodukte handelt, bei denen Endnutzern bestimmte Funktionen zur Verfügung stehen, um ihr Produkt zu schützen oder wiederherzustellen. Telekommunikationsprodukte funktionieren jedoch nicht zwingend auf diese Weise. Der Anforderungstext sollte entsprechend angepasst werden, um dies zu berücksichtigen.

## 5.3.9.1 REQ_ER 9.1

In vielen Fällen ist es für zahlreiche Telekommunikationselemente nicht praktikabel, eine funktionierende Standardkonfiguration bereitzustellen. Die standardmäßig verfügbaren Schnittstellen sollten auf ein Minimum beschränkt sein, wobei die Betreiber anschließend angewiesen werden, die Ausrüstung entsprechend ihren Anforderungen zu konfigurieren.

## 5.3.13.3 REQ_ER 13.3

Bezüglich der Anforderung „The TOE MUST have implemented a mechanism to record and monitor the status of all services belonging to the TOE“ stellt sich die Frage, ob damit Funktionen wie das Protokollieren von Ereignissen und Statusänderungen gemeint sind oder ob eine weitergehende Funktionalität verlangt wird.

## 5.3.13.4 REQ_ER 13.4

Dies wird für einige Produkte, beispielsweise im Telekommunikationssegment, nicht möglich sein. Zum Beispiel darf die Deaktivierung der Funktion „Lawful Intercept“ aus rechtlichen Gründen nicht erfolgen. Der Anforderungstext muss dies berücksichtigen.

## 5.3.14 REQ_ER 14

Die Anforderung scheint davon auszugehen, dass es sich bei dem Produkt um eine Anforderung für Endnutzergeräte handelt, was jedoch beispielsweise auf Telekommunikationsprodukte nicht zutrifft. Der Text sollte entsprechend angepasst werden.

## 5.4.2.1 REQ_VH 2.1

Die Anforderung „The manufacturer MUST ensure that identified vulnerabilities are addressed and corrected, i.e. by providing an update or otherwise mitigating a vulnerability, in a timely feasible manner“ setzt voraus, dass alle Schwachstellen schnell adressiert werden. In der Praxis werden jedoch Schwachstellen mit geringer Schwere nicht immer umgehend behoben. Dies sollte im Text entsprechend klargestellt werden.

Die Schwierigkeit dieser Anforderung zeigt sich zudem am Beispiel von Zahlungsverkehrskarten, als nicht-vernetzte digitale Elemente ohne eine permanente

Netzverbindung. Ein Update der Software auf der Karte kann nicht ohne aktive Einbeziehung des Karteninhabers angestoßen werden. Karteninhaber sind heute nicht damit vertraut im Feld (d.h. beim Bezahlvorgang im Geschäft oder am Geldausgabeautomat) solche Updates selbst anzustoßen, noch daran gewohnt, diese in automatischer Form durchzuführen zu lassen. Die heutige technische Infrastruktur im Zahlungsverkehr ist außerdem nicht dafür ausgerichtet, um die nicht permanent verbundenen Zahlungsverkehrskarten im Feld zu aktualisieren und entsprechende Updates bereitzustellen, auch da die Infrastruktur nicht von den Kartenherstellern selbst betrieben wird und damit gesteuert werden kann.

### 5.4.4.1 REQ_VH 4.1

Es muss klargestellt werden, dass die zeitliche Information der Nutzer über Schwachstellen nicht für alle Schwachstellen gelten kann und dass dies insbesondere bei sensiblen Schwachstellen verantwortungsvoll erfolgen muss. Zudem könnte es unverantwortlich sein, öffentlich über Schwachstellen zu informieren, die möglicherweise nicht behoben wurden oder bei denen einige Betreiber die Patches in ihren Netzwerken noch nicht angewendet haben. Der Text sollte diese Sensibilität im Umgang mit der Weitergabe solcher Informationen widerspiegeln.

### 5.4.4.2 REQ_VH 4.2

Die Anforderung „The manufacturer MUST provide the Security Advisories in a machine processable way.“ wirft die Frage auf, ob dies die Verwendung eines bestimmten Formats wie VEX oder eines anderen erfordert.

### 5.4.4.3 REC_VH 4.3

„Common Security Advisory Framework (CSAF)“ ist zu eng gefasst, es sollte daher „Industry best practise“ überlassen werden und eine entsprechende Formulierung verwendet werden.

## Teil 2 "Software Bill of Materials (SBOM)"

### 3.2.1 Component

Der Abschnitt „In the case of compiled code“ spricht über Dateien, die während der Ausführung des Linkers verwendet werden. Bedeutet dies Abhängigkeiten, die zur Bauzeit genutzt werden? Wir sind der Ansicht, dass nicht jedes Mal ein Linker zum Einsatz kommt.

Der Abschnitt „In the case of interpreted code“ impliziert, dass auch Laufzeitabhängigkeiten in das SBOM aufgenommen werden sollten. Dies sollte jedoch nicht der Fall sein, da Abhängigkeiten, die nicht verteilt werden, nicht unter der Kontrolle des Herstellers stehen und daher nicht Teil des SBOM sein sollten (Sie könnten jedoch Teil des SBOM des Betriebssystemanbieters sein).

### 5.2.2 Required data fields for each component

„Data Field: Component version“ liegt nicht in der Verantwortung der Hersteller (die für die Erstellung der SBOMs zuständig sind), sondern der Ersteller, weshalb ein Hersteller das Versionsschema nicht garantieren kann. Üblicherweise wird der Git-Commit-Hash verwendet. Warum ist dies hier nicht zulässig?

### 5.3.1 Additional data fields for the SBOM itself

SBOM-URI: SBOMs sind nicht verpflichtet, veröffentlicht zu werden, daher werden SBOMs nicht automatisch URIs enthalten.

### 6.1.2.2 REQ_TD 2.2

Hier gibt es keine Section 0.

### 8.2.4 Delivery item SBOM

Wir sind der Ansicht, dass ein Lieferobjekt-SBOM keine Komponenten außerhalb der Lieferung enthalten sollte. Diese liegen nicht im Verantwortungsbereich des Herstellers und sollten daher nicht aufgelistet werden.

## Teil 3 "Vulnerability Reports and Notifications"

### 3.1.5 Security advisory

Die Aussage „Commonly, the advisories are sent by the manufacturer to all users of the product and are publicly disclosed“ ist nicht korrekt, da Schwachstellen in der Regel nicht öffentlich bekannt gemacht werden, insbesondere im Telekommunikationsmarkt.

### 4 Cybersecurity requirements for receiving vulnerability reports

Diese Anforderung ist zu restriktiv, da sie einige Schwachstellenmelder davon abhalten könnte, mit Herstellern zusammenzuarbeiten.

### 4.2.1 Roles of responsible cybersecurity contacts

Der Anforderungskatalog geht über die Anforderungen des CRA hinaus und weit in die Selbstbestimmtheit von interner Unternehmensorganisation hinein. Es wäre wünschenswert, dass alternative organisatorische Strukturen, die die angestrebten Sicherheitsziele ebenfalls erreichen könnten, stärker berücksichtigt werden. Die Anforderung, „The manufacturer MUST create two roles of responsible cybersecurity contacts“, wirft zum Beispiel die Frage auf, ob diese beiden Rollen für Backup- oder Redundanzzwecke vorgesehen sind. Der Nutzen von mehr als zwei getrennten

Emailadressen, deren Wortlaut auch noch exakt vorgegeben ist, erscheint nicht unmittelbar ersichtlich, muss sich doch der Hinweisgeber jetzt erst einmal für eine der mehreren Optionen entscheiden.

## 4.3.2 Corresponding CSIRT

Das Erfordernis, alle gültigen Schwachstellen an das BSI bzw. „corresponding CSIRT“ zu melden, ist nicht praktikabel und geht über die Anforderung des CRA hinaus, die aktiv ausgenutzten Schwachstellen zu melden.

## 4.3.5 Guaranteed Response Times

Die vorgegebenen Antwortzeiten auf gemeldete Schwachstellen sollten als Richtlinien- und nicht als Sollwerte formuliert werden. Je nach vermuteter Kritikalität der Schwachstelle müssen diese bei der internen Bearbeitung unterschiedlich priorisiert werden und können entsprechend keine gleichlaufenden Bearbeitungszeiten erfahren.

## 4.3.10 Vulnerability disclosure

Dies stellt eine Offenlegungspflicht für Hersteller dar. Eine pauschale Offenlegung aller Schwachstellen ist jedoch nicht wünschenswert, da dies ein Sicherheitsrisiko darstellt.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.


## Herausgeber

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin



## Ansprechpartner

Felix Kuhlenkamp | Referent Sicherheitspolitik
T 030 27576-279 | f.kuhlenkamp@bitkom.org



## Verantwortliches Bitkom-Gremium

AK Informationssicherheit