VERBAND DER INTERNETWIRTSCHAFT E.V.

Haftung für IT-Sicherheit - Ein Ansatz für die Regulierung

Berlin, 15. April 2019

Die politische Debatte um neue Haftungsregeln für IT-Sicherheit ist in vollem Gange. Verschiedene Akteure bringen ihre Interessen und Anforderungen an gesteigerte Ansprüche an die Sicherheit und Integrität ihrer Systeme in einer zunehmend vernetzten Welt ein. Geführt wird diese Debatte vor dem Hintergrund wachsender Sorgen über IT-Zwischenfälle und deren möglicher Auswirkungen. Durch den breiteren Einsatz von IT-Systemen werden immer neue Anforderungen an Dienste, Produkte, Netze, aber auch an deren Nutzer und Anwender gestellt. Ein stärkerer regulatorischer Druck und der Wunsch nach rechtlicher Klarstellung ist nicht nur im Fokus von Anwendern, Verbraucherschützern und Regierungen. Auch Unternehmen und Internetwirtschaft benötigen Rechtssicherheit. Dafür ist es erforderlich, eine klare Zuordnung von Verantwortlichkeiten, Haftungsumfang und –adressaten vorzunehmen.

Umfassendere und maßgebliche Regulierung existiert in Deutschland einerseits durch das 2015 verabschiedete und 2017 ergänzte IT-Sicherheitsgesetz, sowie durch den kürzlich verabschiedeten Cybersecurity Act der Europäischen Union (COM(2017) 477 final), der in Deutschland unmittelbar anwendbar wird. Neben der verstärkten Regulierung der Auflagen für IT-Sicherheit stellt sich damit auch die Frage, wie diese zusätzlichen Regeln für IT-Sicherheit mit der bestehenden Systematik der gesetzlichen Ansprüche und Haftungsregeln zusammenwirken, inwieweit und wo Haftungsfälle ausgelöst werden und wem in welchem Fall die Verantwortlichkeit zugeschrieben werden muss. Es existieren bereits Haftungsregeln, die auch schon jetzt auf digitale Technologien angewendet werden, so dass sich sowohl die Frage nach etwaigen Regelungslücken als auch nach möglichen Klarstellungsbedarfen stellt.

eco - Verband der Internetwirtschaft hat sich dieses Themenkomplexes angenommen und zusammen mit seinen Mitgliedsunternehmen die nachstehenden Vorschläge formuliert.

I. Herausforderungen für Haftungsregeln bei der IT-Sicherheit

Regulierung muss einem bestimmten Ziel folgen. Die nachstehend formulierten Ziele sind aus Sicht der Internetwirtschaft zentral für eine sinnvolle und zweckmäßige Regulierung von IT-Sicherheit und sollten im Weiteren bei der Erarbeitung von Regulierungsmaßnahmen berücksichtigt werden. Dabei sollte auf bereits etablierte Prinzipien in Haftungsfragen zurückgegriffen werden. Haftung ist nur für Risiken zulässig, die im Verantwortungsbereich oder unter der Kontrolle des potentiellen Adressaten liegen. Der Umfang der Haftung muss im Verhältnis zum wirtschaftlichen Interesse des Adressaten stehen. Auch sind sachgemäße

Exkulpationsmöglichkeiten vorzusehen, z. B. wenn ein Endnutzer sich weigert ein sicherheitsrelevantes Update aufzuspielen.

- **Haftungsregeln für IT-Sicherheit sollen die Verbesserung der Sicherheit in Netzwerken fördern**
  Elementar ist, dass Haftungsregeln für IT-Sicherheit eine tatsächliche Verbesserung von Sicherheit an Produkten, Diensten und Netzen bewirken und ggf. offene Fragen der Verantwortungszuweisung klären. Pauschale Forderungen mit möglicherweise drakonischen Strafen, deren Adressaten unter Umständen nicht klar zuordnungsfähig sind, helfen nicht weiter. Symbolpolitik würde Nutzerinnen und Nutzern möglicherweise anfangs eine „gefühlte“ Verbesserung der Sicherheit geben, am Ende aber insgesamt das Vertrauen in digitale Technologien schwächen. Es gilt, Rahmenbedingungen zu schaffen, die dazu führen, dass alle Beteiligten geeignete technische und organisatorische Maßnahmen ergreifen, um ihre Systeme, Dienste, Produkte und Netze zu schützen.

- **Haftungsregeln für IT-Sicherheit müssen Offenheit und Interoperabilität digitaler Systeme berücksichtigen und bewahren**
  Informationstechnologie und digitale Infrastrukturen sind in den allermeisten Fällen offen angelegt und interoperabel konzipiert. Anwender und Nutzer haben die Möglichkeit, eigene Geräte miteinander zu vernetzen und eigene Software auf Endgeräten einzurichten, zu betreiben und unter Umständen auch anderen zur Verfügung zu stellen. Hersteller und Entwickler können auf einem recht freien Markt eigene Technologieplattformen anbieten oder auf offene Plattformen aufsetzen. Dieses Prinzip ist die Voraussetzung für offene, interoperable digitale Infrastrukturen und befördert den Wettbewerb. Haftungsregeln für IT-Sicherheit sollten diese Freiheit und Offenheit und die damit verbundenen Herausforderungen für Hard- und Softwareentwickler und insbesondere Netzbetreiber im Hinblick auf Interoperabilität berücksichtigen.

- **Mögliche Arten der Haftung für IT-Sicherheit**
  Zunächst ist eine Abgrenzung verschiedener Arten der Haftung für IT-Sicherheit vorzunehmen. Je nach Art der Leistung (wie Hardware mit vorinstallierter Betriebssoftware oder elektronischer Kommunikationsdienst, etc.) und Art des Vertrages kommen die Grundgedanken der Produkthaftung, die Grundsätze des kaufrechtlichen Gewährleistungsrechts und schließlich allgemeine vertragliche sowie gesetzliche Haftungsgrund-sätze in Betracht. Die Art des Vertrages spielt u. a. hinsichtlich der Übertragbarkeit der Grundgedanken und Prinzipien eine wichtige Rolle, ebenso aber die Frage, ob es sich um ein Dauerschuldverhältnis handelt oder auf den einmaligen Austausch von Leistung und Gegenleistung, wie bei einem Kaufvertrag. Produkthaftung in diesem Sinne richtet sich auf die Erwartungen der Allgemeinheit an die Sicherheit des Produktes. Abgesichert werden dadurch die Integritätsinteressen des Benutzers und von Dritten bzgl. anderer

hochrangiger Rechtsgüter vor dem Produkt selbst, die davon allgemein berechtigterweise erwartet werden können.
Gewährleistung hingegen bezieht sich auf die Gebrauchs- und Funktionsfähigkeit des Produktes und seinen Wert. Geschützt wird das ökonomische Nutzungs- und Äquivalenzinteresse des Vertragspartners an der Gebrauchs- und Funktionsfähigkeit des Produktes und dessen Wert im Verhältnis zur Gegenleistung. Unter allgemeine vertragliche sowie gesetzliche Haftungsgrundsätze fallen z. B. vertragliche Ansprüche hinsichtlich Mangelfolgeschäden und gesetzliche wg. deliktischem Handeln.

- **Beispiele**
  Beim Kauf von Hardware mit vorinstallierter Betriebssoftware dürften, ggfs. mit leichten Anpassungen, die Grundgedanken der Produkthaftung und des kaufrechtlichen Gewährleistungsrechts auch auf die Betriebssoftware anwendbar sein. Die Folge sollte sein, dass während der gesetzlichen Gewährleistungszeit sicherheitsrelevante Updates angeboten werden und darauf hingewiesen wird. Soweit die Hardware mit vorinstallierter Betriebssoftware Endnutzern von Unternehmen im Rahmen eines Dauerschuldverhältnisses überlassen wird, sollten die überlassenden Unternehmen zur Bereitstellung der sicherheitsrelevanten Softwareupdates verpflichtet werden und haften.

  Wird ein elektronischer Dienst auf Grundlage eines Dauerschuldverhältnisses erbracht, steht der Anbieter für Gebrauchs- und Funktionsfähigkeit des Dienstes während der Laufzeit des Vertrages ein. Währenddessen sollte bei Bekanntwerden von Lücken oder Fehlern in der Software, die geeignet sind, das Integritätsinteresses des Endnutzers zu beeinträchtigen, sollte der Anbieter des Dienstes auch für den Schutz des Systems (Hardware) des Endnutzers einzustehen haben.

  Diese Beispiele illustrieren, dass sich eine sachgerechte und sinnvolle Auswahl einer Haftungsart immer nach dem jeweiligen Geschäftsmodell der Marktakteure richtet und untrennbar mit der Auswahl des sachgemäßen Adressaten der jeweiligen Haftungsart verbunden ist. D. h., vor der Ermittlung des konkreten Adressaten ist abzugrenzen, hinsichtlich welchen Marktauftretens welche Art von Haftung sachgerecht ist. Zu beachten ist, dass eine verschuldensunabhängige Gefährdungshaftung nur die absolute Ausnahme und ausschließlich zum Schutz hochrangiger Rechtsgüter (wie Leben oder Gesundheit) zulässig ist.

- **Haftungsregeln für IT-Sicherheit sollten sachgerecht adressiert sein**
  Die Verantwortung für IT-Sicherheit muss in einer Haftungsregelung adäquat adressiert werden. Eine Inanspruchnahme über den sinnvoll abbildbaren Verantwortungsbereich hinaus trägt nicht zur Verbesserung der IT-Sicherheit von Produkten und Netzen bei, sondern setzt falsche Anreize und ist leere Symbolpolitik. Bei Leistungen gegen Entgelt erscheint es grundsätzlich sachgerecht, den jeweiligen Anbieter im Sinne von Haftung und Gewährleistung zu adressieren. Bei Diensten auf

Grundlage eines Dauerschuldverhältnisses, auch jene ohne Entgelt, bspw. werbefinanziert, könnte man die Haftung und Gewährleistung während der Vertragslaufzeit als angemessen betrachten. Dies sollte auch entsprechend beim Erwerb von Softwarelizenzen gegen Bezahlung gelten. Bei der weiteren Ausgestaltung sind auch rechtsökonomische Ansätze zu diskutieren. So sähe der Ansatz des Cheapest Cost Avoider vorrangig diejenige Partei in der Verantwortung IT-Sicherheit zu gewährleisten, die einen potentiellen Schaden am günstigsten vermeiden kann.

Anders gelagert sind Fälle, in denen Source Code im Sinne der Offenheit auf Plattformen zur freien Verwendung steht. Hier sollte Haftung grundsätzlich ausgeschlossen werden können, abgesehen von Vorsatz und grober Fahrlässigkeit. In diesen Konstellationen fehlt es bereits an der Gegenleistung, welche dem Anbieter ermöglicht im Sinne des Äquivalenzinteresses, Risiken abzusichern. Daraus folgt, dass es hier lediglich sehr eingeschränkte Möglichkeiten gibt, für Risiken über das vom jeweiligen Entwickler intendierten Verwendungszweck und zugesicherten Sicherheitsniveau hinaus zu übernehmen.

Je nach Zuordnung in die oben aufgezeigten Kategorien sollten Anbieter von Diensten und Produkten Sicherheitslücken, die ihnen bekannt werden, schließen (soweit möglich) und Anwendern und Käufern entsprechende Patches oder Updates zur Verfügung stellen. Sie können sie zudem über die Bereitstellung entsprechender Updates informieren. Anwenderinnen und Nutzer tragen Verantwortung für die Aktualität und den sicheren Betrieb ihrer Endgeräte und ihrer Heimnetzwerke. Für zahlreiche Probleme und Phänomene existieren bereits Haftungsregeln, die ggfs. klarer zugeordnet werden müssten, um klarzustellen, in welchen Fällen welcher Akteur die Verantwortung trägt.

II. Anforderungen an Haftungsregeln für IT-Sicherheit

Um wirkungsvoll und markttauglich zu sein und um den formulierten Zielen gerecht zu werden, sieht eco - Verband der Internetwirtschaft folgende Anforderungen an Haftungsregeln als zentral an:

- **Internationalität**

  Um ein möglichst breites Regulierungsfeld zu schaffen, ist die internationale Anknüpfung einer Haftungsregulierung erforderlich. Rein nationale Regelungen erreichen im europäischen Binnenmarkt nicht alle Beteiligten. Es ist daher zwingend notwendig, dass Verantwortung für IT-Sicherheit einen europarechtlichen Rahmen bekommt. Daher ist der Anschluss an international anerkannte Standards erforderlich, da sie allen Marktteilnehmern nachvollziehbare und erfüllbare Anforderungen auferlegen und eine konsistente Regulierung auch über Staatsgrenzen hinweg ermöglichen.

- **Tatbestände mit Haftungsrelevanz**
  IT-Produkte, insbesondere Software und Hardware mit Betriebssoftware, sind komplex. Ihre komplett fehlerfreie Auslieferung ist gerade bei komplexen Anwendungen oft nicht möglich. Auch die Europäische Kommission erkennt dies in ihrer Cybersicherheitsstrategie an. Zudem haben Entwickler und Hersteller nach Auslieferung des Produkts meist nur eingeschränkte Kontrolle darüber. Updates können zwar angeboten und ggfs. registrierte Kunden darüber informiert werden. Aber gerade bei lokal installierten und betriebenen Systemen und Software außerhalb großer Rechenzentren oder einer Cloud wird es schwer werden, entsprechende Updates automatisch einzuspielen. Die Frage, ab wann eine Haftungs- bzw. Gewährleistungsregelung sinnvoll geltend gemacht werden kann oder wirksam im Sinne einer Verbesserung der IT-Sicherheit in Netzen und Systemen ist, ist dementsprechend komplex. Das bloße Vorhandensein eines Fehlers in einer Software oder einem Dienst kann somit bisher nur in den Fällen als Anknüpfungspunkt für eine Haftungs- bzw. Gewährleistungsregelung dienen, in denen der Softwarefehler auch einen Mangel im Rahmen des Gewährleistungsregimes des BGB fällt. Anknüpfungspunkte für Haftungs- bzw. Gewährleistungsregeln sollten daher mit Bedacht gewählt werden.

  Ein möglicher Ansatzpunkt könnte die Nichteinhaltung von (teilweise noch zu definierenden) Mindestsicherheitsanforderungen für Produkte oder Komponenten sein. Diese Anforderungen müssten der Komplexität offener, interoperabler Systeme und Netzwerke Rechnung tragen. Sie sollten sich daher primär am Verhalten von Herstellern und Entwicklern orientieren und so eine umfassende, marktgreifende Regulierung ermöglichen und gleichzeitig den besonderen Umständen moderner Informationstechnologie Rechnung tragen.

  Um gerade dem Problem der nicht vollständigen Sicherheit in komplexen IT-Systemen adäquat zu begegnen, stellt sich zudem die Frage, inwieweit durch bestehende Softwarefehler oder Sicherheitslücken ein Mangel definiert werden kann. Ausgangspunkt ist hier der Umstand, dass im Zuge der Entwicklung von IT-Produkten, der Bereitstellung neuer Schnittstellen oder Funktionen, aber auch durch die einfache Auslieferung einer Software oder eines Bauteils Sicherheitslücken entstehen können oder diese erst zu einem späteren Zeitpunkt bekannt werden. Der zurzeit geltende Mangelbegriff des BGB erstreckt sich nicht auf in der Zukunft auftretende bzw. entdeckte IT-Sicherheitsschwachstellen. Bestimmte Angriffsvektoren (bspw. DDOS-Attacken), die keine unmittelbare Schädigung des Eigentümers verursachen, sind ebenfalls nicht abgedeckt. Das schiere Vorhandensein einer Sicherheitslücke kann daher schlecht als Anknüpfungspunkt für eine Haftungs- bzw. Gewährleistungsregelung gelten. Maßgeblicher wäre hier der Umgang mit der Sicherheitslücke.

Ein Ansatz wäre es den Fehlerbegriff zu erweitern, bspw. könnte man den nicht erfolgten Hinweis des Herstellers an den Verbraucher zum Einspielen von Softwareupdates als Fehler definieren.

Weiterhin könnte auch die Nichteinhaltung einer bestimmten Reaktionsfrist nach Bekanntwerden einer Sicherheitslücke oder das zu späte Schließen einer solchen unter einen erweiterten Mangelbegriff fallen. Dehnbare Begriffe wie „Stand der Technik“ einerseits und konkret im Gesetzestext verankerte technische Anforderungen andererseits sollten vermieden werden, da sie die bestehenden Haftungsregeln zu stark diversifizieren, u.U. nicht mit den Entwicklungen im Markt Schritt halten können und dadurch einen hohen administrativen Aufwand sowohl bei Aufsichtsbehörden als auch in Unternehmen verursachen.

Zuletzt stehen aber auch Anwender von Systemen ebenfalls in der Verantwortung. Sie sind gehalten, ihre Systeme aktuell zu halten und bereitgestellte kritische Sicherheitsupdates zeitnah zu installieren. Wenn dieser Obliegenheit nicht nachgekommen wird, sind Haftungsausschlüsse und -begrenzungen vorzusehen, in denen grob fahrlässiges oder vorsätzliches Anwender- oder Nutzerverhalten im Rahmen einer Haftungsregelung für Betreiber oder Anbieter berücksichtigt wird.

- **Adressaten für Gewährleistungs- bzw. Haftungsregeln**
  Die zentrale Frage des Adressaten von Haftungs- bzw. Gewährleistungsbestimmungen ist gerade in einem dynamischen Umfeld mit offenen, interoperablen Plattformen und Netzen oft nur sehr schwer zu beantworten. Die Haftung eines einzelnen Akteurs, wie sie sonst häufig vorkommt, wäre problematisch, da keiner der genannten Akteure die alleinige Möglichkeit hat, alle Aspekte in offenen vernetzten Plattformen zu kontrollieren. Zudem wäre es auch bei einzelnen Komponenten nicht immer möglich, den Verpflichteten eindeutig und zweifelsfrei zu bestimmen. Unklar wäre auch, wie in diesem Kontext mit Abandonware umzugehen ist.

  Inwieweit eine Haftungsadressierung oder eine Gewährleistungsgrundlage auf Basis der oben benannten Szenarien tatsächlich sinnvoll möglich ist, sollte auch die Möglichkeiten und Kapazitäten der einzelnen Akteure berücksichtigen, die im Folgenden näher beschrieben werden.

  Inverkehrbringer wie Elektrowarenhändler besitzen in der Regel nicht die ausreichende Kompetenz, um die Sicherheit eines Produkts angemessen zu beurteilen oder zu beeinflussen. Sie können aber darauf achten, Geräte, deren Sicherheit in Frage steht (beispielsweise, weil der Produktlebenszyklus abgelaufen ist), nicht in Verkehr zu bringen bzw. beim Verkauf eines solchen Gerätes darauf hinzuweisen. Schwieriger wird es, Inverkehrbringer zu verpflichten, zusätzlich auf bekannte Sicherheitslücken hinzuweisen. Die dynamischen Entwicklungen in

diesem Bereich dürften insbesondere beim Einzel- und Elektrohandel zu großen Problemen führen.

Entwickler von Software können ihre eigenen Produkte absichern und bis zu einem gewissen Grad die Integration in verschiedene digitale Ökosysteme unterstützen. Indem Sie ihre Software regelmäßig aktualisieren und identifizierte Sicherheitslücken zeitnah schließen, können sie so mehr Sicherheit für ihre Dienste und Produkte schaffen. Darüber hinaus sollten sie insbesondere bei der Entwicklung ihrer Anwendungen auch entsprechenden Sicherheitsaspekten Rechnung tragen.

Hersteller von Geräten müssen sicherstellen, dass diese technisch dafür ausgerüstet sind, regelmäßig Updates zu empfangen. Sie müssen auch sicherstellen, dass auf den Geräten fest installierte Software ggf. dazu imstande ist, Sicherheitsupdates zu empfangen. Je nach Nutzungskontext müssen Sie außerdem Anwendern eine Möglichkeit zur Verfügung stellen, in der diese den Updatestatus überprüfen können und u.U. eigene Updates einspielen oder Onlinefunktionen deaktivieren können. In diesen Fällen sollten ausdrückliche und verständliche Hinweise an den Nutzer erfolgen, welche auch die damit einhergehende Verantwortung und Haftung erläutern.

- **Abgrenzung von Produkten**
  Eine Herausforderung bei der Formulierung einer Haftungs- bzw. Gewährleistungsregelung im Bereich der IT-Sicherheit besteht darin, dass aufgrund der teilweise sehr kurzen Updatezyklen und des dynamischen Umfelds mit sich schnell entwickelnden Angriffsvektoren sowohl der Zeitpunkt des Inverkehrbringens als auch das Nachliefern von Updates sich nur bedingt sinnvoll durch Haftungsregelungen adressieren lassen. Darüber hinaus ist aufgrund der Offenheit der Technologieplattformen die Abgrenzung der verschiedenen Produkte und Dienste voneinander nur bedingt durchführbar. Dementsprechend problematisch ist eine pauschale Herangehensweise für sämtliche Soft- und Hardware und vernetzte Geräte, die versucht, gänzlich unterschiedliche Produkte und Dienstleistungen zu regulieren oder mit gänzlich neuen Haftungsregeln oder Konstrukten zu adressieren.

  Die bestehenden Regelungen im Produkthaftungs- bzw. Produktsicherheitsgesetz sowie dem BGB bieten Anknüpfungspunkte für Haftungsregime und werden durch die im EU-Cybersecurity Act vorgesehen Maßgaben zur Zertifizierung und Kennzeichnung von Produkten sowie durch das IT Sicherheitsgesetz 2.0. erweitert.

- **Produktlebenszyklen sinnvoll in Regelungen mit einbeziehen**
  Die Lebenszeit vernetzter Geräte lässt sich anders als bei vielen anderen Produktgruppen oft nicht pauschal beziffern. Während bestimmte Betriebssysteme und Computerprogramme u.U. nur wenige Jahre im Markt angeboten werden, können vernetzte Werkzeuge oder

Haushaltsgeräte unter Umständen mehrere Jahrzehnte in Betrieb sein. Eine einheitliche Haftungsdauer kann daher nicht sinnvoll adressiert werden. Sinnvoll wäre, die Gewährleistungsdauer an den entsprechenden Produktlebenszyklen und ggf. im Anschluss an diese für einen bestimmten Zeitraum zu orientieren, ähnlich den bestehenden gesetzlichen Regelungen für die Gewährleistung bei Verbrauchern. Für diesen Zeitraum wären Hersteller dazu verpflichtet, Sicherheitsupdates für die entsprechenden Produkte bereitzustellen.

- **Umfang von Haftungs- und Gewährleistungsregeln**
  Vor dem Hintergrund der zuvor geschilderten Umstände bleibt zuletzt auch die Frage nach einem Umfang der Haftungs- bzw. Gewährleistungsregeln. Wie bereits ausgeführt, muss der Umfang der Haftung im Verhältnis zum wirtschaftlichen Interesse des Adressaten stehen. Bei Fehlen des wirtschaftlichen Interesses, wie bei der Bereitstellung von Source Code im Sinne von Open Source, sollte eine Abbedingung der Haftung, abgesehen von grober Fahrlässigkeit und Vorsatz möglich sein.

  Außerdem ist auch dem Umstand Rechnung zu tragen, dass sich Schäden von IT-Sicherheitslücken nicht ohne weiteres beziffern lassen. Eine Sicherheitslücke kann existieren und geschlossen werden, ohne das tatsächlich an irgendeiner Stelle ein Schaden entsteht. Daneben besteht die Frage, inwieweit bspw. durch die vorübergehende Nichtverfügbarkeit oder eine eingeschränkte Verfügbarkeit eines Produktes, einer Komponente o.ä. ein Schaden abgeleitet werden kann. Zudem bestehen auch Probleme dabei, entsprechende Kausalitäten bei bspw. entwendeten Daten und deren Missbrauch herbeizuführen, die ohnedies bereits datenschutzrechtlich geregelt sind. Auch stellt sich die Frage eines Haftungsübergangs, wenn bspw. entsprechende Updates bereitstehen, vom Anwender aber nicht installiert werden und so u.U. der Betreiber eines Gerätes oder eines kleineren (Heim-)Netzwerks selbst zur Gefahr wird und bei Dritten Schäden verursachen kann. Daher sollte im Rahmen einer Haftungsregelung überdacht werden, bis zu welchem Umfang welche Partei für die Schäden bei Dritten aufkommen müssen und unter welchen Rahmenbedingungen ein Haftungsübergang auf Inverkehrbringer, Anwender oder Betreiber überhaupt darstellbar ist.

  Zusammenfassend lässt sich festhalten, dass im Produktsicherheitsgesetz, im Produkthaftungsgesetz und im BGB bereits zahlreiche Anknüpfungspunkte für Haftungsregeln im Bereich der IT-Sicherheit existieren, so dass weitere spezialgesetzliche Regelung für Informations- und Kommunikationstechnologie nicht zwingend erforderlich ist. Sollten weitere Konkretisierungen für Haftungsregeln im Bereich der

IT-Sicherheit erwogen werden, sollten diese schwerpunktmäßig den Bereich der Gewährleistung betreffen.

Über eco: Mit über 1.100 Mitgliedsunternehmen ist eco der größte Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, formt Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. Leitthemen sind Zuverlässigkeit und Stärkung der digitalen Infrastruktur, IT-Sicherheit und Vertrauen sowie Ethik und Selbstregulierung. Deshalb setzt sich eco für ein freies, technikneutrales und leistungsstarkes Internet ein.