Wirtschaftsrat der CDU e.V.
Bereich Innovation und Digitales
Luisenstr. 44
10117 Berlin
Tel.: +49 (0) 30 / 240 87 - 150
E-Mail: digitales@wirtschaftsrat.de

Andreas G. Barke
Referent Innovation und Digitales
Tel.: +49 (0) 30 / 240 87 - 227
E-Mail: a.barke@wirtschaftsrat.de

Stand: 14.02.2022

Positionierung des Wirtschaftsrats zur NIS2.0-Richtlinie

Verfasser: Bundesarbeitsgruppe Cybersicherheit und Taskforce NIS2.0

Die **Richtlinie über die Sicherheit von Netz- und Informationssystemen** (*Directive on Security of Network and Information Systems*) oder kurz NIS 2.0-Richtline wird derzeit im **Trilogverfahren** zwischen der EU-Kommission, dem Rat der Europäischen Union und dem Europäischen Parlament verhandelt. Die Trilogberatungen haben im Januar 2022 begonnen und werden laut Zeitplan **bis spätestens zum 28. April 2022 abgeschlossen** sein. Ab Inkrafttreten ist die Richtlinie durch die jeweiligen Institutionen je nach Ausgestaltung innerhalb von 18 bis 24 Monaten in nationales Recht zu überführen.

Kern dieser Richtlinie ist die **Gewährleistung eines gemeinsamen Niveaus harmonisierter Sicherheitsstandards und -vorschriften im gesamten digitalen Binnenmarkt der EU** (*Digital Single Market, DSM*). Eine einheitliche Definition von IT-Sicherheitspflichten für Unternehmen und Organisationen stellt die Grundlage hierfür dar. Insbesondere sogenannte **kritische Infrastrukturen** stehen im Fokus, u. a. Unternehmen aus folgenden Sektoren: **öffentliche Verwaltung, Energie- und Wasserversorgung, Verkehr, medizinische Versorgung, Transport und Verkehr sowie diverse Lieferketten**. Ziel der Richtlinie ist eine Verbesserung der **Cyber-Resilienz**, der **Souveränität** und der **Sicherheit der EU** und **ihrer Mitgliedstaaten**. Es sollen gleiche und faire Wettbewerbsbedingungen für kritische Infrastrukturen im digitalen Binnenmarkt gefördert werden.

Angesichts der **weitreichenden und umfassenden Folgewirkungen für Unternehmen und für den Wirtschaftsstandort Deutschland**, die sich aus der Umsetzung der Richtlinie ergeben werden, stellt der Wirtschaftsrat mit der Expertise seiner Mitglieder im Folgenden eine Reihe von Forderungen auf, die sich an **politische Entscheidungsträger auf nationaler und insbesondere EU-Ebene** richten. Dadurch wollen wir eine **Anpassung der benannten Inhalte** erreichen. Zugleich soll die Bedeutung der Thematik hervorgehoben und die Aufmerksamkeit dafür geschärft werden.

Insbesondere kritisch sieht der Wirtschaftrat die **erheblichen zusätzlichen bürokratischen und finanziellen Belastungen**, die auf zahlreiche Unternehmen zukommen werden, wobei **mittelgroße Unternehmen überproportional betroffen** wären. Gemeint sind hierbei vor allem **Vorgaben zu Meldefristen**, innerhalb derer Berichte zu Cybervorfällen an die zuständigen Behörden zu schicken sind. Problematisch ist der **Umfang sowie die Anzahl der einzubeziehenden Unternehmen**, d. h. konkret alle Unternehmen ab 50 Mitarbeitern und mit mehr als EUR 10 Mio. Jahresumsatz. Nach einer Auswertung des Statistischen Bundesamtes würden statt der bisher vom IT-Sicherheitsgesetz 2.0 (IT-SiG2.0) betroffenen 4.500 Unternehmen zukünftig **45.000 Unternehmen in Deutschland** unter diese Regulierung fallen. In der gesamten EU wird dies etwa 110.000 Unternehmen betreffen, was einer Versiebenfachung im Vergleich zur ersten NIS-Richtline entspricht (etwa 15.000 Unternehmen gemäß EU-Kommission). Daher fordern wir, als **maßgebliches Kriterium zur Einstufung eines Unternehmens in den Anwendungsbereich der Richtlinie die Kritikalität** heranzuziehen (siehe auch erste Forderung im Folgenden). Aufgrund des **Fachkräftemangels** in der IT-

Branche stellt sich unmittelbar die kritische Frage inwiefern die Richtlinie im vorgegeben Zeitrahmen tatsächlich umsetzbar ist.

Konkret sollten die folgenden **Probleme und Herausforderungen** angegangen werden:

- Einer der größten Mängel der aktuellen NIS-Richtlinie ist die **uneinheitliche Umsetzung auf nationaler Ebene der EU-Mitgliedsstaaten**. Parallele, sich bisweilen überschneidende EU-Rechtsakte und nationale Gesetze schaffen Rechtsunsicherheit und Verwirrung für Unternehmen jeder Größe. Der Gesetzgeber muss diese rechtliche Uneinheitlichkeit abstellen.
- Die **Ausbildung und Qualifizierung von IT-Sicherheitsexperten** hat mit den rasanten Entwicklungen der Digitalwirtschaft und ihren (potenziellen) Bedrohungen nicht Schritt gehalten.
- Um den Anforderungen der Regulierungsbehörden gerecht zu werden, sind für die Umsetzung neuer Vorschriften, Normen und Zertifizierungsverfahren **ausreichende Fachkenntnisse und Ressourcen** erforderlich. Diese fehlen derzeit im öffentlichen und privaten Sektor.
- Die NIS 2.0 muss flexibel genug sein, um mit den sich **ständig ändernden Bedrohungsszenarien** umgehen zu können.

Wir stellen folgende **zehn Forderungen** auf:

1. **Festlegung eines klaren Anwendungsbereichs** der NIS-Richtlinie 2.0, mit dem Ziel diesen nicht unnötig aufzublähen und den Erfüllungsaufwand für alle Organisationen und Einrichtungen, die Auswirkungen auf die digitale Lieferkette haben, angemessen und möglichst gering zu halten. Das maßgebliche Kriterium sollte die Bedeutung eines Ausfalls der Unternehmen für die Gesellschaft sein (Kritikalität), unabhängig von der Größe und dem Umsatz.
2. **Harmonisierung der IT- und Cybersicherheitslandschaft innerhalb der EU**, um der zunehmenden Komplexität und Dynamik von Cyberangriffen entgegenzuwirken und die Umsetzung für Unternehmen zu erleichtern.
3. **Förderung einer sicheren Ende-zu-Ende-Verschlüsselung ohne Hinter- und Vordertüren für nationale Behörden**, um sicherzustellen, dass die Sicherheit nicht geschwächt wird.
4. **Vermeidung einer „Einbahnstraße" bei der Meldung von Sicherheitsschwachstellen**, um allen Beteiligten die Möglichkeit zu geben, Sicherheitsschwachstellen schnellstmöglich zu beheben.
5. **Stärkung der Cyber-Resilienz in ganz Europa** durch Zusammenarbeit zwischen den nationalen *Computer Security Incident Response Teams* (*CSIRTs*).
6. **Klärung der Aufgaben, Kompetenzen und Verantwortlichkeiten von Führungskräften** in Bezug auf das Management von Cybersicherheitsrisiken und die Berichterstattung.
7. **Förderung der Umsetzung organisatorischer Cybersicherheitsmaßnahmen für Mitarbeiter in Schlüsselpositionen**, um den erhöhten Cybersicherheitsrisiken zu begegnen.
8. **Einräumung von erweiterten Meldefristen von mindestens 72 Stunden bei Cybervorfällen**, um der Komplexität von Cyberangriffen in technischer und organisatorischer Hinsicht gerecht zu werden (analog zur Datenschutzgrundverordnung, DSVGO). Die damit verbundenen Berichtspflichten sollten hinsichtlich der Definition von Cybervorfällen klar und transparent formuliert werden, um die Handlungsfähigkeit zu erhöhen.
9. **Umsetzung von Cybersicherheitsanforderungen auf der Grundlage des neuen Rechtsrahmens** (*New Legislative Framework, NLF*) **und internationalen Standards**, um nationale Insellösungen zu vermeiden und Kompatibilität und Transparenz zu fördern.
10. **Begrenzung der Bedingungen für die Verhängung von Geldbußen** gegen wichtige und bedeutende Einrichtungen, um ein angemessenes Gleichgewicht zwischen der Höhe der Strafe und dem Schaden zu erreichen.