position

Stellungnahme zum 3. Entwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungs-gesetz

17. Juni 2024

Der BGA

Der BGA vertritt die Interessen von mehr als 139.000 Unternehmen des Groß- und Außenhandels sowie der B2B-Dienstleistungen auf nationaler, europäischer und internationaler Ebene. Er setzt sich ein für Weltoffenheit, freien Wettbewerb in einer liberalen, marktwirtschaftlichen Ordnung und verantwortungsvolles Unternehmertum.

Vorbemerkung

Die Bedrohungslage durch Cyberangriffe auf die deutsche Wirtschaft im Allgemeinen und den mittelständisch geprägten Groß- und Außenhandel sowie den B2B Dienstleistungssektor im Speziellen spitzt sich seit Jahren erheblich zu. Geopolitische sowie kriminelle Akteure fügen der deutschen Wirtschaft durch hochgradig professionalisierte Angriffe auf IT-Infrastrukturen einen jährlichen Schaden in einem dreistelligen Milliardenbereich zu und bedrohen damit die Prosperität der Wirtschaft und die Funktionsfähigkeit des Gemeinwesens insgesamt. Der Groß- und Außenhandel ist davon aufgrund seiner nationalen und internationalen Verflechtungen und seiner Rolle als Wirtschaftsstufe (Jahresumsatz >1,7 Billionen Euro) für die deutsche Volkswirtschaft in besonderem Maße betroffen. Unsere Unternehmen sind vor allem mittelständisch geprägt, überaus heterogen und enorm erfolgreich. Auf unterschiedliche Weise sind sie damit attraktive Ziele für kriminelle Akteure. Gleichzeitig bilden unsere Unternehmen die Infrastruktur der Handelsnation Deutschland und sind auch in Bezug auf Cybersecurity auf die Verlässlichkeit (inter-) nationaler Lieferketten angewiesen. Natürlich sind die 139.000 Unternehmen unserer Wirtschaftsstufe sensibilisiert für die Situation und haben ein großes Eigeninteresse daran, Unternehmensprozesse und Infrastruktur resilient zu gestalten. Aufgrund der hohen Vernetzung aller wirtschaftlicher Akteure in Deutschland und Europa beinhaltet dies natürlich die Etablierung von Standards und die Synchronisierung nationaler und internationaler Cybersecurity-Maßnahmen.

Der BGA unterstützt daher ausdrücklich das Bestreben der Europäischen Union und der Bundesregierung die Resilienz der Wirtschaftsstandorte Europa und Deutschland gegen Cyberattacken von innen und außen zu stärken. Das NIS-2-Umsetzungsgesetz setzt einen wichtigen Impuls, welcher die IT-Sicherheitsstandards sowohl in der Wirtschaft als auch für

Einrichtungen des öffentlichen Sektors potenziell zu erhöhen vermag. Die Neuordnung von Unternehmen in „wichtige“ und „besonders wichtige Einrichtungen“ unterhalb der Schwelle für „kritische Anlagen“ stärkt die Harmonisierung innerhalb der europäischen Union. Dennoch fehlt eine Definition „kritischer Anlagen“ im Gesetz, was den umständlichen Weg einer nachgelagerten Rechtsverordnung nötig machen wird, um für Klarheit zu sorgen. Bedenklich ist zudem, dass die Bundesregierung die NIS-2 Umsetzung in nationale Gesetzgebung deutlich zu spät angegangen ist, sodass die EU-weite Umsetzungsfrist (17. Oktober 2024) mit hinreichender Wahrscheinlichkeit nicht zu halten ist. Dies führt zu einem erhöhten und vermeidbaren Zeit- und Kostendruck für mittelständische Unternehmen, der kontraproduktiv für die grundsätzlich richtigen Ziele der NIS-2 Richtline wirken wird. Besonders problematisch sind nicht nur die unverständlichen Ausnahmen für öffentliche Einrichtungen, sondern auch, dass sich hier ein Muster nicht eingehaltener Umsetzungsfristen fortschreibt, das ein bedenkliches Bild der legislativen Disziplin der Bundesregierung und der beteiligten Ressorts zeichnet.

Kritikpunkte:

1. **Ausnahmen für öffentliche Einrichtungen**

   Wiederholte Angriffe auf Einrichtungen der Kommunen, der Länder, des Bundes haben nicht nur gezeigt, wie verwundbar große Teile unserer öffentlichen Institutionen sind. Sie haben auch offengelegt, wie mit vergleichsweise geringen, kriminellen Mitteln größte Schäden in Verwaltung angerichtet werden können. Dies führt zu erheblichen Kosten nicht nur für die Bevölkerung, sondern auch für die häufig regional verankerte, mittelständische Wirtschaft. Es ist daher nicht verständlich, warum Ausnahmen für Einrichtungen der Länder und der Kommunen oder für entgeltliche arbeitende Dienstleister des Bundes gelten sollen. Von den Ländern vorgetragene verfassungsrechtliche Bedenken drohen erneut zu einem Flickenteppich zu werden, der die angestrebten Standards für IT-Sicherheit bereits im Vorhinein torpediert. Die Unternehmen des Groß- und Außenhandels und des B2B-Dienstleistungssektors haben ein großes Interesse an einer verlässlichen, digitalen und belastbaren Ausgestaltung von Verwaltungen und öffentlicher IT-Infrastruktur. Grundsätzlich sollten staatliche Institutionen aller Ebenen als entsprechende Dienstleister mindestens als „besonders wichtige Einrichtungen“ gelten, sobald diese personenbezogene Daten, Daten aus Berichtspflichten von Unternehmen erheben und vorhalten oder sonstige Aufsichtspflichten gegenüber der Wirtschaft erfüllen oder wesentlich an der Bereitstellung von Infrastruktur jedweder Art beteiligt sind. Ausnahmen für Einrichtungen des öffentlichen Sektors sind ein fataler Fehler, der korrigiert werden muss. Zudem zeigt dies ein bedenkliches Bild, bei dem Unternehmen erneut enorm belastet werden, während der öffentliche Sektor weitgehend ausgespart bleiben soll, obwohl dieser evident verwundbar ist.

2. Große Unsicherheiten zu Betroffenheit

Der aktuelle Entwurf sorgt für große Verunsicherung bei Unternehmen, da in zu vielen Fällen nicht klar ist, ob Unternehmen von der NIS-2-Regulierung betroffen sind. Der Entwurf begründet die Regulierung von Unternehmen und Einrichtungen sowohl durch die Zugehörigkeit zu Sektoren als auch durch die Rolle einer Einrichtung oder eines Unternehmens innerhalb einer Lieferkette. Dieser Gedanke folgt einem systemischen Verständnis von IT-Sicherheitsarchitektur und ist im Grunde zu begrüßen. Allerdings führt dies zu einer bereits jetzt steigenden Verunsicherung von mittelständischen Großhandelsunternehmen zur eigenen Betroffenheit, die nicht unwesentlich durch die negativen Erfahrungen mit dem Lieferkettensorgfaltspflichtengesetz (LkSG) begründet ist. Die in Anlage 2 des Entwurfs beschriebenen Sektoren bieten eine zu unscharfe Definition dessen, was als Teil einer Lieferkette gelten kann. Allein der Begriff „Handel mit chemischen Stoffen“ umfasst eine kaum zu überblickende Zahl von Produktgruppen, die von Farben, Grundstoffe pharmazeutischer Produkte über Erzeugnisse im Baugroßhandel bis hinein in den Lebensmittelhandel reichen. Sind Händler bereits betroffen, wenn Sie Reinigungsmittel für Produktionsstätten „chemischer Stoffe“ liefern oder erst dann, wenn deren Produkte unmittelbar zur Herstellung verwendet werden? Der Gesetzgeber und das BSI müssen dringend für Klarheit in der Frage sorgen, ob sich die regulatorische Betroffenheit insbesondere für Handelsunternehmen eher durch die Produkte oder durch ihre Position in komplexen Lieferketten ergibt und diese in einfache und transparente Orientierungspunkte überführen. Fehlen diese, werden Unternehmen unter Regulierungsdruck geraten, die von der NIS-2-Umsetzung möglichweise nicht erfasst werden, verbunden mit hohen und unnötigen Kosten. Wie Unternehmen von Mitgliedsverbänden des BGA berichten, prüfen einzelne Versicherungen auf Basis der Unsicherheiten, die für Unternehmen mit der NIS-2 verbunden sind, bereits pauschal den Versicherungsstatus von beispielsweise Farbengroßhändlern, da diese mit „chemischen Stoffen“ handeln, während auf Basis von Größe und Produktgruppen dieser Unternehmen noch unklar ist, ob diese durch NIS-2 und auf Basis von Anlage 2 überhaupt erfasst sein werden.

3. Zertifizierung

Die aktuell noch sehr schwache Skizzierung von Zertifizierungsverfahren ist ebenfalls problematisch. Die bisherigen Ausführungen in § 30 Abs. 6 BSIG-E oder § 54 reichen hierfür nicht und decken insbesondere die Pflichten der zertifizierten Unternehmen gegenüber deren Kunden nicht ab. Alle Unternehmen, die entweder Teil einer relevanten Lieferkette oder eines der beschriebenen Sektoren sind, sehen sich nun der Situation gegenüber, dass sie zumindest zu Beginn der Geltung der NIS-Umsetzung in Deutschland kaum überprüfen können, ob ihre Dienstleister NIS-2 konform arbeiten. Dies ist insbesondere vor dem Hintergrund der noch immer installierten Geschäftsführerhaftung ein Problem, da Unternehmen nach aktueller Lesart auch für Versäumnisse ihrer Dienstleister haften. Unternehmen, die die Umsetzung selbst organisieren müssen, werden durch § 54 nicht erfasst. Auch ob § 55, der eigene Konformitätserklärungen regelt, oder § 57 hier genügen, ist derzeit unklar. Ohne geeignete Zertifikate kann ein Großhandelsunternehmen auch seinen

Kunden gegenüber und im Rahmen der Lieferkette nur schwerlich belegen, dass es NIS-2-konform arbeitet, ohne umfangreichste Unterlagen vorzulegen. Dies ist mit der täglichen Geschäftsrealität nicht vereinbar und wird zu weiteren Unsicherheiten führen. Das BSI muss ein Zertifizierungsregime auflegen, das auch kleinen Unternehmen gerecht wird, die nicht umfänglich auf einen zertifizieren Dienstleister zurückgreifen können oder ihre IT selbst organisieren.

4. Zu kurze Fristen, hohe Belastung mittelständischer Unternehmen, erwartbare Staus bei Dienstleistern

Obwohl der BGA die Ziele der NIS-2 Umsetzung im Grunde befürwortet, stellen wir fest, dass deren Umsetzung insbesondere für Mittelständler erneut hohe bürokratische und monetäre Belastungen bedeutet. Neben den wiederholt gestiegenen Belegpflichten für mittelständische Unternehmen wird auch der Beratungsbedarf aufgrund der bereits beschriebenen Unsicherheiten für einen hohen Beratungsbedarf sorgen, der durch das BSI nicht abgedeckt wird. Dieser erstreckt sich nicht nur auf hohe Kosten für rechtliche Beratungen, sondern auch auf Cybersecurity-Maßnahmen, Schulungen und Monitoring. Nach derzeitiger Lesart werden Regelungen für wichtige und sehr wichtige Einrichtungen unmittelbar mit Veröffentlichung des Umsetzungsgesetzes gelten. Durch die kurzen Umsetzungsfristen für wichtige und besonders wichtige Einrichtungen und den sehr späten Anstoß zur Überführung der NIS-2 Richtlinie in nationale Gesetzgebung wird es kurzfristig zu einer erhöhten Nachfrage nach Expertise am Markt kommen. Es ist zu befürchten, dass dies zu erblichen Engpässen, steigenden Beratungskosten und weiterer Verunsicherung führen wird, die mit einer deutlich früheren Beschäftigung durch die Bundesregierung hätten vermieden werden können. Dies wird potenziell zur Verzögerung der Umsetzung der NIS-2 Ziele beitragen. Damit tragen die mittelständischen Unternehmen die Kosten nicht nur für die Umsetzung selbst, sondern auch für deren erhebliche Verzögerung durch die Bundesregierung.