bitkom

Nationale Umsetzung der NIS-2-Richtlinie

Handlungsempfehlungen aus Sicht der Digitalwirtschaft

Nationale Umsetzung der NIS-2-Richtlinie

Bitkom-Bewertung

Der Bitkom sieht die zwingende Notwendigkeit für einen stärker harmonisierten und zukunftssicheren Cybersecurity-Regulierungsrahmen und begrüßt daher die NIS-2-Richtlinie im Grundsatz. Der im Gesetzgebungsprozess gefundene Kompromiss schafft eine vernünftige Balance zwischen gezielten regulatorischen Eingriffen und einer ganzheitlichen Stärkung der Cyber-Resilienz der EU. In der Umsetzung in nationales Recht ist aus Sicht des Bitkom jedoch insbesondere die Schaffung von legislativer Konsistenz mit angrenzenden Rechtsakten und die praktische Umsetzbarkeit in den Fokus zu nehmen. Außerdem zentral ist eine möglichst gute nationale und EU-weite Harmonisierung.

Das Wichtigste

Für eine erfolgreiche und rechtssichere Umsetzung der NIS-2-Richtlinie ist ein strukturierter Dialog mit den betroffenen Unternehmen, Verbänden und dem Bundesministerium des Inneren und für Heimat (als für die Umsetzung zentralem Ministerium) sowie weiteren relevanten Ministerien und Behörden, essenziell. Dies betrifft insbesondere

- **Die Abgrenzung & Verflechtungen zu anderen Rechtsakten**

  Bei der Abgrenzung zu anderen Rechtsakten liegt dabei das Augenmerk auf der Nationalen Cybersicherheitsstrategie, dem KRITIS Dachgesetz (EU-CER-Richtlinie als ein Ausgangspunkt) sowie der DORA-Verordnung. Dabei sind auch Dopplungen und Inkonsistenzen, wie z.B. beim Melde- und Berichtspflichten ausdrücklich zu vermeiden. Auch ist sicherzustellen, dass die für die Erfüllung der Pflichten aus der NIS-2-Richtlinie notwendige Verarbeitung personenbezogener Daten rechtmäßig möglich ist. Diesbezüglich kann es erforderlich und sinnvoll sein, im nationalen Recht entsprechende Erlaubnistatbestände vorzusehen, die der europäische Gesetzgeber nicht geschaffen hat, was zu Rechtsunsicherheit führen könnte.
- **Die Harmonisierung des Anwendungsbereichs**

  Das deutsche IT-Sicherheitsgesetz 2.0 hat neue Klassifizierungen (UBI 1 & 2 & 3) für die Unternehmen im Anwendungsbereich eingeführt. Dies ist bei der NIS-2-Richtlinie (essential entities“/wesentliche Einrichtungen und „important entities“/wichtige Einrichtungen) nun ebenso der Fall. Daher gilt auch hier durch einen harmonisierten Anwendungsbereich Rechtssicherheit zu gewährleisten und die EU-weite Harmonisierung möglichst optimal umzusetzen.
- **Die konkrete Umsetzung der „EUCS-NIS 2.0-Brücke“**

  Auf Basis des Cybersecurity Acts wird derzeit seitens ENISA ein Cloud-Zertifizierungsschemata entwickelt. Eine kontrovers diskutierte Frage ist die mögliche Inkludierung von sogenannten Souveränitätsanforderungen in diesen Schemata. Auf Basis der NIS-2-Richtlinie ist es möglich das die Nutzung von zertifizierten Cloud Services verpflichtend werden könnte für wesentliche und

Bitkom-Zahl

Für

77%

der Unternehmen ist der bürokratische Aufwand bei der Meldung von Vorfällen zu hoch. (lt. Wirtschaftsschutzstudie 2022 von Bitkom Research)

wichtige Einrichtungen. Dabei handelt es sich um grundsätzliche Entscheidungen mit weitreichenden Folgen für die Digitale Transformation in diesen Sektoren. Eine systematische Analyse und Folgeabschätzung der Auswirkungen muss Grundlage einer politischen Entscheidung in diesem Kontext sein.

1 Abgrenzung & Verflechtungen zu anderen Rechtsakten

Bei der Abgrenzung zu anderen Rechtsakten liegt ein Fokus auf der der Erneuerung der Cybersicherheitsstrategie für Deutschland, der Umsetzung der CER-Richtlinie durch das KRITIS- Dachgesetz[1] sowie der DORA-Verordnung. Dabei sind auch Dopplungen und Inkonsistenzen, wie z.B. bei Melde- und Berichtspflichten ausdrücklich zu vermeiden, insbesondere da noch unklar ist welche Pflichten aus der Weiterentwicklung der Cybersicherheitsstrategie für Deutschland[2] und dem KRITIS-Dachgesetz für die Unternehmen entstehen können.

Artikel 7 der NIS2-Richtlinie legt fest, dass Mitgliedsstaaten nationale Cybersicherheitsstrategien erlassen müssen und spezifiziert auch welche konkreten Inhalte diese Strategie haben müssen. Es stellt sich daher die Frage, wie dies bei der nationalen Umsetzung der NIS-2-Umsetzung konkret erfolgen soll bzw. inwiefern dies mit den existierenden und geplanten nationalen Strategien und Handlungssträngen interagiert und wechselwirkt. Dabei möchten wir auch hier nochmals darauf hinweisen, dass die Weiterentwicklung der Cybersicherheitsstrategie für Deutschland ebenso mit dem KRITIS-Dachgesetz kohärent und konsistent sein muss. Die NIS-2-Richtlinie sieht in Artikel 7 lit. g „eine verstärkte Koordinierung zwischen den [...] zuständigen Behörden [...] zum Zweck des Informationsaustauschs über Risiken, Bedrohungen und Sicherheitsvorfälle“ vor. Es gilt daher ein einheitliches Verständnis darüber zu entwickeln, wie physische Sicherheit und Cybersicherheit umgesetzt werden können. In der Unternehmenspraxis sind diese Bereiche eng miteinander verzahnt und sollten nicht isoliert voneinander betrachtet und umgesetzt werden müssen.

Durch DORA wurde eine spezifische Regelung geschaffen, die Informationssicherheit im EU-Finanzsektor verbessern soll. Eine bloße deklaratorische Klarstellung, dass DORA im Verhältnis zu NIS als *lex specialis* anzusehen ist, halten wir für nicht ausreichend. Es ist bis heute nicht abzusehen, wie viel Teile der Wertschöpfungskette im Finanzsektor von DORA betroffen sind. Um Rechtsunsicherheit für die Unternehmen zu vermeiden,

1 Eckpunkte für das KRITIS-Dachgesetz

2 Diese wird gerade von der Bundesregierung vorbereitet/entwickelt. Diese sollte nach ursprünglichen Planungen in Q2 2022 erscheinen. Die Ankündigung dieser Strategie ist im Koalitionsvertrag explizit erwähnt (siehe dazu Link)

ist es essenziell, seitens NIS eine klare Abgrenzung zum Anwendungsbereich der DORA-Richtlinie zu schaffen. Dementsprechend ist es wünschenswert, dass das nationale Umsetzungsgesetz klarstellend regelt, dass das IKT-Risikomanagement auch das IKT-Drittparteienrisikomanagement mit umfasst. Dies allein würde allerdings die Rechtsunsicherheit bzgl. der Durchschlagskraft des EUCS auf Unternehmen im Anwendungsbereich von DORA nicht auflösen: Grundsätzlich erstreckt sich der Anwendungsbereich von DORA auf Finanzinstitute, sowie auf deren IKT-Dienstleister. Gleichzeitig erfolgt die Durchsetzung der Regelungen auf IKT-Dienstleister zum Großteil nur mittelbar über das IKT-Drittparteienrisikomanagement (mit Ausnahme der kritischen IKT-Drittdienstleister). In diesem Zusammenhang stellt sich die Frage, was passiert in Fällen, in denen die IKT-Drittdienstleister sowohl DORA als auch NIS-2 unterliegen, sollten die Vorschriften nicht identisch umgesetzt werden? Das Risiko, dass Dienstleister aus Drittstaaten nicht in der Lage sind, die Souveränitätsanforderungen zu erfüllen, wird nicht dadurch verringert, dass man die Anforderungen im Rahmen der Wertschöpfungskette vom Kunden auf den Dienstleister verlagert.

Im Rahmen der nationalen NIS-2-Umsetzung ist außerdem offen, inwiefern existierende Freiheitsgrade, die sich aus dem Rechtstext ergeben und die bei der nationalen Umsetzung genutzt werden können, konkret umgesetzt werden sollen. Aus Sicht der Digitalwirtschaft ist hier eine weitere Konkretisierung notwendig, um Rechtssicherheit und Rechtsklarheit in der Praxis zu erzeugen. Der Bitkom steht hier mit seinen Mitgliedern für den Dialog zu diesen Fragestellungen bereit.

2 Harmonisierung des Anwendungsbereich

Die NIS-2-Richtlinie erweitert den Kreis der Betreiber und Sektoren, welche unter die Richtlinie fallen signifikant. Dabei werden erneuerte Kategorien von „essential entities“/wesentliche Einrichtungen und „important entities“/wichtige Einrichtungen eingeführt, welche auch ungeachtet der Größe der Unternehmen gelten. Auch das IT-Sicherheitsgesetz 2.0 hat neue Klassifizierungen (UBI 1 & 2 & 3) für die Unternehmen im Anwendungsbereich eingeführt und die CER-Richtlinie/KRITIS Eckpunktepapier der Bundesregierung führt neue Sektoren als KRITIS ein. Hier gilt es den Anwendungsbereich entsprechend der NIS-2-Richtlinie zu vereinfachen und zu harmonisieren, um Rechtssicherheit zu gewährleisten und die EU weite Harmonisierung nicht zu konterkarieren.

Dazu sollte der Gesetzgeber bei der Umsetzung die Vorgaben aus der Richtlinie zielgerichtet auslegen und neben den Sicherheitsinteressen auch marktrelevante Faktoren wie Wettbewerbsnachteile, z.B. steigende Aufwände und Kosten mit in den Blick nehmen. Beispielhaft ist hier Anhang 1, Ziff. 1 a) letzter Spiegelstrich zu nennen, welcher „Betreiber von Ladepunkten“ zu den wesentlichen Einrichtungen zählt. Bei

weiter Auslegung wären bereits Unternehmen als „wesentliche Einrichtung“ zu qualifizieren, wenn sie einen (1) Ladepunkt für ihre Mitarbeiter oder etwa für Kunden (z.B. Ladesäulen vor Supermärkten) betreiben. Dies würde eine Vielzahl von Unternehmen erfassen und auch den Ausbau von Elektromobilität hemmen. Es sollte daher klargestellt werden, dass nur solche Unternehmen als wesentliche Einrichtungen zählen, deren primärer Geschäftszweck in der NIS-2-Richtlinie erfasst ist.

Um eine unverhältnismäßige Ausweitung des Anwenderkreises zu vermeiden, muss auch sichergestellt werden, dass Sektoren, welche nicht im Anwendungsbereich der NIS-2-Richtlinie fallen, aber bisher nach der BSI-KritisVO als kritische Anlage definiert wurden, ausgenommen werden. Deutschland würde bei der Umsetzung ansonsten unverhältnismäßig weit über die Ziele der NIS-2-Richtlinie hinausgehen und die EU-weite Harmonisierung unterminieren.

Es ist außerdem klarzustellen, wie die UBI-Kategorien in den Anwendungsbereich fallen und diese insgesamt harmonisieren. Entsprechend müssen für die Kategorien der Unternehmen die Fristen zur Umsetzung von Pflichten und Verordnung ausgesetzt bzw. verlängert werden. Dabei sollte der ursprüngliche Maßnahmenumfang für die s.g. „Unternehmen im besonderen öffentlichen Interesse“ (*Definition der Unternehmen von besonderer volkswirtschaftlicher Bedeutung per RVO § 10 Abs. 5)* nicht überstiegen werden. Dies ist insbesondere in Anbetracht der Tatsache zu beachten, dass viele Unternehmen das erste Mal unter eine vergleichbare Richtlinie fallen werden und diese größtenteils der KMU angehören werden. Eine Vereinfachung der Kategorien erlaubt zu dem eine schnellere Identifizierung der Unternehmen und damit eine schnellere Umsetzung in Deutschland, welche im Hinblick auf die momentane Sicherheitslage essenziell ist.

Im Hinblick auf die verheerenden Cyberangriffe auf deutsche Universitäten und Kommunen, welche sich in langfristigen und gravierenden Einschränkungen für Bürgerinnen und Bürger manifestierten spricht sich der Bitkom für eine Inkludierung von Bildungseinrichtungen und der öffentlichen Verwaltung auf kommunaler Ebene in den Anwendungsbereich laut Artikel 2(5) aus, um eine flächendeckende Verbesserung des Cybersicherheitsniveau in Deutschland zu erreichen.

3 Konkrete Umsetzung der „EUCS-NIS-2-Brücke“

Artikel 24(1) der NIS-2-Richtlinie gibt den Mitgliedstaaten der EU den Spielraum, dass sie „wesentliche und essentielle“ Einrichtungen dazu verpflichten, IKT-Prozesse, -Dienste und -Prozesse verwenden, die auf Basis von Schemata nach dem Cybersecurity-Act (Artikel 49 CSA) zertifiziert sind. Es handelt sich dabei in Artikel 24(1) um eine „Kann-Regelung“. Artikel 24(2) der NIS-2-Richtlinie in Verbindung mit Artikel

38(2) legt fest, dass die Europäische Kommission delegierte Rechtsakte in Ergänzung zur NIS-2-Richtlinie erlassen kann, um wesentliche und essenzielle Einrichtungen zu verpflichten, Zertifizierungen auf Basis des CSA zu nutzen, wenn ein „unzureichendes Niveau der Cybersicherheit“ festgestellt wurde. Aus Sicht des Bitkoms ist es hier elementar, dass EU-weit harmonisiert und einheitlich vorgegangen wird, um eine weitere Fragmentierung des digitalen EU-Binnenmarktes zu vermeiden.

Der CSA bildet die regulatorische Grundlage für Zertifizierungsschemata.[3] Aus Sicht des Bitkoms basiert der Ansatz bzw. der Geist des CSA in diesem Zusammenhang auf der Freiwilligkeit der Nutzung von CSA-Schemata (siehe dazu u.a. Recital 91 & Artikel 56) mit dem Ziel, den digitalen Binnenmarkt zu stärken, Vergleichbarkeit zu erhöhen und das grenzüberschreitende Angebot von Produkten zu erleichtern. Daher sieht der Bitkom eine mögliche verpflichtend vorgeschriebene Nutzung von CSA-Schemes in diesem Zusammenhang als nationale Entscheidung nach Artikel 24(1) kritisch und spricht sich in diesem Zusammenhang gegen nationale Alleingänge nach Artikel 24(1) aus . Aus Sicht des Bitkoms definiert Artikel 24(2) der NIS-2-Richtlinie Voraussetzungen („unzureichendes Niveau der Cybersicherheit“ wurde festgestellt) für den Erlass eines delegierten Rechtsaktes, welcher die Nutzung von CSA-Schemata EU-weit verpflichtend macht. Es muss also zuerst ein „unzureichendes Niveau der Cybersicherheit“ festgestellt worden sein, um eine verpflichtende Zertifizierung zu rechtfertigen. Übergeordnet (also betreffend Artikel 24(1) & 24(2)) ist der Bitkom daher der Meinung das eine verpflichtende Nutzung von CSA-Zertifizierungen nur die ultima ratio sein sollte. Auch die Nutzung von Normen (z.B. harmonisierte europäischen Normen) könnte eine Möglichkeit sein, um über Zertifizierungen Konformität nachzuweisen. Jedenfalls sollte die Umsetzung der NIS-2-Richtlinie keinen weiteren Anforderungskatalog schaffen, sondern auf erprobte Regelwerke verweisen, wie z.B. ISO27001. Der in der NIS-2-Richtlinie aufgeführte Maßnahmenkatalog entspricht dem Anforderungskatalog der ISO27001 im Wesentlichen. Gerade Unternehmern die unterschiedliche Sicherheitsstandards umsetzen müssen, sind ausreichend mit dem damit verbundenen „Multistandardmanagement“ beschäftigt.

Seit längerer Zeit werden im Rahmen des CSA „Cloud Services Certification Schemes EUCS“ mögliche Souveränitätsanforderungen als zusätzliche Anforderungen neben den reinen IT-Sicherheitsanforderungen in den Strukturen der ENISA diskutiert. Der Bitkom hat diesen Prozess begleitet und dazu auch Positionierungen entwickelt. Generell lehnt Bitkom eine Vermengung von technischen Anforderungen mit Souveränitätsanforderungen in einem technischen Schema (Mandat/Scope CSA) ab. Politische und legalistische Fragen und Ziele der digitalen Souveränität/Datenhoheit sollten von den EU-Institutionen (Europäisches Parlament, Europäische Kommission, Europäischer Rat) und Mitgliedsstaaten im Rahmen der etablierten Gesetzgebungsprozesse und -verfahren entschieden werden.

Das kürzlich erschienene Non-Paper „Joint document: alternative solutions regarding the issue of Independence to non-EU law in the context of EUCS“, diskutiert und vergleicht verschiedene Optionen zum Ansatz der möglichen Inkludierung von Souveränitätsanforderungen. Grundsätzlich begrüßt Bitkom, dass Vor- und Nachteile verschiedener möglicher Optionen diskutiert werden. Bevor jedoch Entscheidungen

[3] Derzeit vorangetrieben werden insbesondere EUCC (Common Criteria) und EUCS (Cloud). Schemata für IoT und 5G sind angedacht seitens ENISA.

mit hoher und langfristiger Tragweite getroffen werden, muss eine umfassende Folgeabschätzung erfolgen. Die Perspektiven der betroffenen Unternehmen sollten dabei allerdings stärker als bisher mit in diese Lagebildbewertung und Folgeabschätzung miteinbezogen werden.

Ein offener & strukturierter Dialog mit betroffenen Ministerien und Unternehmen (sowohl Cloud-Anbieter als auch Cloud-Anwender aus potenziell betroffenen Sektoren) bleibt aus Sicht des Bitkoms Grundlage für ein möglichst klares und ganzheitliches Lagebild möglicher Auswirkungen a) einer möglichen verpflichtenden Nutzung von CSA-Schemes im Allgemeinen und b) möglichen Souveränitätsanforderungen als Teil des Cloud-CSA-Schemes im Speziellen. Ein solches ganzheitliches Lagebild kann wiederum die Grundlage bilden für eine ganzheitliche Folgeabschätzung sein bezüglich der Auswirkungen derartiger Anforderungen Eine solche ganzheitliche Folgeabschätzung ist aus Sicht des Bitkoms eine Grundlage für politische Entscheidungen in diesem Zusammenhang. Bisher ist das nach Kenntnis des Bitkom nicht erfolgt seitens der Ministerien, ENISA und EU-Kommission.

Der Bitkom ist hier bereit einen solchen strukturierten Dialog mit den Perspektiven seiner Mitglieder systematisch zu begleiten (Cloud-Anbieter, Vertreter/innen aus den Sektoren der potenziell betroffene „wesentliche und kritische“ Einrichtungen im Sinne der NIS-2-Richtlinie).

4 Kapitel IV: Risikomanagement & Berichtspflichten

Die Meldung von Vorfällen kann eine wichtige Rolle dabei spielen, auf Vorfälle zu reagieren, aber auch weitere Auswirkungen von imminenten Bedrohungen oder Schwachstellen einzudämmen. Die Auswirkungen der Meldepflicht müssen daran gemessen werden, wie die Informationen aus gemeldeten Cyber-Vorfällen anonymisiert analysiert, angereichert und verbreitet werden, um die Sicherheit des gesamten Cyber-Ökosystems zu erhöhen. Zu diesem Zweck möchten wir einige wichtige Punkte und Ansätze hervorheben.

Die Risikomanagementmaßnahmen schreiben in Artikel 21 die Sicherheit der Lieferkette vor. Dabei bleibt momentan noch unklar, welche Anforderungen an die Sorgfaltspflicht der Lieferkettensicherheit angestrebt wird und wie dies auch nachweisbar sein können. Eine weit gefasste Lieferkettensicherheitsnachweispflicht, kann zu Lieferkettenproblemen für Unternehmen und Organisationen führen, welche unter den Anwendungsbereich der NIS-2 Richtlinie fallen, da Lieferanten wie, z.B. KMUs, die Lieferkettensicherheitsnachweis lediglich mit enorm hohem finanziellem

und personellem Aufwand stemmen können. Denken könnte man z.B,. die in der ISO27001 geforderten Sicherheitsmaßnahmen zum Supplier-Management als Grundlage für eine generische Vorgehensweise nehmen, die für die betroffenen Unternehmen – auf der Grundlage einer risikobasierten Lieferantenbewertung – Flexibilität zulässt.

In Anlehnung an die Erwägungsgründe 24 und 25 der NIS-2-Richtlinie ist es von größter Wichtigkeit, dass Melde- und Berichtspflichten kohärent und wirksam bearbeitet werden. Dies bedeutet auch, das Unternehmen eine einzelne Anlaufstelle haben und auch nur einmal melden bzw. berichten müssen. Dabei gilt es auch alte Strukturen zu erneuern, wie z.B. die separate Anlaufstelle für UBI 1 und UBI 2. Dies ist insbesondere im Hinblick der Tatsache, dass Unternehmen in alle drei UBI-Kategorien fallen können und trotzdem separat melden müssen unbedingt zu verschlanken.

Des Weiteren sollten global praktizierte Standards bei der Entdeckung von Schwachstellen durch Dritte berücksichtigt werden, die dem Softwarehersteller gemeldet werden und bei denen der Softwarehersteller entscheidet, wann er diese Schwachstelle bekannt gibt, was sinnvollerweise regelmäßig erst nach Veröffentlichung eines Patches oder einer Abhilfemaßnahme erfolgt. Eine Ausnahme hiervon bilden regelmäßig nur solche entdeckten Schwachstellen, die von Kriminellen und feindlich gesinnten Stellen aktiv ausgenutzt werden, was eine sofortige Bekanntmachung erfordert. Der Bitkom schlägt vor ein verschlüsseltes Onlineformular zur Meldung bereitzustellen, welches die Möglichkeit bietet sich selbst als Unternehmen eines gewissen Sektors und Kategorie zu identifizieren und an die zu meldenden Behörden, wie z.B. das BSI, die BNetzA und die Datenschutzbehörden auszuwählen. Damit kann sichergestellt werden, dass Unternehmen ihre Melde- und Berichtspflichten problemlos wahrnehmen können und minimiert zudem den Arbeitsaufwand durch die Schaffung von Synergien.

Berichtselementen, welchen CSIRTs die Möglichkeit geben, den Betroffenen oder dem breiteren Cyberökosystem einen Gegenwert zu bieten sollten dabei priorisiert werden. Beispielsweise können spezifische Identifikatoren von Bedrohungsakteuren, Taktiken, Techniken oder Verfahren erfragt werden. Dies kann dazu beitragen, die gemeldeten Informationen über Vorfälle zur Entwicklung von verwertbaren Erkenntnissen effektiv und in Echtzeit an die zu schützenden Stellen weiterzuleiten. Die Sicherheit des Meldewesen-Systems muss dabei den zu übermittelnden sensiblen Informationen entsprechen.

5 Förderung des deutschen Stakeholderdialogs

Um eine praxisnahe und fristgerechte Umsetzung der NIS-Richtlinie in deutsches Recht zu gewährleisten ist die frühzeitige Einbindung von Unternehmen durch eine

Stakeholder-Konsultation und einen frühzeitigen und fortlaufenden Dialog essenziell. Der Stakeholderdialog sollte die Erfahrungen aus den Unternehmen, welche unter das IT-Sicherheitsgesetz-2.0 fallen, bündeln und als Erfahrungswerte für die zukünftige Umsetzung nehmen. Dies schließt die Kommunikation der zuständigen Stellen zur Aufklärung über den Stand der Technik im Cybersicherheitsbereich ein.

Die Zusammenarbeit und der Austausch im UP KRITIS zwischen Betreibern von Kritischen Infrastrukturen, nationalen Fach- und Branchenverbänden, anerkannten SPOCS sowie zuständigen Behörden ist ein zentrales Dialoggremium zu relevanten Fragen des Betriebs und von kritischen Infrastrukturen damit zusammenhängenden Herausforderungen in der Praxis. Unternehmen, die durch die Ausweitung des Scopes nun auch Adressaten sind, sind rasch in die entsprechenden Strukturen des UP KRITIS zu integrieren.

Bitkom vertritt mehr als 2.000 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. 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 oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. 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 weltweit führenden Digitalstandort zu machen.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner
Simran Mann | Referentin Sicherheitspolitik
T 030 27576-214 | s.mann@bitkom.org

Lukas Klingholz | Leiter Cloud & Künstliche Intelligenz
T 030 27576-101 | l.klingholz@bitkom.org

Verantwortliches Bitkom-Gremium
AK Sicherheitspolitik und AK Cloud-Politik & Gaia-X