Positionspapier

zum Vorschlag für eine Richtlinie zur Erreichung eines hohen Netzwerk- und Informationssicherheitsstandards der Europäischen Kommission (COM 2013/0027 (COD))[1]

17.06.2013
Seite 1

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.700 Unternehmen, davon über 1.100 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software & IT-Services, Telekommunikations- und Internetdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für eine Modernisierung des Bildungssystems, eine innovative Wirtschaftspolitik und eine zukunftsorientierte Netzpolitik ein.

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: +49.30.27576-0
Fax: +49.30.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Marc Fliehe
Referent Sicherheit
Tel. +49. 30.27576-242
Fax. +49. 30.27576-51242
m.fliehe@bitkom.org

Präsident
Prof. Dieter Kempf

Hauptgeschäftsführer
Dr. Bernhard Rohleder

1. Hintergrund

Die Europäische Kommission hat am 7. Februar 2013 einen Vorschlag für eine Richtlinie zur Erreichung eines hohen Netzwerk- und Informationssicherheitsstandards innerhalb der europäischen Union vorgelegt. BITKOM nimmt gerne die Gelegenheit wahr, seine Position zum Vorschlag darzustellen.

Der BITKOM unterstützt den Ansatz der Europäischen Kommission nachdrücklich, die Union widerstands- und handlungsfähiger gegen die wachsende Anzahl von Cyberbedrohungen zu machen. Datensicherheit ist ein hohes Gut und in Deutschland bereits durch eine Vielzahl von Maßnahmen entscheidend gestärkt. Das intendierte Ziel, einheitliche Sicherheitslevels bei unterschiedlichen Betreibern kritischer Infrastrukturen zu etablieren, wird daher ausdrücklich begrüßt, vor allem auch deshalb, weil sich die Kommission in ihren Vorschlägen auf Maßnahmen gegen Vorfälle beschränkt, die sich auf die Verfügbarkeit des Kerngeschäfts der betroffenen Sektoren beziehen. Dadurch wird verhindert, dass eine übertrieben umfassende Absicherung sämtlicher Systeme bereits getätigte Sicherheitsinvestitionen gefährdet. Weiterhin wird begrüßt, dass Telekommunikationsprovider wegen bereits vorhandener Regulierungen auf EU-Ebene (Richtlinie 2002/21/EG) von der Richtlinie ausgenommen werden. Auch eine erhebliche Regulierung auf nationaler Ebene findet durch §109 TKG bereits statt.

Daneben erscheint BITKOM der Ansatz der Kommission sehr sinnvoll, die Kooperationsmechanismen der Mitgliedsstaaten im Bereich der Netzwerk- und Informationssicherheit zu stärken. Unabdingbar ist hierfür die Aufforderung an die Mitgliedsstaaten, sich so noch nicht geschehen, eine Netzwerk- und Informationssicherheitsstrategie zu geben und eine kompetente Stelle zum Thema zu schaffen, die die Mitgliedsstaaten handlungs- und kooperationsfähig macht. Auch der Aufbau einer sicheren Kommunikationsinfrastruktur zwischen diesen Stellen erscheint in diesem Zusammenhang sinnvoll. Diese Auflagen sind in

[1] Diese Position repräsentiert die Mehrheitsmeinung der Mitgliedsunternehmen im BITKOM e.V. Eine signifikante Minderheit vertritt die Ansicht, dass die Richtlinie eine höhere Anzahl von Marktteilnehmer sowie alle Dienstanbieter entlang der Wertschöpfungskette gelten soll.

Deutschland bereits durch die nationale Cybersicherheitsstrategie, das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Bundesnetzagentur (BNetzA) in begrüßenswerter Art und Weise realisiert. Hier sollte auf die in Deutschland gemachten Erfahrungen zurückgegriffen werden, um andere Mitgliedsstaaten in ihren Bemühungen zu unterstützen. Um hier eventuelle unnötige Nachsteuerungen bei den bereits vorhandenen Strategien und Institutionen und zu vermeiden, sollte die Kommission bereits im Vorfeld klarmachen, welche bereits vorhandenen nationalen Strukturen sie für hinreichend hält. Dies würde ebenfalls dabei helfen, ein level-playing-field in den Mitgliedsstaaten zu sichern.

Die Einrichtung leistungsfähiger Computer Emergency Response Teams (CERTs) zur Reaktion auf Cyberangriffe erscheint aus Sicht des BITKOM ebenfalls ein sinnvoller Schritt, der sektoren- und industrieübergreifend erfolgen muss. Auch hier kann aus den deutschen Erfahrungen gelernt werden, wo bereits auf verschiedenen Ebenen mit dem CERT Bund, dem CERT-Verbund und dem Bürger CERT wertvolle Erfahrungen gemacht und gute Erfolge erzielt worden sind.

Unumgänglich ist unseres Erachtens dabei eine enge Zusammenarbeit von Staat und Wirtschaft

- zum verstärkten Aufbau von fachlicher Expertise zur Informationssicherheit in der Privatwirtschaft und bei der öffentlichen Hand
- bei der Entwicklung eines dynamischen, risiko-basierten Ansatzes zur Bekämpfung von Cyber-Gefahren
- im vertrauensvollen, gegenseitigen Informations- und Erfahrungsaustausch bis hin zu einem gemeinsamen Verständnis der Bedrohungslage insb. im Hinblick auf Gefahren und Angriffe auf die IT-Infrastruktur in Deutschland
- bei der Strafverfolgung von Cyber-Kriminalität
- bei präventiven und reaktiven Maßnahmen gegen akute IT-Sicherheitsvorfälle
- zur Schaffung einer öffentlichen Sicherheitskultur, die bestehende Gefahren und Risiken im Cyberraum reflektiert und einer entsprechenden Sensibilisierung des einzelnen Nutzers

Im Hinblick auf eine erfolgreiche Zusammenarbeit von Staat und Wirtschaft setzt der BITKOM auf den Grundsatz der Freiwilligkeit und unterstützt dabei direkt oder durch seine Mitgliedsunternehmen eine Vielzahl von erfolgreichen deutschen Initiativen. Insbesondere die vom BITKOM mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) initiierte Allianz für Cybersicherheit kann als Beispiel auch im europäischen Rahmen dienen, denn sie hat das Potenzial, nachhaltig die Sicherheitskultur in Wirtschaft und Bevölkerung zu verändern. Hier wurde beispielsweise ein unkomplizierter und auf Wunsch anonymer Meldeweg geschaffen, um das Bundesamt für Sicherheit in der Informationstechnik - den kompetenten Ansprechpartner in Sachen Cybersicherheit auf nationaler Ebene - über aktuelle Angriffe zu unterrichten. Gleichwohl eröffnet eine regulatorische Verankerung des Themas Informationssicherheit die Chance, Wirtschaft und Staat einen klaren Handlungsrahmen vorzugeben. Dieser sollte für alle Beteiligten Planungs- und Rechtssicherheit erzeugen. BITKOM befürwortet also den Vorschlag der Kommission, hier einen geeigneten

Kooperationsmechanismus zwischen staatlichen Akteuren und Privatwirtschaft zu entwickeln. Dabei erscheint es BITKOM der richtige Ansatz, dass der Entscheidung, ob eine übergreifende, zentral koordinierte Reaktion nötig ist, eine Risikoanalyse vorausgeht und der Grundsatz gilt, dass lokale Abwehrmaßnahmen auch lokal gesteuert werden.

Weiterhin ist es aus Sicht BITKOM absolut zu begrüßen, dass der Richtlinienvorschlag davon absieht, Marktteilnehmern und öffentlicher Verwaltung technische Vorgaben hinsichtlich der zu nutzender Produkte zu geben. Damit hat die Kommission unterstrichen, dass sie sich für die Förderung von Innovation und Wettbewerb einsetzt. Zertifizierungen wie sie beispielsweise das Bundesamt für Sicherheit in der Informationstechnik durchführt sollten weiterhin möglich sein, jedoch keine unüberwindbare Marktzugangshürde für internationale Anbieter darstellen.

BITKOM befürwortet, dass die Europäische Kommission die Entwicklung von Standards auch im Sicherheitsbereich als marktgetriebenen Prozess ansieht. Gerade im Bereich der IT-Sicherheit und Risiko-Management haben sich bereits internationale Standards wie ISO 27001 und ISO/IEC 31010:2009 herausgebildet. Hier sollten keine nationalen oder regionalen Sonderwege gewählt werden.

Um die Vorbereitung der Richtlinie möglichst zielgerichtet und sachdienlich vorzubereiten, hat die Kommission angemessene Konsultation, auch unter Anhörung von Fachexperten angekündigt. Dies begrüßt BITKOM ausdrücklich, möchte jedoch unterstreichen, dass es sich bei hierbei nicht nur um Fachexperten zum Bereich Netzwerk- und Informationssicherheit handeln sollte, sondern vor allen Dingen auch Fachexperten, die den Impact der Maßnahmen auf die einzelnen betroffenen Wirtschaftsbereiche ausreichend bewerten können.

Vor diesem Hintergrund erlauben wir uns, den vorliegenden Richtlinienentwurf in den folgenden Punkten zu kommentieren.

2. Artikel 3 Absatz 5, 8 Buchst. a und b - Begriffsbestimmungen

Eine Regulierung der sogenannten „Dienste der Informationsgesellschaft“ lehnt BITKOM ab, da es sich hierbei nicht um kritische Infrastrukturen im angesprochenen Sinne handelt. Beim Ausfall eines „Dienstes der Informationsgesellschaft“ ist in keinem Falle mit ähnlichen Auswirkungen zu rechnen wie beim Ausfall einer kritischen Infrastruktur. Eine Gleichsetzung würde den Begriff der kritischen Infrastruktur aufweichen. Weiterhin ist die in Art. 3 Abs. 8 Buchst. a gewählte Formulierung so weit auslegbar, dass eine Folgenabschätzung aus Sicht der ITK-Branche kaum noch möglich ist. Diese Dienste sollten folglich nicht von der Richtlinie erfasst werden.

Die betroffenen Marktteilnehmer sollen in Annex II in nicht abschließenden Listen aufgeführt werden. Hier erscheint aus hiesiger Sicht unklar, wie eine Erweiterung der Listen vorgenommen werden soll und wer entscheidet, wer Teil dieser Listen und damit Regulierungsobjekt ist. Eine solche Unklarheit ist im Sinne der Planungssicherheit für betroffene Sektoren auszuschließen.

3. Artikel 7 – IT-Notfallteam

BITKOM begrüßt ausdrücklich die Schaffung eines CERT, verknüpft damit aber eine weitergehende Hoffnung, nämlich die Ausbildung eines umfassenden CERT-Netzwerkes ähnlich wie in Deutschland. Deshalb sollte der Artikel um einen Absatz ergänzt werden, der einen CERT-Verbund unter Einbindung der wirtschaftsbetriebenen CERTs vorsieht. Damit wäre ein großer Schritt zu einer bestmöglichen Kooperation zwischen öffentlichem Sektor und Privatwirtschaft auch auf europäischer Ebene eingeleitet.

4. Artikel 8 Absatz 3 Buchst. f und Absatz 4 - Kooperationsnetz

Die Kommission regt in ihrem Vorschlag an, einen regelmäßigen Austausch zwischen europäischen Institutionen, die mit dem Thema Netzwerk- und Informationssicherheit betroffen sind, sicherzustellen. Dabei sollen auch europäische Institutionen eingebunden werden, die mit den betroffenen Wirtschaftssektoren befasst sind. Hier empfehlen wir – auch im Sinne einer Kooperation zwischen Staat und Wirtschaft – auch die Einbindung der entsprechenden Wirtschaftsvereinigungen, die den Austausch durch unternehmensnahe Expertise bereichern würden.

In Absatz 4 schlägt die Kommission vor, die Kooperationsmechanismen in Durchführungsrechtsakten festzulegen. Dies ist abzulehnen, da hierdurch bereits etablierte und funktionierende Mechanismen auf nationaler Ebene gefährdet werden. Die Abstimmung der Kooperationsmechanismen sollte durch die von den Staaten bestimmten Behörden und weiteren beteiligten Institutionen (auch der Privatwirtschaft) ausgearbeitet werden, um sich nah an der tatsächlichen Praxis zu orientieren und das notwendige Element der Kooperation zwischen Staat und Wirtschaft in diesem Feld abzubilden.

5. Artikel 9 Absatz 3 - Sicheres System für den Informationsaustausch

Aus Sicht des BITKOM erscheint eine Implementierung der Zugangsvoraussetzungen durch Durchführungsrechtsakte fragwürdig. Dies ist bereits im Vorfeld verbindlich festzulegen, damit keine Fehlinvestitionen getätigt werden und Staaten mit bereits vorhandenen oder geplanten sicheren Infrastrukturen keine unnötigen Neuinvestitionen tätigen müssen.

6. Artikel 10 Absatz 3, 4 und 5 - Frühwarnungen

BITKOM hält es nicht für erforderlich, dass einzelne europäische Organe innerhalb eines Kooperationsnetzwerkes zwischen Staaten das Recht eingeräumt bekommen, Fachinformationen bei den Mitgliedsstaaten abzurufen. Dies würde aus Sicht des BITKOM die Stellung der Staaten, die letztlich operativ für die Bekämpfung von Cyberrisiken verantwortlich sind, unnötig schwächen. BITKOM begrüßt ausdrücklich die Rolle der ENISA als zentraler Behörde zur Bündelung und Auswertung von Informationen zur Cybersicherheit in Europa. Aus Sicht der Wirtschaft ist insbesondere die kurzfristige Bereitstellung konsolidierter Informationen von hohem Wert. Hierbei sollten nicht ausschließlich die Meldungen von

Betreibern kritischer Infrastrukturen einbezogen werden, sondern – wo sinnvoll – ebenfalls wichtige Informationen der staatlichen Sicherheitsorgane, der staatlichen und privatwirtschaftlichen CERTs (insbesondere auch der CERTs der Bundesländer), international verfügbare Lageinformationen und sonstige Meldungen zu Cybersicherheitsvorfällen. ENISA sollte demnach nicht nur in seiner Rolle als Informationssenke, sondern insbesondere auch als Informationsquelle für alle Beteiligten, auch Wirtschaftsunternehmen, gestärkt werden. Diese erweiterte Sichtweise sollte sich dringend in einer gesetzlichen Regelung wiederfinden.

Einen Automatismus des Informationsüberganges von IT-Sicherheitsbehörden an Polizeibehörden hält BITKOM für unangemessen. So könnte das zum Beispiel in Deutschland gültige Legalitätsprinzip dafür sorgen, dass Einzelunternehmen von Meldungen absehen, da sie Auswirkungen auf den Geschäftsbetrieb durch polizeiliche Ermittlungen befürchten. Stattdessen hat sich aus unserer Sicht eine Stärkung der Ressourcen im Bereich Cybercrime bei Ermittlungsbehörden als zielführend für die Stärkung des Vertrauens der Wirtschaft erwiesen. Polizeibehörden, die im Bereich Cybercrime eine Stärkung erfahren haben, werden von den Unternehmen als vertraute und professionelle Ansprechpartner bei Cybercrime-Delikten gesehen, was zu einer freiwilligen Verbindungsaufnahme führt.

Die Festlegung der eine Frühwarnung auslösenden Ereignisse und Risiken durch delegierte Rechtsakte erscheint aus Sicht des BITKOM nicht zielführend. Um eine Flut unnötiger Meldungen zu verhindern sollte dies nicht auf Ebene der Europäischen Kommission geschehen, sondern gemeinsam zwischen den zuständigen Fachbehörden und den betroffenen Sektoren dynamisch ausgearbeitet werden, um auch der Bewegung im Bedrohungsszenario gerecht zu werden.

7. Artikel 12 - NIS-Kooperationsplan der Union

Dieser Kooperationsplan sollte nicht auf Ebene der Europäischen Kommission und durch Implementierungsrechtsakte erarbeitet werden, sondern grundsätzlich durch die Fachbehörden der Mitgliedsstaaten und die betroffenen Wirtschaftszweigen, damit sich die Zusammenarbeit nah an der Praxis weiterentwickeln kann und bereits existierende und praxiserprobte Mechanismen weitergeführt werden können.

8. Artikel 14 - Sicherheitsanforderungen und Meldung von Sicherheitsvorfällen

Grundsätzlich ist eine transparente und klare Informationspolitik im Falle von IT-Sicherheitsvorfällen richtig und wichtig. Mit Blick auf die Frage, welche konkreten Vorkommnisse zu melden sind, ist die Formulierung „[…] Sicherheitsvorfälle melden, die erhebliche Auswirkungen auf die Sicherheit der von Ihnen bereitgestellten Kerndienste haben“ aber viel zu allgemein gefasst. Hiervon könnte eine Vielzahl, wenn nicht praktisch alle Vorkommnisse betroffen, da selbst geringe und kurzzeitige Beeinträchtigungen der Funktionsfähigkeit hierzu zählen würden. Grundsätzlich muss die Meldepflicht eng zugeschnitten sein und es muss klar werden welche Informationen zu welchem Zweck an welche Empfänger übersandt werden sollen. Der Informationsaustausch selbst ist nicht Ziel, sondern

muss als Mittel zu einem bestimmten Zweck konkretisiert werden. Es darf hierbei ferner nicht um „alle Vorkommnisse, an alle möglichen Empfänger, zu jeder Zeit“ gehen.

An dieser Stelle (wie aber auch an anderen Stellen des Richtlinienentwurfes und der Erläuterungen) muss wesentlich präziser dargestellt werden, was unter einer schwerwiegenden Beeinträchtigung zu verstehen ist. Für BITKOM ist dies eine essentielle Voraussetzung, um einen schnellen Informationsfluss zu gewährleisten und eine valide Aussage über die aktuelle Cyber-Gefährdungslage treffen zu können.

Besonders kritisch erscheint dies in Zusammenhang mit Absatz 4, in dem beschrieben wird, dass die fachlich zuständige Behörde selbst und ohne Rücksprache mit dem betroffenen Marktteilnehmer entscheiden können soll, ob eine Veröffentlichung des Vorfalls im öffentlichen Interesse ist. Diese Vorgehensweise wäre dazu geeignet, eine notwendige vertrauensvolle Zusammenarbeit zwischen Verwaltung und Marktteilnehmern nachhaltig zu schädigen. Gleiches gilt für Festlegung der meldepflichtigen Ereignisse sowie der formalen Prozesse in delegierten Rechtsakten. Auch hier erscheint die Erarbeitung durch die fachlich zuständigen Behörden gemeinsam mit den Behörden der zielführendere Weg.

9. Artikel 15 Absatz 2 Buchst. b und Absatz 4 - Umsetzung und Durchführung

Absatz 2 Buchst. b spricht von der Durchführung von Security-Audits durch qualifizierte unabhängige Stellen oder nationale Behörden. Hier erscheint es aus Sicht des BITKOM unklar, wer genau damit gemeint sein wird und welche Voraussetzungen diese Stellen erfüllen müssen. Hier ist aus Sicht des BITKOM besonders zu vermeiden, dass ein Eingriff in den funktionierenden Markt für Audit-Dienstleister kommt.

Absatz 4 erscheint insofern problematisch, als dass an dieser Stelle wieder die Einrichtung eines automatisierten Informationsflusses zwischen IT-Sicherheits- und Ermittlungsbehörden befürchtet wird. Dies erscheint aus bereits ausgeführten Gründen nicht hilfreich in der Stärkung der Union gegen Cybersicherheitsrisiken.