VDA | Verband der Automobilindustrie

Kurzposition

Zum KRITIS Dachgesetz in nationales Recht

Gemäß der Critical Entities Resilience Directive

Berlin, Mai 2023

Inhaltsangabe

1 Einleitung

Der VDA begrüßt grundsätzlich die Schaffung eines sicheren Rechtsrahmens für die Sicherheit von kritischen Infrastrukturen. Im Dezember 2022 hat das Bundeskabinett Eckpunkte für ein Gesetz zum Schutz Kritischer Infrastrukturen beschlossen. Der VDA sieht hier erheblichen Änderungsbedarf.

Vor dem Hintergrund der aktuellen geopolitischen Entwicklung sowie hybriden Bedrohungen sieht der VDA die Notwendigkeit eines engen Schulterschlusses zwischen Staat und Wirtschaft. Es muss das gemeinsame Ziel sein, die deutsche Wirtschaft in ihren sensiblen Wertschöpfungs- und Lieferprozessen nachhaltig und wirkungsvoll zu schützen. Dabei muss in Zeiten des Fachkräftemangels darauf geachtet werden, dass es zu keinem akuten Personalmehraufwand kommt.

2 Unternehmenskategorien

Ein KRITIS Dachgesetz muss dem Anspruch, ein „Dach“ über dem Rechtsrahmen zur Sicherheit von Unternehmen zu sein, gerecht werden.

- ➔ Ein Dachgesetz sollte gesetzlichen Vorgaben zur Sicherheit im Real-Raum (physische Sicherheit) wie auch im Cyber-Raum (IT-Sicherheit) harmonisieren.
- ➔ Darüber hinaus müssen die Zuständigkeiten der verschiedenen Bundesressorts eindeutig und rechtssicher beschrieben werden. Hierbei sollten auch die föderalen Strukturen (Zuständigkeiten der Bundesländer) berücksichtigt werden.

Größtmögliche Harmonisierung des Geltungsbereiches mit der EU CER-Richtlinie „Critical Entities Resilience Directive“

Für den wirkungsvollen Schutz von Gemeinwohl und Leben in Deutschland sowie zur Aufrechterhaltung des sozialen Zusammenhalts, ist es unabdingbar die sensiblen und damit kritischen Wertschöpfungs- und Lieferketten (KWL) zu identifizieren und zu klassifizieren. Dies sollte anhand einer Methodik erfolgen, die es ermöglicht, eindeutig eine Zugehörigkeit zu KWL auf den Ebenen Prozess, Leistung, Produkt und/oder Service vorzunehmen.

- ➔ Anstelle einer reinen Betrachtung von KRITIS Unternehmen (nach Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen), sollte sich an den Kategorien der EU 2022/2555 nach „essential Entities“ und „important Entities“ orientiert werden.
- ➔ Dazu sollten die „KRITIS“ und Unternehmen im besonderen öffentlichen Interesse (UBI) Kategorien mit den „essential Entities“ und „important Entities“ harmonisiert werden. Maßgebend dazu sollte die jeweilige Branchenzugehörigkeit sowie die Unternehmensgröße bzw. der Jahresumsatz sein.
- ➔ Die Kategorien UBI 1-3 sollten aufgelöst werden.
- ➔ UBI 1 sollte als Kategorie zusätzlich zu den in der NIS 2 definierten Branchen in den Anwendungsbereich des Umsetzungsgesetzes aufgenommen werden.
- ➔ Der VDA spricht sich dafür aus, den Titel des Dachgesetzes anzupassen – beispielsweise „Dachgesetz zur Erhöhung der Resilienz von Wertschöpfungs- und Lieferketten in Deutschland“.

3 Meldeprozess

Eine getrennte Betrachtung von IT und physischen Angriffen darf es nicht geben. Cybervorfälle zeigen ihre wirklichen Auswirkungen immer auch im realen Raum. Getrennte Meldeprozesse führen nur zu getrennten Lagebildern und im schlimmsten Fall zu fehlenden Informationen an entscheidenden Stellen. Hybride Bedrohungen benötigen einen einheitlichen Meldeprozess.

Pflichten zur Meldung von Sicherheitsvorfällen müssen einen Mehrwert für die Gefahrengemeinschaft von Staat und Unternehmen bringen. Das beinhaltet auch, dass die Bedeutung und der Nutzen eines integrierten Lagebildes für die physische Sicherheit und IT-Sicherheit gestärkt werden müssen. Hierzu ist es notwendig, dass:

- ➔ Sicherheitsvorfälle unabhängig von ihrem Wirkungsbereich (Real-Raum oder Cyber-Raum) an eine zentrale Stelle gemeldet werden.
- ➔ Meldungen zu Sicherheitsvorfällen in digitaler Form, nach dem Once-Only-Prinzip durch betroffene Unternehmen abgesetzt werden können. Die Meldungen müssen dabei durch das Unternehmen bearbeitbar bleiben.
- ➔ das BSI dadurch ein zentrales Lagebild zu dem Vorfall führen kann.
- ➔ Behörden des Bundes und der Länder sowie von der Regulierung betroffene Unternehmen nach dem Need-To-Know-Prinzip auf ein solches Lagebild rechtssicher zugreifen können.

4 Vertrauenswürdigkeit von Mitarbeitern

Die Möglichkeit zur Prüfung der Vertrauenswürdigkeit von Personal an sensiblen Stellen schaffen.

Um sensible Bereiche in Unternehmen vor schädigenden Handlungen zu schützen, dürfen an besonders sicherheitssensitiven Stellen keine Personen beschäftigt sein, bei denen Sicherheitsbedenken bestehen.

- ➔ Die geltenden Definitionen und der Begriff einer „sicherheitsempfindlichen Stelle“ bedarf einer Ausweitung und Schärfung.

In der Praxis scheitert der Informationsaustausch zwischen Sicherheitsbehörden untereinander, Regelungen bzw. Vorgaben des amtlichen Geheimschutzes. Das betrifft Unternehmen, die nicht als geheimschutzbetreute Unternehmen gelten. Somit sind in der Praxis dem Austausch von Lageinformationen von staatlicher Seite enge Grenzen gesetzt.

- ➔ Mitarbeiter der Sicherheitsabteilungen mit entsprechender herausgehobener Stellung sollten einer Sicherheitsüberprüfung nach Sicherheitsüberprüfungsgesetz unterzogen werden. Hier ist es von absoluter Dringlichkeit, dass offizielle Behörden ihre Prozessdauer verkürzen, um Wartezeiten zu reduzieren.
- ➔ Des Weiteren sollten die rechtlichen Voraussetzungen geschaffen werden, dass Unternehmen Mitarbeiter mit Tätigkeiten in sensiblen Bereichen sowie entsprechende Mitarbeiter von Fremdfirmen, die interne Kenntnisse über sensible Abläufe und Prozesse haben (z. B. Systemadministratoren, Information Security Manager,

Sicherheitspersonal), einer Prüfung der Vertrauenswürdigkeit unterziehen zu können. Es ist vorstellbar, dass eine solche Prüfung - in den Grenzen der Vorgaben des Gesetzgebers -, von der Wirtschaft eigenverantwortlich vorgenommen wird. Der Gesetzgeber müsste hierzu lediglich den Rechtsrahmen schaffen. Hierbei sollte stets von der KANN-Möglichkeit ausgegangen werden.

5 Expertengruppe

Vermeiden von „Schnellschüssen“ und forcieren eines engen Schulterschlusses von Staat und Wirtschaft.

Um eine nachhaltige und qualitativ hochwertige Regulierung zu erreichen, regt der VDA an:

➔ Einrichtung einer Gruppe von Experten, die mit sachverständigen Vertretern der Unternehmenssicherheit sowie aus dem politischen Raum und aus Forschung und Lehre besetzt ist.

Auftrag dieser Gruppe sollte es sein, Vorschläge zu erarbeiten und den Gesetzgeber hinsichtlich zu ergreifender Maßnahmen zu beraten. Durch die frühzeitige Einbindung von Experten könnte der Ablauf der gesetzgebenden Verfahren verkürzt und qualitativ verbessert werden. Zusätzlich ist es möglich, eine bessere Umsetzbarkeit und höhere Akzeptanz der Gesetzgebung zu schaffen.

Ansprechpartner

Dr. Marus Bollig
Geschäftsführer
marcus.bollig@vda.de

Martin Lorenz
Abteilungsleiter (komm.) Fahrzeugtechnologie & Eco-Systeme
Fachgebietsleiter Cybersecurity, Daten & Wirtschaftsschutz
martin.lorenz@vda.de

Der Verband der Automobilindustrie (VDA) vereint mehr als 650 Hersteller und Zulieferer unter einem Dach. Die Mitglieder entwickeln und produzieren Pkw und Lkw, Software, Anhänger, Aufbauten, Busse, Teile und Zubehör sowie immer neue Mobilitätsangebote. Wir sind die Interessenvertretung der Automobilindustrie und stehen für eine moderne, zukunftsorientierte multimodale Mobilität auf dem Weg zur Klimaneutralität. Der VDA vertritt die Interessen seiner Mitglieder gegenüber Politik, Medien und gesellschaftlichen Gruppen. Wir arbeiten für Elektromobilität, klimaneutrale Antriebe, die Umsetzung der Klimaziele, Rohstoffsicherung, Digitalisierung und Vernetzung sowie German Engineering. Wir setzen uns dabei für einen wettbewerbsfähigen Wirtschafts- und Innovationsstandort ein. Unsere Industrie sichert Wohlstand in Deutschland: Mehr als 780.000 Menschen sind direkt in der deutschen Automobilindustrie beschäftigt. Der VDA ist Veranstalter der größten internationalen Mobilitätsplattform IAA MOBILITY und der IAA TRANSPORTATION, der weltweit wichtigsten Plattform für die Zukunft der Nutzfahrzeugindustrie.

Herausgeber	Verband der Automobilindustrie e.V. (VDA) Behrenstraße 35, 10117 Berlin www.vda.de
Copyright	Verband der Automobilindustrie e.V. (VDA) Nachdruck und jede sonstige Form der Vervielfältigung ist nur mit Angabe der Quelle gestattet.
Version	Version 1.1, Mai 2023