Stellungnahme der Deutschen Telekom

zum Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union

Das Bundesministerium des Innern (BMI) hat am 09. Dezember 2016 einen Referentenentwurf des Gesetzes zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union versandt.

Angesichts der wachsenden Bedeutung des Cyberraums, des Internet und informationstechnischer Systeme ist es wichtig, Risiken und Bedrohungen der Netz- und Informationssicherheit zu minimieren. Die Deutsche Telekom begrüßt daher ausdrücklich die weltweite Debatte um die Verbesserung der Cybersicherheit und kann auch aufgrund jüngster Ereignisse durchaus die Intention des Gesetzgebers nachvollziehen, hier eine zeitnahe Umsetzung der Richtlinie in nationales Recht zu forcieren.

Die Deutsche Telekom ist selbstverständlich gerne bereit, im Rahmen des Gesetzgebungsverfahrens ihre praktischen Erfahrungen im Umgang mit derartigen Risiken zur Verfügung zu stellen. Allerdings benötigt unser Haus für eine eingehende und sachgerechte Auseinandersetzung mit den vorgeschlagenen Regelungen und die Erarbeitung einer fundierten Stellungnahme eine angemessene Bearbeitungszeit. Innerhalb der den Verbänden und Fachkreisen eingeräumten kurzen Stellungnahmefrist ist eine eingehende Beschäftigung mit dem vorgeschlagenen Gesetzestext und eine umfassende Bewertung nicht möglich. Insofern war uns lediglich eine kursorische Prüfung des Entwurfs möglich. Unsere Stellungnahme berücksichtigt daher auch nur die wesentlichen kritischen Punkte. Dies vorausgeschickt, gibt es auch im Zuge der nationalen Implementierung der NIS-Richtlinie einige grundlegende, vor die Klammer zu ziehende Anmerkungen:

- Für eine ganzheitliche Sicherheitsbetrachtung der Wertschöpfungskette des Cyberraums ist es erforderlich, alle relevanten Marktteilnehmer bei der Umsetzung von Sicherheits-Anforderungen zu berücksichtigen, die Produkte oder Dienste im Cyberraum anbieten. Dies betrifft insbesondere Anbieter, 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. Hierzu zählen auch Anbieter von Internetdiensten sowie Hardware- und Softwarehersteller. Erfreulich ist aus dieser Sicht die inhaltliche Erweiterung auf bestimmte Dienste. Allerdings greift die Richtlinie eher unsystematisch drei Bereiche (Online-Marktplätze, Suchmaschinen, Cloud-Dienste) heraus, die nun mit der Umsetzung entsprechend verpflichtet werden sollen. Gerade im Kontext des „Internet of Things“ (IoT) wird deutlich, dass Hersteller von Hard- und Software genauso ebenso wie Netz- und Diensteanbieter bekannte Schwachstellen unverzüglich beseitigen müssen. Bei besonders kritischen Komponenten sollte die Sicherheit und Vertrauenswürdigkeit der Produkte zudem durch eine unabhängige Prüfstelle nachgewiesen werden. Ferner ist der Ausschluss von Infrastrukturen und Diensten des Bundes und der Länder zur Erhöhung der IT-Sicherheit nicht zweckdienlich. 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. Vor diesem Hintergrund halten wir es für erstrebenswert, dass die Bundesregierung als Vorreiter für mehr IT-Sicherheit in Europa die Hersteller von Hard- und Software im Rahmen dieses Gesetzgebungsverfahrens ebenfalls regulatorisch einbezieht.

- Absehbar muss als weiteres Lenkungsziel sichergestellt werden, dass in dem gemeinsamen Binnenmarkt auch ein möglichst hohes Sicherheitslevel erreicht wird. In jedem Fall muss gewährleistet werden, dass alle Anbieter, die im europäischen Binnenmarkt tätig sind und europäische Nutzer adressieren, unabhängig von

ihrer geographischen Herkunft EU-Recht zur Cybersicherheit anwenden. Vor diesem Hintergrund kann der vorgelegte Entwurf zu Implementierung der NIS-Richtlinie nur als Zwischenschritt gewertet werden. Es wäre daher wünschenswert, wenn der Gesetzgeber auch einen entsprechenden Impuls in Richtung der EU-Institutionen geben könnte. Als Stichwort dient in diesem Kontext bspw. die Kritikalität sogenannter IoT-Geräte. Die Bundesregierung sollte sich für eine Novellierung der NIS-Richtlinie sowie eine entsprechende Einbeziehung der Hersteller von Hard- und Software in den Anwendungsbereich einsetzen. Einbeziehung in diesem Sinne meint auch die Verpflichtung der Hersteller zur Übernahme etwaige Kosten und zur Vornahme von Sicherungsmaßnahmen auch über den Supportzeitraum hinaus. Durch diesen Harmonisierungsschritt würde sich ein weiterer Schritt in Richtung Rechtssicherheit ergeben, der von allen KRITIS Betreibern gewünscht ist.

- Über den vorgelegten Implementierungsentwurf und seine bekannte Limitierung auf KRITIS sowie die benannten Dienste hinaus, sollte aus Sicht der Deutschen Telekom das Bewusstsein für die Bedeutung von Cybersicherheit geschärft und damit auch über die Chancen, Risiken und Kosten von Cybersicherheit informiert werden. Dies gilt auch und gerade mit Blick auf Start-Ups und kleine und mittelständische Unternehmen. Entsprechend investieren wir umfangreich in interne und externe Initiativen und Kampagnen zur Sensibilisierung im Kontext Cybersicherheit und setzen korrespondierende Sicherheitsmaßnahmen und Kontrollen in der gesamten Deutsche Telekom Gruppe für die unterschiedlichen Kunden- und Unternehmenssegmente um. Darüber hinaus hat die Deutsche Telekom, in Kooperation mit dem Bundesamt für Sicherheit in der Informationstechnik, zahlreiche Projekte aufgesetzt, um die Sichtbarkeit der internationalen Bedrohungen zu erhöhen. Mit dem Sicherheitstacho (sicherheitstacho.eu / securitydashboard.eu) stellt die Deutsche Telekom zudem jedem Interessierten kostenfrei Informationen über die aktuelle Angriffssituation im Cyberraum zur Verfügung.

- Zur Erreichung eines möglichst hohen Sicherheitslevels existieren auf europäischer und internationaler Ebene bereits zahlreiche Initiativen und Zusammenschlüsse sowie Standardisierungsgremien. Diese sollten genutzt werden, um hohe Sicherheitsstandards in der EU und weltweit zu verankern. Mit einem solchen Standardisierungsansatz kann dynamisch auf sich ändernde Technologietrends, Bedrohungen und Risikoszenarien reagiert werden. Die Normen der ISO 27000- Reihe formulieren beispielsweise dabei konkrete Sicherheitsanforderungen, beschreiben die Methodik für ein Risiko Management und die Feststellung des Umsetzungsgrades von Richtlinien und Standards.

Neben diesen allgemeinen Einlassungen, sind zudem einige Bestimmungen im vorgelegten Entwurf i.S. eine reibungslosen Umsetzung zu präzisieren:

1. *§2 Absatz 9 BSI-Gesetz*
   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.

2. *§8b BSI-Gesetz*
   Durch die geänderte Gesetzgebung erhöht sich der Aufwand für die Meldung von Sicherheitsvorfällen qualitativ und quantitativ. Für die Verpflichteten und für die Empfänger einer Meldung ist eine eindeutige Festlegung der Meldekriterien notwendig, um die Voraussetzung für eine Meldeverpflichtung im Einzelfall prüfen zu können. Die bislang in den FAQ des BSI wohl unverbindlich gegebenen Hinweise zu den Meldekriterien greifen hier zu kurz.

Insofern regen wir eine verbindliche Festlegung der Meldekriterien an. Dieses sollte mit den Betreibern im Vorfeld abgestimmt sein, um die Umsetzbarkeit sicherstellen zu können.

3. *§8b Absatz 4*
   Nach dem Referentenentwurf sollen zukünftig „mögliche grenzübergreifende Auswirkungen" bei Störungen gemeldet werden. Dann sind Meldewege in den einzelnen relevanten Mitgliedsstaaten ggf. zu berücksichtigen, was zu mehrfachen Meldungen nach möglicherweise unterschiedlichen Kriterien führen würde. International agierende Konzerne betreiben meist Dienste in mehreren Staaten der EU, bieten Dienste aus verschiedenen Staaten für verschiedene Staaten an und beziehen Dienste aus verschiedenen Mitgliedsstaaten. Eine nicht harmonisierte Umsetzung der NIS-RL in den einzelnen EU-Mitgliedstaaten führt dann ggf. zu unterschiedlichen oder gar widersprüchlichen Umsetzungen der Anforderungen, die ggf. nicht realisierbar sind. Ein entsprechender Austausch zwecks Harmonisierung in den Mitgliedsstaaten ist wünschenswert.

4. *§ 8c Absatz 2 (e)*
   Das genannte Meldekriterium entspricht dem Meldekriterium in der NIS-Richtlinie. Allerdings ist eine Bewertung der Auswirkung des Vorfalls auf wirtschaftliche und gesellschaftliche Tätigkeiten für die Betreiber in aller Regel mangels entsprechender Informationen nicht durchführbar.

5. Abschließend wollen wir anregen, dass die Anbieter digitaler Dienste sowie die Betreiber kritischer IT-Infrastrukturen das Recht erhalten, die bei der Nutzung der Dienste entstehenden Daten der Nutzer zu erheben und zu verwenden, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder beseitigen zu können.

Wir stehen Ihnen für Rückfragen und einen vertiefenden Dialog selbstverständlich gerne zur Verfügung.