Stellungnahme

zum Vorschlag der EU-Kommission über den Cybersecurity Act

12. Dezember 2017

Zusammenfassung

Angesichts der wachsenden globalen Bedeutung des Cyberraums, des Internets und informationstechnischer Systeme müssen Risiken und Bedrohungen der Netz- und Informationssicherheit zukünftig durch noch intensivere europäische und internationale Ansätze minimiert werden. Bitkom begrüßt daher ausdrücklich die europäischen Bemühungen um die Verbesserung der Cybersicherheit. Der Cybersecurity Act der EU-Kommission kann dabei ein wichtiger Schritt hin zu mehr Sicherheit im europäischen digitalen Binnenmarkt und zu größerem Vertrauen auch in das Internet der Dinge (IoT) sein.

Ein rechtlicher Rahmen – der Prüfverfahren zur Zertifizierung von IT-Infrastrukturen, Produkten, Dienstleistungen und Systemen auf europäischer Ebene harmonisiert – bringt zum einen Klarheit für den Verbraucher und kann zum anderen einen positiven Effekt auf das Risikomanagement in den betroffenen Unternehmen haben. Ein Ziel des Cybersecurity Acts muss es auch sein, mehr Rechtssicherheit für paneuropäisch tätige Unternehmen zu schaffen. Eine Cybersicherheitszertifizierung darf aber nicht suggerieren, dass es absolute Sicherheit gibt.

Die richtige Ausgestaltung des Rahmens birgt somit die Chance auf einheitliche Wettbewerbsbedingungen und auf die Beseitigung unterschiedlicher nationaler Zertifizierungssysteme, die den Zugang zu europäischen Märkten erschweren. Gleiche Wettbewerbsbedingungen sind für einen funktionierenden digitalen Binnenmarkt innerhalb der EU und für die internationale Wettbewerbsfähigkeit europäischer Unternehmen, für die Stärkung der Innovationsfähigkeit sowie für die Attraktivität des europäischen Standorts insgesamt unerlässlich. Infrastrukturbetreiber, Diensteanbieter und Gerätehersteller sind gleichermaßen gefordert, ihre Lösungsangebote (Produkte, Services, Infrastrukturen) so zu entwickeln, dass Schwachstellen vermieden, frühzeitig erkannt bzw. behoben und damit das Risiko von Angriffen gesenkt werden kann. Der vorgeschlagene rechtliche Rahmen kann daher nur effektiv und erfolgreich sein, wenn er grundsätzlich einen harmonisierten europäischen Raum für Zertifizierungssysteme im Bereich IT-Sicherheit schafft und dabei die gesamte Wertschöpfungskette adressiert. Der Wirtschaft sollte eine zentrale Rolle bei der Ausgestaltung zukommen und die Umsetzung selbst transparent und offen erfolgen. Die nationalen und europäischen Normungsorganisationen DIN, CEN/CENELEC und ETSI sollten eine zentrale Rolle für die Bereitstellung von Normen und Standards spielen. Sie sind mit ihren technischen Gremien sowie mit ihren internationalen Kollaborationsvereinbarungen dafür hervorragend aufgestellt.

Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Teresa Ritter
Referentin Sicherheitspolitik
T +49 30 27576-203
t.ritter@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Darüber hinaus reicht aufgrund der zunehmend globalen Bedeutung von IT-Sicherheit aber auch ein rein europäischer Bezug letztendlich nicht mehr aus. Im Sinne eines übergeordneten Sicherheits- und Harmonisierungsziels ist vielmehr eine Orientierung und Kompatibilität zu internationalen Standards unbedingt notwendig. Dies beinhaltet auch klare Regelungen für den Übergang von bestehenden Zertifizierungen.

Aus Sicht des Bitkom muss deshalb ein effektiver Zertifizierungsrahmen für IT-Infrastrukturen, Produkte, Dienstleistungen und Systeme auf europäischer Ebene folgende Punkte berücksichtigen:

1. Bei der Ausgestaltung des Rahmenwerks muss den bereits bestehenden hohen internationalen Standards und Abkommen Rechnung getragen werden.

2. Eine Unterscheidung zumindest zwischen Gütern in den Bereichen Consumer, Business, kritische Infrastruktur und Hochsicherheit, mit ggf. starker nationaler Komponente, ist dringend geboten.

3. Eine EU-weite Harmonisierung darf nicht dazu führen, dass das in einigen Mitgliedsstaaten bereits heute sehr hohe Sicherheitsniveau abgesenkt und die Zielstellung des Cybersecurity Acts damit konterkariert würde.

4. Bei der Ausgestaltung des Systems und der späteren Standards müssen die Industrie sowie nationale Behörden und Normungsorganisationen mit einbezogen werden.

5. Die Zertifizierung sollte grundsätzlich, wie im Verordnungsvorschlag vorgesehen, freiwillig sein. Im weiteren Gesetzgebungsprozess ist zu beobachten, ob durch den Zertifizierungsrahmen ausreichende Hebelwirkungen zur Einhaltung der Standards und damit zur Sicherung eines adäquaten Sicherheitsniveaus erzielt werden.

6. Zur weiteren Bewertung des vorliegenden Verordnungsvorschlags werden Vorschläge für die Ausgestaltung des Frameworks gegeben sowie ergänzende Zertifizierungsmethoden, wie beispielsweise prozessorientierte Schemata, vorgestellt.

7. Eine erweiterte Rolle der ENISA muss so ausgestaltet sein, dass Belange der nationalen Souveränität nicht beschnitten werden.

Cybersicherheitszertifizierung

Bitkom begrüßt ausdrücklich, dass mit dem Verordnungsvorschlag die Etablierung ebenso wie die notwendige Herausarbeitung eines in der EU harmonisierten und international anerkannten Frameworks zur Zertifizierung von Cybersicherheit angestoßen werden. Aus Sicht des Bitkom müssen im weiteren EU-Beschlussverfahrensprozess sieben Schlüsselelemente berücksichtigt werden:

1. Stärkerer Bezug auf bestehende internationale Prozesse und Standards:

Ein Zertifizierungsrahmen darf nicht im Sinne neuer zusätzlicher Standards verstanden werden, sondern vielmehr als ein Rückgriff auf bestehende, anerkannte Standards und Normen, die als bewährte Praktiken angesehen werden, wie beispielsweise das Common Criteria (als Standard) mit dem CCRA oder SOG-IS (als Abkommen)-MRA. Auch etablierte Cyber-Sicherheitszertifizierungen – soweit bereits in Mitgliedstaaten vorhanden – sollten, sofern sie EU-weit als bewährte Praktiken gelten, die Grundlage für eine europäische Harmonisierung bilden. Dort, wo ein europäischer Ansatz ein höheres Sicherheitsniveau verspricht als internationale Ansätze, sollte dieser im Rahmen der Standardisierung von Europa aus global vorangetrieben werden.

2. Kritikalität der unterschiedlichen Anwendungsszenarien beachten:

Bitkom unterstützt die im Vorschlag vorgeschlagenen drei Vertrauensstufen (Artikel 46). Um den unterschiedlichen Anwendungsszenarien Rechnung zu tragen, muss das Zertifizierungssystem einen risikobasierten Ansatz verfolgen, der Kontext und Kritikalität der Nutzungsszenarien mit einbezieht und zwischen den verschiedenen Risiken im Bereich der Computersicherheit unterscheidet. In diesem Rahmen fordert Bitkom eine weitere Präzisierung des mehrgliedrigen Ansatzes und empfiehlt eine strikte, auf einer individuellen Risikobewertung basierende Unterscheidung. Damit wird beispielsweise eine Differenzierung zwischen Konsumgütern und industriellen Anwendungen oder kritischen Infrastrukturen ermöglicht. Die Skalierbarkeit des Zertifizierungssystems muss auf unterschiedliche Bereiche gewährleistet sein und dem »Moving Target« bei Sicherheit Rechnung tragen. Es bedarf zudem klarer Regelungen und Garantien für den Übergang von bestehenden Zertifizierungen hinsichtlich der weiteren Nutzung von den im Einsatz befindlichen Produkten.

Insbesondere mit der zunehmenden Nutzung vernetzter Geräte im sog. »Internet der Dinge« entsteht hinsichtlich der Schaffung einer angemessenen Cybersicherheit ein zusätzlicher Handlungsbedarf im digitalen Binnenmarkt. IoT-Geräte können, wenn geeignete

Sicherheitsfeatures fehlen, prinzipiell auch als Angriffsvektoren dienen und haben durch ihr großes Verkaufsvolumen in den EU-Mitgliedsstaaten einen hohen europäischen Stellenwert. Besonders für diesen Bereich ist es erforderlich, mindestens europäische bzw. internationale Standards zu entwickeln, die unter wirtschaftlichen Rahmenbedingungen zu vertrauenswürdigen Produkten führen. Hochsicherheitsanwendungen – wie beispielsweise Verschlüsselungsprodukte für den hoheitlichen Einsatz, die Auswirkungen auf den Schutz nationaler öffentlicher Sicherheit haben – müssen unbedingt in der Kompetenz der nationalen Behörden bleiben.

Von Überlegungen, wie sie in Erwägungsgrund 62 vorgetragen werden – Einbindung einer mit erweiterten Kompetenzen ausgestatteten ENISA in nationale kryptographische Zulassungsverfahren – rät Bitkom ab. Diese Themen betreffen den Kern des nationalen Government-Bereichs. Hier muss die nationale Souveränität gewahrt werden.

3. Gewährleistung eines angemessenen Sicherheitsstandards

Eine EU-weite Harmonisierung darf nicht dazu führen, dass bereits erreichte hohe und allgemein für sinnvoll erachtete Standards abgesenkt werden. Dadurch würde das Ziel dieser Initiative, mehr Cybersicherheit in Europa zu schaffen, konterkariert werden. Neben der Berücksichtigung bewährter internationaler und nationaler Standards und Abkommen hält Bitkom folgende Punkte für wichtig:

Bitkom unterstützt die Bildung der Europäischen Gruppe für die Cybersicherheitszertifizierung (im Folgenden die Gruppe), wie in Artikel 53 beschrieben. Um einer qualitativ hochwertigen Besetzung Rechnung tragen zu können, empfiehlt Bitkom aber, die vorhandene Kompetenz, Erfahrung und Infrastruktur im Bereich der Cybersicherheit in den jeweiligen Mitgliedsländern zu berücksichtigen und auf den in einigen Ländern vorhandenen hohen Sicherheitsstandards aufzusetzen. Eine Nichtbeachtung dieser Komponenten birgt die Gefahr eines Herabsinkens des in einigen EU-Ländern bereits hohen Sicherheitsstandards.

Es besteht Konsens, dass die Berücksichtigung von »Security by Design«-Prinzipien besonders für die Datensicherheit im Internet der Dinge unerlässlich ist. Deshalb muss aus Sicht des Bitkom »Security by Design« auch Grundelement der Prüfverfahren innerhalb eines europäischen Zertifizierungsrahmens sein. Die Herangehensweise sollte dabei generischer Natur sein, da die meisten Sicherheitsvorfälle auf der Tatsache basieren, dass die betroffenen Geräte noch nicht einmal die grundlegendsten Sicherheitsanforderungen erfüllen. Darüber hinaus ist ein solcher Ansatz von Anfang an flexibel auf die sich ändernden technischen Gegebenheiten einzelner Produkte anpassbar.

4. Stärkere Beteiligung der Industrie, nationaler Behörden und Normungsorganisationen

Freiwillige Initiativen der Wirtschaft sind eine der wesentlichen Säulen der Verbesserung der IT-Sicherheit. Deshalb fordert Bitkom, dass EU-weite Zertifizierungsregelungen in Zusammenarbeit mit den einschlägigen Interessengruppen und damit unter Beteiligung der Industrie entwickelt werden. Der derzeitige Vorschlag sieht eine sehr begrenzte Beteiligung der Industrie an der Ausarbeitung und Annahme von Zertifizierungsregelungen vor. Um ein hohes Qualitätslevel an IT-Sicherheit realisieren zu können, fordert Bitkom, dass neben der Kommission und der Gruppe sowohl die Industrie direkt als auch nationale und europäische Normungsorganisationen (DIN, CEN/ CENELEC, ETSI) in die Ausarbeitung der Regulierungen mit einbezogen werden, beispielweise als Teil »der Gruppe«. Europäische und internationale Standards, die in einem Vollkonsensprozess entwickelt wurden, müssen dann die Basis für die Zertifizierung bilden. Auf diese Weise wird die Offenheit des Prozesses garantiert; ebenso bietet die Standardisierung den besten Weg, um Innovationen im Bereich Cybersicherheit schnell und zuverlässig verfügbar zu machen.

5. Freiwilligkeit der Zertifizierung

Der Verordnungsvorschlag sieht eine Freiwilligkeit der Zertifizierung vor (Artikel 48, Paragraph 2). In den Mittelpunkt der zu führenden Diskussion sollten neben der Ausgestaltung der Zertifizierung – ob verpflichtend oder nicht – auch die Notwendigkeit der Standardharmonisierung gestellt werden. Verpflichtende Regulierungen könnten als Markteintrittsbarriere wirken und Innovationen behindern. Gleiche Wettbewerbsbedingungen sind aber eine Voraussetzung für die globale Wettbewerbsfähigkeit der europäischen Industrie. Neben der Erreichung eines adäquaten Sicherheitslevels, sind gleiche Wettbewerbsbedingungen deshalb essenziell. Dieser Dualismus sollte bei der Ausgestaltung des gesamten Systems immer Ausgangslage der Überlegungen sein.

Der Verordnungsvorschlag schränkt die Freiwilligkeit der Zertifizierung allerdings dahingehend ein, dass im Unionsrecht nichts anderes bestimmt ist (Artikel 48, Absatz 2, zweiter Halbsatz). Nach dem Verständnis von Bitkom könnte diese Regelung vor allem dann greifen, wenn die freiwillige Zertifizierung nicht zum gewünschten Ziel, namentlich der Cybersicherheit von IKT-Produkten und –Dienstleistungen und der Stärkung des Vertrauens in den digitalen Binnenmarkt, führt. Die Regelung erscheint daher zunächst verständlich. Gleichsam besteht dann aber die Gefahr, dass, als Reaktion auf eine gescheiterte freiwillige Zertifizierung, unverhältnismäßige Maßnahmen folgen könnten. Die Regelung öffnet die Tür für eine verpflichtende Zertifizierung durch Konformitätsbewertungsstellen im Sinne des Art. 51 auf der Grundlage von Anforderungen zur Cybersicherheit, die zunächst nur für eine freiwillige Zertifizierung vorgesehen waren. Hiervon rät Bitkom ab. Vielmehr

sollten bei der notwendigen Ausgestaltung von einzelnen Standards und deren Einhaltung die jeweiligen Hebelwirkungen zur Erreichung eines adäquaten Sicherheitsniveaus im Zentrum der Diskussion stehen. Diese können neben Mindestanforderungen an die Lösungsangebote von Infrastrukturbetreibern, Diensteanbietern und Geräteherstellern insbesondere andere Maßnahmen sein, die zur Erreichung der Sicherheitsziele ebenfalls geeignet erscheinen und die Grundfreiheiten des Binnenmarkts weniger einschränken. Hierüber fordert Bitkom eine intensive Fachdiskussion im weiteren Gesetzgebungsprozess.

6. Ausgestaltung des Frameworks und ergänzende Zertifizierungsmethoden

Das Framework sollte abgestufte Bereiche für verschiedene Sektoren beinhalten. Zumindest für diese verschiedenen Sektoren sollten internationale Standards gewählt werden, der Bereich nationaler Sicherheit ist weiterhin nationalen Regelungen zu unterstellen. Für die Ausgestaltung von den jeweiligen Sicherheitsanforderungen sollten internationale Standards gewählt werden, welche anwendungs- und zielgruppenbezogen die optimalen Anforderungen zur jeweiligen Cybersicherheitszertifizierung beinhalten.

Zudem sollte die Sicherheitszertifizierung wenn möglich auch aus Prozesssicht erfolgen, welche Anforderungen an den Entwicklungsprozess eines Herstellers stellt. Eine Produktzertifizierung, die sich auf eine konkrete Version bezieht und eine teilweise Wiederholung der Prüfung nach einer Aktualisierung des Produkts erfordert, würde insbesondere bei cloudbasierten Anwendungen an ihre Grenzen stoßen, sowohl hinsichtlich des Zeitrahmens als auch des Aufwandes. Bitkom empfiehlt daher, neben produktfokussierten Schemata auch prozessorientierte Schemata als Ergänzung in einem europäischen Sicherheitszertifizierungsrahmen vorzusehen, vorausgesetzt solche Ergänzungen führen zu einem vergleichbar hohen Sicherheitsniveau unter Berücksichtigung der Kritikalität der jeweiligen Anwendung. Um ein hohes Sicherheitsniveau zu gewährleisten, sollte ein Prozesszertifikat zum Ausdruck bringen, dass die sicherheitsbezogenen Entwicklungs- und Betriebsprozesse hohen Qualitätsansprüchen genügen und dem Stand der Technik entsprechen. Existierende internationale Standards, die diesen Ansatz verfolgen (z. B. ISO 27034 für Applikationssicherheit), sollten als Grundlage eines prozessorientierten Schemas herangezogen werden. Um Transparenz und Vergleichbarkeit zu gewährleisten, muss in einem weiteren Schritt klar geregelt werden, für welchen Fall, welche Art von Schema (produktfokussiert oder prozessorientiert) anzuwenden ist.

7. Erweiterte Rolle der ENISA

Die angedachte erweiterte Rolle der ENISA ist grundsätzlich begrüßenswert. Die Aufwertung der Agentur ist insbesondere im Zuge einer weiteren Harmonisierung der Cyber-Sicherheitsmaßnahmen im gesamten digitalen Binnenmarkt der EU von Bedeutung. Mit

einem ständigen Mandat kann sie die Zusammenarbeit zwischen den Mitgliedstaaten, bei der Vorbereitung und Bewältigung grenzüberschreitender Herausforderungen im Bereich der Cybersicherheit in der EU, besser koordinieren.

Deshalb ist es ein positiver Schritt, wenn eine finanziell und personell aufgewertete ENISA künftig die operationelle Koordination der genannten Zusammenarbeit, den Aufbau von Abwehrfähigkeiten sowie den Austausch von Informationen (Info-Hub) – auch im direkten Austausch mit Unternehmen – vorantreiben soll. Mit diesen Maßnahmen wäre ein größerer Grad an Harmonisierung und Rechtssicherheit im digitalen Binnenmarkt zu erreichen.

Laut Artikel 3 Paragraph 3 des Verordnungsvorschlags bleiben die Zuständigkeiten der Mitgliedsstaaten in Bezug auf die Öffentliche Sicherheit unberührt. Dies unterstützt Bitkom in vollem Umfang. Den Mitgliedsstaaten muss ein effektives Maß an Eigenständigkeit erhalten bleiben und zwar überall dort, wo Belange der nationalen Sicherheit berührt sind. Dies sollte auch für den Bereich des angestrebten Zertifizierungsrahmens gelten. Hier ist der Vorschlag noch zu unscharf formuliert. Damit dieses Argument im Sinne der Subsidiarität von den Mitgliedstaaten genutzt werden kann, müssen hier klare Regelungen getroffen werden. Ein gewisses Maß an Eigenständigkeit darf indes nicht bedeuten, dass dadurch regulatorische Lücken entstehen, die letztlich dazu führen, dass innerhalb der EU doch wieder ein fragmentiertes Cybersicherheitssystem entsteht. Darüber hinaus ist wichtig zu beachten, dass bei der personellen Aufwertung der ENISA Qualität – und nicht Quantität – im Vordergrund steht.

Fazit

Die in dem Verordnungsvorschlag formulierten Schritte können unter Berücksichtigung der oben genannten Punkte einen wesentlichen Beitrag zur Stärkung der IT-Sicherheit in Europa leisten. Größtes Anliegen sollte es aber sein, sich nicht alleine auf den europäischen Markt zu konzentrieren, sondern anzufangen, international zu denken. Diese internationale Dimension erstreckt sich dabei nicht nur auf die Entwicklung und Harmonisierung von Standards. Im Rahmen des B20-Prozesses haben Unternehmen weltweit die internationale Staatengemeinschaft aufgefordert, Normen für ein verantwortungsvolles staatliches Verhalten im Bereich Cybercrime zu entwickeln. Eine wesentliche Norm ist die Verpflichtung jedes Staates, sich konsequent gegen jede Art von Cyberkriminalität zu stellen, die von ihrem Territorium ausgeht. Hier kann und sollte die EU treibende Kraft werden.

Darüber hinaus fehlt dem Bitkom ein breit gefasster Ansatz, der auch die Verbraucher und Anwender mit in den Fokus nimmt. Für weitere Gesetzesvorhaben empfiehlt Bitkom deshalb künftig über Strategien zur Steigerung der IT-Sicherheit nachzudenken, welche ein

Zusammenspiel von mehreren Instrumenten zulassen. Zertifizierung ist immer nur eine Momentaufnahme und lässt künftige technische Entwicklungen sowie die Veränderung der Umwelt außer Acht. Deshalb ist es von besonderer Wichtigkeit, Zertifizierungsverfahren zu beschleunigen, handhabbarer zu machen und sie so auszugestalten, dass sie neben der damit geförderten hohen Produktqualität auch stärker auf die damit verbundene Verbesserung der Prozesse im Hinblick auf sichere IT-Entwicklung innerhalb der Unternehmen achten. Gleichzeitig muss klar sein, dass eine reine Zunahme der Anzahl Zertifizierungsstellen nicht automatisch zu einer Beschleunigung führt.

Notwendig erscheint außerdem, den »Cybersecurity Act« im Kontext der seitens der EU-Kommission und der Hohen Vertreterin für Außen- und Sicherheitspolitik in einer gemeinsamen Mitteilung parallel vorgestellten neuen Cybersicherheitsstrategie »Resilience, Deterrence and Defence: Building strong cybersecurity in EU« zu betrachten. Gerade für den Hochsicherheitsbereich sollte der Cybersecurity Act in den Kontext der sich gerade weiterentwickelnden gemeinsamen Sicherheits- und Verteidigungspolitik gesetzt werden, der auf den Stärken der unterschiedlichen Mitgliedsstaaten aufsetzt.