

Formulierungshilfe

Änderung § 165 Abs. 3 TKG – Systeme zur Angriffserkennung

Anlass

Das Gesetz zur Änderung des Telekommunikationsgesetzes (TKG) verknüpft in § 165 TKG bestimmte Sicherheitsanforderungen an die Einstufung als „besonders wichtige Einrichtung“ nach § 28 Abs. 1 S. 1 Nr. 3 BSI-G. Dies führt dazu, dass Unternehmensgröße und wirtschaftliche Bedeutung an die Stelle einer risikobasierten Betrachtung der konkret angebotenen TK-Dienste und -Netze treten.

Problem

Unternehmensgröße allein erlaubt keine belastbare Aussage über die Kritikalität oder das Sicherheitsrisiko der angebotenen TK-Dienste. Besonders betroffen sind hybride Anbieter, deren TK-Dienste lediglich unterstützende Bestandteile anderer Angebote darstellen und kein vergleichbares Risikoprofil wie klassische Telekommunikationsnetze aufweisen. Deren Einbeziehung in § 165 TKG löst zudem deutlich umfassendere Pflichten im BNetzA-Sicherheitskatalog aus, die implementiert werden müssen.

Lösungsansatz

§ 28 Abs. 3 BSI-G sieht vor, dass vernachlässigbare Geschäftstätigkeiten bei der Zuordnung zu einer Einrichtungsart unberücksichtigt bleiben. Dieser Grundsatz muss konsequent auch in § 165 TKG und im Sicherheitskatalog der BNetzA zur Anwendung kommen. Verweise auf § 28 Abs. 1 S. 1 Nr. 3 BSI-G sind stets um den Vorbehalt des § 28 Abs. 3 BSI-G zu ergänzen.

Gegenüberstellung - § 165 Abs. 3 TKG

Regierungsentwurf (geltende Fassung)	Formulierungsvorschlag (neue Fassung)
(3) Als eine angemessene Maßnahme im Sinne des Absatzes 2 können Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste Systeme zur Angriffserkennung im Sinne des § 2 Nummer 41 des BSI-Gesetzes einsetzen. Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste, die besonders wichtige Einrichtungen im Sinne des § 28 Absatz 1 Satz 1 Nummer 3 des BSI-Gesetzes sind , haben entsprechende Systeme zur Angriffserkennung einzusetzen. Die eingesetzten Systeme zur Angriffserkennung müssen in der Lage sein, durch kontinuierliche und automatische Erfassung und Auswertung Gefahren oder Bedrohungen zu erkennen. Sie sollen zudem in der Lage sein, erkannte Gefahren oder Bedrohungen abzuwenden und für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen. Weitere Einzelheiten kann die Bundesnetzagentur im Katalog von Sicherheitsanforderungen nach § 167 festlegen.	(3) Als eine angemessene Maßnahme im Sinne des Absatzes 2 können Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste Systeme zur Angriffserkennung im Sinne des § 2 Nummer 41 des BSI-Gesetzes einsetzen. Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste, die besonders wichtige Einrichtungen im Sinne des § 28 Absatz 1 Satz 1 Nummer 3 des BSI-Gesetzes sind , haben entsprechende Systeme zur Angriffserkennung einzusetzen, <u>sofern ihre Telekommunikationsnetze und Telekommunikationsdienste nicht im Sinne des § 28 Absatz 3 BSI-Gesetz als vernachlässigbare Geschäftstätigkeit betrachtet werden müssen, da sie lediglich als integrierte und unterstützende Bestandteile anderer Angebote erbracht werden</u> . Die eingesetzten Systeme zur Angriffserkennung müssen in der Lage sein, durch kontinuierliche und automatische Erfassung und Auswertung Gefahren oder Bedrohungen zu erkennen. Sie sollen zudem in der Lage sein, erkannte Gefahren oder Bedrohungen abzuwenden und für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen. Weitere Einzelheiten kann die Bundesnetzagentur im Katalog von Sicherheitsanforderungen nach § 167 festlegen.

Begründung

§ 28 Abs. 3 BSI-G stellt klar, dass vernachlässigbare Geschäftstätigkeiten – also TK-Dienste, die lediglich als integrierte und unterstützende Bestandteile anderer Angebote erbracht werden – bei der Zuordnung zu einer Einrichtungsart unberücksichtigt bleiben. Die vorgeschlagene Ergänzung stellt die Kohärenz zwischen BSI-G und TKG sicher und verhindert eine unverhältnismäßige Regulierungsausdehnung auf hybride Anbieter ohne entsprechendes Risikoprofil.