# ZVEI-Seiter

# Cyber Resilience Act (CRA)

Angesichts der zunehmenden Fragmentierung der Regulierungslandschaft hinsichtlich Cybersicherheit, ist der ZVEI schon seit langem ein vehementer Befürworter für eine horizontale Produktregulierung im Rahmen des New Legislative Frameworks (NLF)[1]. Daher begrüßen wir den kohärenten Entwurf des Cyber Resilience Acts (CRA) welcher der Logik des NLF folgt. Zwar stellt die Ergänzung von Anforderungen im Lebenszyklus zur Etablierung eines Schwachstellenmanagement-Prozesses eine Erweiterung des NLF über das Bekannte hinaus dar, dies ist in diesem Fall in seiner moderaten Gestaltung jedoch durchaus sinnvoll und begrüßenswert.

## Unsere Positionen

- **Der CRA sollte der zentrale Referenzpunkt für Cybersicherheitsanforderungen für Produkte sein.** Nur mit einem solchen Referenzpunkt, an dem sich das Zusammenspiel mit anderen (sektoralen) Regulierungen ausrichtet, lässt sich Doppelregulierung vermeiden. Hierfür müssen sowohl Anknüpfungspunkte für die Anforderungen aus der neuen Maschinen-Verordnung (Anhang III, Sektion 1.1.9 & 1.2.1) gefunden werden, als auch eine Lösung für die Übergabe zwischen dem delegierten Rechtsakt unter Art. 3(3) d,e,f der Funkanlagenrichtlinie (RED) und dem CRA, z. B. durch eine Rücknahme des delegierten Rechtsaktes.
- **Ausreichend lange Übergangsfristen zur Umsetzung des CRA von mindestens 48 Monaten und eine zielgerichtete Umsetzungsstrategie sind notwendig.** Gerade bei einem neuen Rechtsakt, der ein neues Regelungsziel behandelt und nicht oder nur bedingt auf vorhandene Ergebnisse und Strukturen aufsetzen kann, sind ausreichend langen Fristen wichtig. Ebenfalls helfen kann ein stufenweises Vorgehen nach Kritikalität. Es muss sichergestellt werden, dass alle für die Umsetzung des CRA notwendigen Stellen rechtzeitig ihre Aufgaben erfüllen und Produkte reibungslos in Verkehr gebracht werden können. [2] Dies ist besonders wichtig, da mit der umfassenden Adressierung von (Software-)Schwachstellen ein grundlegend neuer Regulierungsgegenstand eingeführt wurde.
- **Definitionen und der Anwendungsbereich des CRA müssen klar und sinnvoll gewählt sein:** Dabei sollte man sich auf Produkte konzentrieren, die spürbare Auswirkungen auf die Resilienz haben können und in der Lage sind (bi-direktional) Daten auszutauschen. Von zentraler Wichtigkeit ist außerdem eine **Ausnahmeregelung für Ersatzteile**, um die kontinuierliche Nutzung von langlebigen Gütern zu ermöglichen. Fehlende Definitionen müssen ergänzt werden und die Regulierung muss so eindeutig und klar formuliert sein, dass Unklarheiten in der Erarbeitung harmonisierter Europäischer Normen (hEN) und für die Wirtschaftsakteure vermieden werden.
- **Hinsichtlich kritischer Produkte muss ein differenzierter Ansatz gefunden werden**, der die bestimmungsgemäße Verwendung in kritischen Funktionen stärker berücksichtigt. Die derzeitige Klassifizierung ist zu umfangreich und unspezifisch. Sie differenziert außerdem nicht zwischen Komponenten, Produkten und Systemen. Artikel 6 (5) sollte gestrichen werden, da eine gleichwertige Adressierung von hochkritischen Produkten bereits mittels der in Art. 24 (3) beschriebenen Konformitätsbewertungsverfahren unter Einbindung einer Drittstelle erfolgen kann.
- **Die Pflichten der Hersteller und die grundlegenden Cybersicherheitsanforderungen entsprechend Anhang I sollten noch besser verknüpft werden.** Anforderungen an die Auslieferung von Produkten mit Schwachstellen müssen realistisch gestaltet sein und auf Grundlage der Risikobewertung erfolgen. Es muss weiterhin gängige Praxis bleiben können, dass mögliche Schwachstellen mittels entsprechender Prozesse, z. B. durch (initiale) (Security)-Updates bei Inbetriebnahme, behoben werden können.
- **Hinsichtlich der Konformitätsbewertungsverfahren muss der konsistente NLF-basierte Ansatz des CRA weiter gestärkt werden.** Andere Mittel zum Nachweis der Konformität, wie „Common Specifications“ und CSA-Schemata, sollten ähnlichen Verpflichtungen und Qualitätssicherungsmaßnahmen unterliegen wie hEN. Außerdem sollte die Verwendung etablierter internationaler Normen wie der IEC 62443 bei der Entwicklung der hEN ermöglicht werden.
- Mögliche zusätzliche Verwerfungen durch den CRA in bereits angespannten Lieferketten können vermieden werden, indem der **unvollständige Charakter der meisten Komponenten** und ihr bestimmungsgemäßer Gebrauch ausreichend berücksichtigt werden - insbesondere im Hinblick auf ihre Konformitätsbewertung und -prüfung. Eine zusätzliche Entlastung könnte durch die Ausnahme von Komponenten, die nur ein minimales Risiko darstellen, erreicht werden.

[1] Vgl. hierzu auch das entsprechende ZVEI-Whitepaper aus dem Jahr 2018 Horizontale Produktregulierung für Cybersicherheit welches in vielen Aspekten in der Position der deutschen Industrie aufgegangen ist: Europaweite Cyberregulierung

[2] Vgl. Auch das ZVEI-Positionspapier „Funktionsfähiger EU-Binnenmarkt – angemessene Übergangsfristen sicherstellen“: https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2023/Maerz/2023-03-21_Positionspapier_UEbergangsfristen/2023-03-21-Positionspapier-UEbergangsfristen.pdf

- **Die Meldepflichten für Cybersicherheitsvorfälle und Schwachstellen sollten mit den Anforderungen der NIS-2-Richtlinie abgeglichen und an diese angeglichen werden.** Die Anforderungen sollten auf bedeutende Vorfälle mit erheblichen Auswirkungen und aktiv ausgenutzten Schwachstellen zu beschränkt bleiben. Außerdem sollte sich auf bereits etablierte internationale Referenzpunkte und Bewertungssysteme, wie die MITRE-Referenzmethode für "common vulnerabilities and exposures" (CVE) und den CISA "known exploited vulnerabilities catalog" (KEV), bezogen werden.

# Aktueller Sachstand:

- Es existiert eine **komplexe Regulierungslandschaft in Bezug auf Cybersicherheit,** die sich in Regulierungen zu operativer Cybersicherheit im Betrieb und Regulierungen, die sich auf Produkte beziehen, unterteilen lässt. Was die Cybersicherheit von Einrichtungen und Unternehmen anbelangt, so wird die derzeitige Richtlinie über die Netz- und Informationssicherheit (NIS) mit Wirkung vom 18. Oktober 2024 durch die überarbeitete NIS-2-Richtlinie abgelöst. Die Cybersicherheit von Produkten wird aktuell in verschiedenen, meist in Überarbeitung befindlichen, sektoralen Verordnungen im Zusammenhang mit anderen Schutzzielen behandelt (neue Maschinenverordnung; allgemeine Produktsicherheitsverordnung; AI-Act; Entwurf der neuen Produkthaftungsrichtlinie und delegierter Rechtsakt zur Funkanlagenrichtlinie (RED)). Sowohl die Produktregulierungen als auch die NIS-2-Richtlinie haben hierbei Anknüpfungspunkte an den freiwilligen Zertifizierungsrahmen des Cybersecurity Acts von 2019.
- Der **delegierte Rechtsakt unter Art. 3(3) d,e,f der RED spielt eine besondere Rolle**, da sein Anwendbarkeitsdatum, aktuell der 1. August 2024, vor dem des CRA liegt. Somit werden durch den delegierten Rechtsakt für Produkte, die unter die RED fallen, die ersten Cybersicherheitsanforderungen festgelegt.
- Um die komplexe Regulierungslandschaft zu vereinfachen und der weiteren Ausbreitung fragmentarischer Cybersicherheitsanforderungen entgegenzuwirken, hat die Europäische Kommission daher am 15. September 2022 den Entwurf des Cyber Resilience Acts veröffentlicht, der derzeit von den europäischen Co-Gesetzgebern diskutiert wird und noch unter der jetzigen Kommission in Kraft treten soll.

# Hintergrund: Zahlen, Daten, Fakten

- **Kritischer Fachkräftemangel:** Alleine in Deutschland fehlen 100.000 IT-Sicherheits-Experten. Für Europa gehen Schätzungen für den Bereich von ca. einer Million fehlender Fachkräfte aus, da auch andere europäische Mitgliedstaaten ähnliche Bedarfe haben, z. B. Frankreich und Spanien mit jeweils etwa 60.000 fehlenden Fachleuten. Dabei wird der steigende Bedarf durch die bevorstehende Umsetzung der NIS-2-Richtlinie und des CRA noch gar nicht ausreichend mitberücksichtigt.[3]
- **Kontinuierliche Zunahme vernetzter Geräte:** Die Zahl der IoT-Geräte wird in den kommenden Jahren noch weiter ansteigen und im Jahr 2028 voraussichtlich über 30 Milliarden IoT-Verbindungen erreichen, derzeit sind es bereits über 13 Milliarden.[4]
- **Unverändert hohe Bedrohungslage:** Cyberkriminalität ist nach wie vor ein lukratives Betätigungsfeld für Kriminelle und andere böswillige Akteure. Dabei steigt das Bedrohungsniveau, trotz der Bemühungen der nationalen Behörden und der Industrie sowie einer gewissen Sensibilisierung für die Cybersicherheit insgesamt, weiterhin an. So ist z. B. die Zahl der vom BSI registrierten neuen Malware-Varianten um 116,6 Millionen auf über eine Milliarde angestiegen.[5] Auch gab es im letzten Jahr den größten Denial of Service-Angriff (DDoS), der jemals in Europa gestartet wurde.[6] Bei diesen Angriffen war weiterhin der Trend zu erkennen, dass solche Attacken häufig von kompromittierten Servern oder Verbrauchergeräten wie (IoT)-Produkten und Breitband-Routern aus gestartet werden. Ursache sind oft Verzögerungen bei der Aktualisierung und beim Patchen der kompromittierten Geräte.[7] Diese Ambivalenz in Bezug auf Updates war auch in einer ZVEI-Umfrage mit über 1.500 Verbrauchern ablesbar, bei der weniger als zwei Drittel der Befragten angaben, regelmäßig Updates auf IT- und Kommunikationsgeräte zu installieren. Bei den Besitzern von vernetzbarer Unterhaltungselektronik waren es sogar nur 43%, bei vernetzbaren Haushaltsgeräten nur 32%.

[3] https://blogs.microsoft.com/eupolicy/2022/03/23/the-urgency-of-tackling-europes-cybersecurity-skills-shortage/ Cybersecurity Workforce Study, 2022; S. 3 & 8. Die weltweite Lücke wird auf 3,4 Millionen Beschäftigten im Bereich der Cybersicherheit geschätzt.
[4] 13,2 Milliarden Verbindungen im Jahr 2022 und eine Prognose von 34,7 Milliarden IoT-Verbindungen für das Jahr 2028 (gemeinsame Anzahl von Wide, Area, Cellular und Short Range IoT-Verbindungen); Ericsson Mobility Report, November 2022, S. 11.
[5] BSI-Lagebericht: Die Lage der IT-Sicherheit in Deutschland 2022; p. 13, 52.
[6] Threat Landscape — ENISA (europa.eu)
[7] ENISA TREAT LANDSCAPE 2022, November 2022, p. 71.


## Kontakt

Marcel Hug • Manager Cyber Security & Strategy • Abteilung Digital- und Innovationspolitik •
Telefon: +49 69 6302 432 • Mobil: +49 162 2664 941 • E-Mail: Marcel.Hug@zvei.org

ZVEI e. V. • Verband der Elektro- und Digitalindustrie • Lyoner Straße 9 • 60528 Frankfurt am Main • www.zvei.org
Lobbyregisternr.: R002101 • EU Transparenzregister ID: 94770746469-09 • www.zvei.org

06/2023