Bundesverband

Positionspapier

Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/1148

Verpflichtung aller relevanter Marktteilnehmer und europäische Harmonisierung essentiell

Stand: 16. Dezember 2016

Entwurf wird aktueller Bedrohungslage nur in Teilen gerecht.

Allgemein

Der ASW Bundesverband begrüßt die Bemühungen zur Verbesserung des Sicherheitsniveaus von Netz- und Informationssystemen im europäischen Raum.

Der Zeitraum, der den Verbänden und Unternehmen zur Verfügung gestellt wurde, um eine Stellungnahme zum Umsetzungsgesetz zu verfassen, ist nicht ausreichend. Für eine gründliche Prüfung und fundierte Stellungnahme hätte eine angemessene Bearbeitungszeit zur Verfügung gestellt werden müssen.

Der ASW Bundesverband sieht es als erforderlich an, Sicherheitsaspekte im Cyberraum ganzheitlich zu betrachten. Hierzu sind **alle relevanten Marktteilnehmer bei der Umsetzung von Sicherheitsanforderungen zu berücksichtigen**, die Produkte oder Dienste im Cyberraum anbieten. Dies schließt explizit Anbieter mit ein, bei denen ein Ausfall oder eine Beeinträchtigung ihres Dienstes mit dem Ausfall oder der Beeinträchtigung kritischer Infrastrukturen vergleichbar ist, bzw. den Ausfall oder die signifikante Beeinträchtigung kritischer Infrastrukturen bedingen können. Dazu können auch Anbieter von Internetdiensten sowie Hardware- und Softwarehersteller zählen.

Erfreulich ist daher die inhaltliche Erweiterung auf bestimmte Dienste. Die Richtlinie greift jedoch eher unsystematisch drei Bereiche (Online-Marktplätze, Suchmaschinen, Cloud-Dienste) heraus, die nun mit der Umsetzung entsprechend verpflichtet werden sollen. Nicht zuletzt jüngste Cyber-Sicherheitsvorfälle zeigen, dass in Zeiten des „Internet of Things“ (IoT) **Hersteller von Hard- und Software genauso wie Netz- und Diensteanbieter** bekannte Schwachstellen unverzüglich beseitigen müssen. Daher sollten diese im Rahmen des Gesetzgebungsverfahrens regulatorisch miteinbezogen werden.

Unverständlich ist für uns der **Ausschluss von Infrastrukturen und Diensten des Bundes und der Länder**. Da die NIS-Richtlinie eine derartige Ausnahme für Infrastrukturen und Dienste der Mitgliedsstaaten nicht vorsieht, sehen wir die NIS-Richtlinie in diesem Punkt nicht vollständig umgesetzt. Die Bundesregierung sollte vielmehr als Vorreiter in Sachen Cyber-Security in Europa agieren.

Das Thema **MIRT** (Mobil Incident Response Team) mit in das Gesetz aufzunehmen wird begrüßt. Hier ist jedoch sorgfältig darauf zu achten, wann wer diese Unterstützung anfordern kann. Aus unserer Sicht muss die Mobile Einsatztruppe ausschließlich bei Anfrage durch den „Betroffenen“ selbst zum Einsatz kommen. Des Weiteren sind evtl. Haftungsfragen zu klären. Darüber hinaus heißt es im Gesetzestext, dass das BSI Dritte hinzuziehen kann. Hier muss sichergestellt sein, dass dies nur mit dem Einverständnis des Betroffenen geschehen kann.

Verbundunternehmen stehen weiterhin vor der Herausforderung, sich an unterschiedliche Regelungen halten zu müssen. Ein einheitlicher Unternehmensstandard ist so de facto nicht möglich. Eine einheitliche Vorgabe wäre hier wünschenswert.

Mittelfristig muss durch eine **EU-weite Harmonisierung** sichergestellt werden, dass alle Anbieter, die im europäischen Binnenmarkt tätig sind und europäische Nutzer adressieren, unabhängig von ihrer geographischen Herkunft, EU-Recht zur Cybersicherheit anwenden. Der vorgelegte Entwurf zu Implementierung der NIS-Richtlinie darf daher nur ein Zwischenschritt sein. Der Gesetzgeber sollte einen entsprechenden Impuls in Richtung der EU-Institutionen geben. Die Bundesregierung sollte sich für eine **Novellierung der NIS-Richtlinie** sowie eine entsprechende **Einbeziehung der Hersteller von Hard- und Software in den Anwendungsbereich** einsetzen. Dies

ASW Bundesverband | Allianz für Sicherheit in der Wirtschaft e.V.
Neue Schönhauser Straße 20 | 10178 Berlin
Telefon +49 (0)30 200 77 200 | Telefax +49 (0)30 200 77 056
info@asw-bundesverband.de | www.asw-bundesverband.de

schließt die Verpflichtung der Hersteller zur Übernahme etwaige Kosten und zur Vornahme von Sicherungsmaßnahmen auch über den Supportzeitraum hinaus ein. Eine solche Harmonisierung brächte die für KRITIS-Betreiber notwendige Rechtssicherheit.

Der **Erfüllungsaufwand** für die Wirtschaft wird mit max. 3,5 Mio. Euro angegeben. Dieser Wert erscheint zu gering. Wenn bspw. ein Energieversorger zukünftig auch Online-Vertriebsplattformen „zertifizieren" lassen muss, reicht diese Summe bei weitem nicht aus.

Änderungen des BSI Gesetztes

§2 Absatz 9

Die geänderte Gesetzgebung enthält die Definition von kritischen Diensten. Derzeit mangelt es aber noch an einer Entsprechung für die digitalen Dienste in der derzeit gültigen KRITIS VO, die lediglich eine Definition von kritischen Anlagen vorsieht.

Die Definition für Cloud-Computing-Dienste ist wenig griffig und sollte sich noch stärker an der Definition der NIS-Richtlinie (Ziff.17) orientieren. Andernfalls ist der Geltungsbereich nicht hinreichend bestimmt. In Bezug auf § 2 Abs. 9 regen wir an, die zahlreichen Verweise auf Richtlinien und Verordnungen der EU durch dem EU-Recht entsprechende Formulierungen zu ersetzen und so in nationales Recht umzusetzen. Dies dürfte auch die Lesbarkeit und Anwendbarkeit erheblich verbessern.

§5a Absatz (4)

„[…] kann das Bundesamt auf deren Ersuchen" Wir schlagen vor, „kann" durch „muss" zu ersetzen. Das Gesetz spricht hier von „herausgehobenen Fällen". Ein Ersuchen sehen wir daher vergleichbar mit dem Notruf bei der Polizei.

§8b

Der Aufwand für die Meldung von Sicherheitsvorfällen erhöht sich durch die Änderungen qualitativ und quantitativ. Wir regen daher eine eindeutige Festlegung der Meldekriterien an, so dass die Voraussetzungen für eine Meldeverpflichtung im Einzelfall leichter zu prüfen sind. Eine entsprechende Abstimmung mit den KRITIS-Betreibern ist notwendig, um die Umsetzbarkeit von Beginn an gewährleisten zu können. Die bislang in den FAQ des BSI eher unverbindlich gegebenen Hinweise zu den Meldekriterien reichen dazu nicht aus.

§8b Absatz 4

Nach dem Referentenentwurf sollen zukünftig „mögliche grenzübergreifende Auswirkungen" bei Störungen gemeldet werden. Hier sehen wir erheblichen Klärungsbedarf, bzw. eine harmonisierte Umsetzung der NIS-RL als unerlässlich. Andernfalls sind unterschiedliche oder gar widersprüchliche Umsetzungen wahrscheinlich, verbunden mit einer hohen Rechtsunsicherheit für die Konzerne.

Das Wichtigste in Kürze

- Zeitraum für die Rückmeldung der Verbände unzureichend
- alle relevanten Marktteilnehmer sind bei der Umsetzung von Sicherheitsanforderungen zu berücksichtigen
- Infrastrukturen und Dienste des Bundes und der Länder sind einzubeziehen
- EU-weite Harmonisierung notwendig

ASW Bundesverband | Allianz für Sicherheit in der Wirtschaft e.V.
Neue Schönhauser Straße 20 | 10178 Berlin
Telefon +49 (0)30 200 77 200 | Telefax +49 (0)30 200 77 056
info@asw-bundesverband.de | www.asw-bundesverband.de