Positionspapier

Anforderungen an eine kohärente Regulierung der Cybersicherheit

07.06.2019

Zusammenfassung

Die Digitalisierung all unserer Lebensbereiche bringt Vorteile für Konsumenten und Chancen für die Wirtschaft. Durch die allgegenwärtige Konnektivität können Verbraucher mehr Lebenskomfort genießen. Durch Zeit- und Kosteneinsparung steigt die Produktivität der Wirtschaft. Aufgrund dieser enormen Potentiale will die Digitalbranche das neueste Kapitel der digitalen Transformation aktiv mitgestalten.

Aber nicht nur Verbraucher und Unternehmen profitieren von Vernetzung und Digitalisierung. Gleichzeitig bietet die wachsende Anzahl von vernetzten Geräten (speziell auch IoT-Geräten), die zunehmende Komplexität digitaler Systeme, fehlerhafte Software und schließlich auch die Sorglosigkeit oder Unerfahrenheit der Anwender digitaler Dienste eine größere Angriffsfläche für Cyber-Kriminelle. Die Aussicht auf finanziellen Gewinn bei sehr geringem Risiko für den Angreifer – z. B. im Falle von Ransomware durch Erpressung der Angriffsopfer – macht Cyberangriffe immer lukrativer. Deshalb stellen wir gerade bei Sicherheitsfragen einen ernst zu nehmenden Anstieg von Angriffen und ein noch wesentlich höheres Bedrohungspotenzial fest. Unser Ziel sollte es daher sein, die Angriffsfläche zu reduzieren. Hersteller und Anwender, Infrastrukturbetreiber und Strafermittlungsbehörden müssen gemeinsam darauf hinwirken die Angriffsfläche so gering wie möglich zu halten.

Regulierung sollte dabei als Rahmenwerk fungieren, innerhalb dessen Unternehmen über alle Branchen hinweg IT-Sicherheit bei der Produktentwicklung beachten, ihre Produkte hinreichend auf Sicherheitslücken überprüfen und Sicherheitsupdates für gemeldete Sicherheitslücken bereitstellen. Der Gesetzgeber muss aber auch sicherstellen, dass sich Regulierungen gegenseitig ergänzen und die den Regulierungen unterworfenen Unternehmen Handlungssicherheit bei der Entwicklung und Vermarktung ihrer Produkte erhalten.

Auf den folgenden Seiten betrachten wir zum einen bestehende Regulierungen auf europäischer Ebene und geben zum anderen Denkanstöße für künftige Entwicklungen im Bereich der Gesetzgebung für IT-Sicherheit. Als Grundlage dieser Betrachtungen wurden fünf Forderungen entwickelt, welche aus Sicht des Bitkom die essenziellen Voraussetzungen für Regulierung im Bereich Cybersicherheit darstellen.

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

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

Dr. Katharina Eylers
Referentin Umweltpolitik und technische Regulierung
T +49 30 27576-220
k.eylers@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

1. Konsistenz gesetzlicher Anforderungen

Neue Regulierung sollte stets nur Bereiche erfassen, in denen Regelungslücken bestehen, um überlappende legislative Anforderungen für dasselbe Produkt zu vermeiden. Sofern sich Regelungsbereiche überlappen, muss die inhaltliche Konsistenz aller Anforderungen und Klarheit hinsichtlich der Zuständigkeiten (insbesondere von Aufsichtsbehörden) sichergestellt sein.

2. Gleiche Anforderungen in der EU – Sicherstellen des einheitlichen Binnenmarkts

Anforderungen an die Cybersicherheit müssen EU-weit harmonisiert sein. Es darf weder zu Fragmentierungen im europäischen Binnenmarkt führen, noch nationale Sonderwege geben. Idealerweise sind die Anforderungen dabei auch global kompatibel. So wird ein einheitlicher Digitaler Binnenmarkt und die globale Wettbewerbsfähigkeit sichergestellt und erweitert.

3. Anforderungen domänenspezifisch und dabei horizontal konsistent

Gute Cybersicherheitsanforderungen folgen produktübergreifend den gleichen Prinzipien beschreiben aber innerhalb der einzelnen Produktkategorien auf diesen Bereich angepasste und zurechtgeschnittene konkrete Anforderungen, die auch bestehende Anforderungen oder Regulierung in diesen Domänen berücksichtigen. Dabei muss sichergestellt werden, dass die Sicherheitsanforderungen kohärent sind und domänenübergreifende Produkte (oder Produkte, die in mehr als einer Domäne eingesetzt werden können) nicht inkonsistenten Anforderungen ausgesetzt sind. An dieser Stelle wird es im besonderen Maße darauf ankommen, dass unterschiedliche domänenspezifische Anforderungen auf eine gemeinsame Basis im Sinne des Standes der Technik zurückgreifen können.

4. Risikobasierte und dem bestimmungsgemäßen Gebrauch entsprechende Anforderungen

Angemessene risikobasierte Sicherheitsanforderungen sollten anhand der möglichen Schäden und der Eintrittswahrscheinlichkeit in den vorhersehbaren Anwendungsfällen definiert werden. Die Sicherheitsanforderungen und der Aufwand für die Maßnahmen zur Umsetzung sollten an die Größe des Risikos angepasst werden. Die Sicherheitsanforderungen sollten entsprechende Anforderungen aus domänenspezifischer Standardisierung berücksichtigen.

5. Agilität und technische Exzellenz der Anforderungen durch Nutzung der europäischen Standardisierungsorganisationen (ESOs)

Die digitale Industrie verfügt über eine langjährige Erfahrung im Umgang mit Cybersicherheit bei der Suche nach Lösungen und bei der Entwicklung von Produkten, die sowohl ihre Geräte als auch ihre Nutzer schützen. In den nationalen und europäischen Standardisierungsorganisationen werden von Experten aus Industrie, Wirtschaft, und Wissenschaft

des jeweiligen Fachgebiets Standards nach transparenten und demokratischen Verfahren nach dem neusten Stand der Technik entwickelt und aktualisiert. Um die Wettbewerbsfähigkeit der Industrie zu stärken, sollte der Verweis auf diese harmonisierten europäischen Standards Vorrang haben. Dadurch werden Unsicherheiten für die Marktteilnehmer reduziert, die Akzeptanz gesteigert, der Grad der direkten technischen Umsetzbarkeit erhöht und die Aktualität der Anforderungen sichergestellt.

Im Folgenden möchten wir auf zwei wichtige Bausteine der europäischen Regulierung – dem Cybersecurity Act (CSA) und dem New Legislative Framework (NLF) – näher eingehen, um deren Mehrwerte für eine Regulierung zur Erhöhung des Niveaus der Cybersicherheit hervorzuheben. Im Anschluss wird aufgezeigt, wie ein konsistentes Zusammenspiel innerhalb der einzelnen Regulierungen sowie zwischen CSA und NLF basierend auf den zuvor genannten fünf Prinzipien möglich wird.

Der Cybersecurity Act (CSA)

Auf EU-Ebene wurde Anfang 2019 der Cybersecurity Act (CSA) beschlossen. Der CSA etabliert einen rechtlichen Rahmen, der Verfahren der Konformitätsbewertung (einschließlich Zertifizierung) von Produkten, Dienstleistungen und Systemen auf europäischer Ebene harmonisiert. In sogenannten Konformitätsbewertungsschemata werden Anforderungen an Cybersicherheit formuliert, gegen die Geräte, Dienstleistungen und Prozesse freiwillig geprüft und ggf. zertifiziert werden können. Die Erklärungen und Zertifikate gelten in jedem europäischen Mitgliedsstaat und substituieren inhaltsgleiche nationale Schemata.

Der Cybersecurity Act kann zum einen Klarheit für den Verbraucher bringen und zum anderen mehr Einheitlichkeit für paneuropäisch tätige Unternehmen schaffen. Er ist damit ein wichtiger Schritt hin zu mehr Sicherheit im europäischen digitalen Binnenmarkt und zu größerem Vertrauen auch in das Internet der Dinge (IoT). Insbesondere im Consumer-Bereich besteht aufgrund der rasant steigenden Zahl an vernetzten Geräten der Bedarf nach Transparenz und Vergleichbarkeit, um weiterhin sichere Produkte auf den europäischen Markt zu bringen.

Wo nötig, können begleitend zur freiwilligen Konformitätsbewertung verbindliche Anforderungen in Abhängigkeit zur jeweiligen Produktkritikalität geschaffen werden. Hierfür sollte im Bereich vernetzter Produkte auf sich bereits bewährte Konzepte der Produktregulierung zurückgegriffen werden, z. B. das New Legislative Framework (NLF).

Das New Legislative Framework (NLF)

Der Neue Rechtsrahmen (das sog. „New Legislative Framework“, kurz NLF) als Regulierungskonzept zur technischen Harmonisierung im EU-Binnenmarkt ermöglicht Flexibilität bezüglich der Konformitätsbewertungsverfahren und auch die Einbeziehung von Interessengruppen im Rahmen der Normung. Dieses System hat sich in den letzten Jahrzehnten erfolgreich bewährt und ist es wert, für die Zukunft erhalten zu werden, insbesondere angesichts der sich schnell verändernden Rahmenbedingungen in der Evolution der Digitalisierung.

Das NLF-Konzept hat in vielen Produktbereichen (Maschinen, Spielzeug, elektronische Konsumgüter), sowohl durch sektorale (z.B. Maschinenrichtlinie) als auch durch horizontale Regulierungen (z.B. Richtlinie zur Elektromagnetischen Verträglichkeit) zur Verbesserung der Wettbewerbsfähigkeit der EU beigetragen und das Innovationspotential gesichert. Falls verpflichtende Anforderungen angemessen sind, ist dieses System daher geradezu prädestiniert die neuen Herausforderungen der Cybersicherheit im Rahmen der Digitalisierung zu bewältigen und eine regulatorische Basis für vernetzbare Produkte im EU-Binnenmarkt zu schaffen.

Nachdem dem NLF werden in den EU-Richtlinien nur grundlegende Anforderungen definiert (z.B. die Produkte können sicher genutzt werden und ihr Betrieb beeinflusst keine anderen Geräte störend), während die konkrete technische Ausgestaltung als mandatierte Harmonisierte Normen unter Beteiligung der Industrie in den europäischen Normungsorganisationen (CEN-CENELEC, ETSI) erfolgt. Alle Produkte, auf die diese Richtlinien zutreffen, müssen die darin vorgeschriebenen grundlegenden Anforderungen einhalten, um in der EU in Verkehr gebracht werden zu können.

In zahlreichen Produktrichtlinien hat der europäische Gesetzgeber eine Revision des Regulierungsinhalts dieser Richtlinien bei ihrem Erlass festgeschrieben. Dadurch wird es in den kommenden Jahren zu einer Überarbeitung kommen. Derzeit werden die produktspezifischen Richtlinien 2014/53/EU (Funkanlagenrichtlinie) und 2006/42/EG (Maschinenrichtlinie) dahingehend untersucht, ob Cybersicherheit mit aufgenommen werden soll.

Aufgrund der steigenden Relevanz von Cybersicherheit für vernetzte Produkte begrüßt der Bitkom das grundsätzliche Vorhaben, die Cybersicherheit von vernetzten Produkten zu stärken. Der Bitkom ist der Meinung, dass sich die Aufnahme von Cybersicherheitsanforderungen grundsätzlich dazu eignet, die Schutzziele der einzelnen Richtlinien, die unter den NLF fallen, zu ergänzen. Es besteht jedoch die Gefahr, dass bei der Überarbeitung oder Ergänzung von bestehenden produktgruppenspezifischen Richtlinien keine einheitlichen Anforderungen definiert werden, sondern heterogene, oder sogar widersprüchliche Cyber-

sicherheitsanforderungen für Produktkategorien, die mehreren Rechtsakten unterfallen, zu erwarten sind. Dies wäre insbesondere der Fall, wenn wie derzeit bei der Funkgeräterichtlinie geplant, delegierte Rechtsakte erlassen würden, die ja nur im Rahmen der existierenden Richtlinie formuliert werden können. Im legislativen Prozess zwischen Kommission, Europäischem Parlament und Rat darf nicht auf Grund von divergierenden Interessenlagen eine Inkonsistenz der überarbeiteten Richtlinien auftreten, eine Fragmentierung ist in jedem Fall zu vermeiden.

Das Zusammenspiel von NLF und CSA

Wie bereits aufgezeigt müssen die fünf genannten Prinzipien bei der Erarbeitung und Bewertung von Regulierung im Bereich der IT-Sicherheit Berücksichtigung finden und daher sowohl bei der oben genannten Überarbeitung innerhalb des NLF als auch bei der Entwicklung von Konformitätsbewertungsschemata gemäß des CSA beachtet werden.

Zudem muss – selbst bei einer guten legislativen Kohärenz innerhalb der beiden Systeme – weiterhin Konsistenz zwischen NLF und dem CSA und seinen zukünftigen Schemata sichergestellt werden. Widersprüchliche Anforderungen zwischen dem NLF und dem CSA müssen verhindert werden, auch wenn die Zertifikate und Verfahren innerhalb des CSA bisher freiwillig sind.

Wie bereits beschrieben, können über die vertikalen Richtlinien hinweg konsistente sektorübergreifende Vorgaben seitens NLF zur Gewährleistung der Cybersicherheit dienen und für alle Anwendungsbereiche gleichermaßen gelten. Ungeachtet dessen, können vertikal je nach Anwendungskritikalität und Eintrittswahrscheinlichkeit weitere Cyber-Schutzmaßnahmen notwendig sein. Diese Anforderungen sollten zueinander konsistent sein. Dabei können Verweise in die eine oder andere Richtung hilfreich sein.

Letztlich wäre es in einem Zielbild vorstellbar und wünschenswert, wenn materiellrechtliche Anforderungen an Produkteigenschaften i.S. des jeweiligen Standes der Technik zentral an einem Ort entwickelt würden, so dass entsprechende Regulierung lediglich einen Ordnungs- und Anwendungsrahmen vorgeben. Dies würde in einem hohen Maße die Entwicklung konsistenter Security-Ansprüche begünstigen und gleichzeitig ordungspolitische Spielräume eröffenen, um einen notwendigen horizontalen und bedarfsweise vertikalen Regulierungsrahmen zu schaffen.

Bitkom vertritt mehr als 2.600 Unternehmen der digitalen Wirtschaft, davon gut 1.800 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.