VERBAND DER INTERNETWIRTSCHAFT E.V.

# Leitlinien zur Debatte um Haftungsfragen im Bereich der IT-Sicherheit

Berlin, 29.06.2018

Im September 2017 veröffentlichte die Europäische Kommission ihre Cyber-Sicherheitsstrategie. Sie legt darin nieder, dass sie sich ab Mitte 2018 mit Haftungsfragen im Bereich der IT-Sicherheit auseinandersetzen möchte. Die Debatte um die Entwicklung einer Haftungsregelung im Bereich der IT-Sicherheit war bereits im Frühjahr 2017 in Deutschland kurz im Rahmen des NIS-Richtlinien-Umsetzungsgesetzes aufgeflammt. Unterstrichen wurde damit auch die wachsende Rolle von Informationstechnologie in allen Bereichen von Gesellschaft, Staat und Wirtschaft und deren Integrität als zentralem Baustein für das Vertrauen in diese Institutionen.

Die beiden Debatten unterstreichen unabhängig voneinander, wie zentral Haftungsfragen im Bereich der IT-Sicherheit gestaltet werden. Vor dem Hintergrund der laufenden Debatte um den EU Cybersecurity Act (COM (2017) 477) stellt sich daher die Frage, wie eine solche Haftungsregelung in Verbindung mit IT-Sicherheit gestaltet werden könnte.

Um die Debatte weiter mit dem Ziel zu begleiten, eine sinnvolle, das IT-Sicherheitsniveau stärkende, Zuordnung von Verantwortlichkeit und handhabbare Haftungsregelungen für Anbieter, Nutzer und Regulierer zu finden, und zentrale und maßgebliche Aspekte aufzugreifen sieht eco - Verband der Internetwirtschaft folgende Leitlinien als maßgeblich für die Diskussion:

- **Komplexität von IT-Sicherheit muss Rechnung getragen werden**

IT-Sicherheit ist eine gemeinsame Herausforderung von Staat, Anbietern von Hardware, Software und Diensten sowie Nutzern bzw. Anwendern. Alle haben unterschiedliche Rollen und sind in diesen Bereichen auch dafür verantwortlich, dass in der vernetzten Welt Sicherheit geschaffen wird bzw. gewahrt bleibt. Eine einseitige Zuweisung der Verantwortung für Sicherheit oder deren Lücken kann daher nicht pauschal erfolgen. Die Rolle und der Beitrag der jeweils involvierten Gruppen müssen daher bei weiteren Überlegungen berücksichtigt werden, wenn es um die Frage geht, wer für welche Bereiche entsprechend seiner Rolle und Möglichkeiten Verantwortung übernehmen muss. Der Grundsatz, dass derjenige haftet, der die Risiken am besten beherrschen kann, bietet dabei eine gute Orientierung.

- **Schutzbedarfe müssen angemessen sein**

Eine Verbindung von IT-Sicherheitsauflagen mit Haftungsregeln muss in einem angemessenen Verhältnis zu den jeweils geschützten Gütern stehen. Auflagen für kritische Infrastrukturen und für Massenware für den breiten Markt können nicht dieselben sein. Ein differenzierter Ansatz bei der Bemessung des Schutzbedarfs ist daher zwingend erforderlich. Bereichsspezifische Regeln sind in diesem Fall ebenso mit einzubeziehen, zu prüfen und ggfs. digitalen Anforderungen anzupassen.

Die Anknüpfung an die Grundlage eines Security by Design Ansatzes kann zusätzlich die verantwortliche Rolle, die Anbieter im IT-Sicherheitsgefüge wahrnehmen, unterstreichen.

- **Haftungslücken und Haftungsbedarfe müssen klar adressiert werden**

Eine der zentralen Fragen in der Diskussion um die Verknüpfung von IT-Sicherheit und Haftungsregeln dreht sich darum, wo exakt Haftungslücken und -bedarfe zu verorten sind und wem eine entsprechende Verantwortung bei der Mängelbeseitigung bzw. die Gewährleistung zuzuschreiben ist. Ziel einer Zuordnung von Verantwortlichkeit oder Haftungsregelung sollte daher sein, zu klären, wie Haftung in Bezug auf IT-Sicherheit und die daraus resultierenden Ansprüchen adressiert werden kann. Im Zuge dessen müssen Adressaten von Haftungsregeln klar definiert werden. Der Komplexität vernetzter Systeme sollte dabei Rechnung getragen werden. Unpräzise Regeln in diesem Bereich können Auseinandersetzung über Verantwortung und Rechtsunsicherheit für Unternehmen und Verbraucher nach sich ziehen.

Des Weiteren ist zu erwägen, ob eine stärkere Einbeziehung zertifizierter Normen und Standards in die Zurechunung und Bewertung von Verantwortlichkeiten sinnvoll ist.

- **Haftungsregeln sollten sinnvoll und handhabbar gestaltet sein - für Wirtschaft und Aufsicht**

Zentrale Überlegungen bei der Verknüpfung von Haftung und Sicherheit gehen in die Richtung, Herstellern bestimmter Produktgruppen konkrete Verantwortlichkeiten im Kontext der Gewährleistung von IT-Sicherheit zu machen. Dabei muss sichergestellt sein, dass v.a. die Zertifizierung von Sicherheitsanforderungen so ausgestaltet sein muss, dass sie mit der technischen Entwicklung Schritt halten kann. Granulare technische Festlegungen in Anforderungen an Produkte oder Dienste sollten daher vermieden werden und so gestaltet sein, dass sie bereichsspezifische Regeln sinnvoll ergänzen können. Kleinteilige, produktspezifische Regelungen sollten in diesem Sinne vermieden werden, da die Implementierung solcher Regeln praktisch nicht leistbar ist und die Gefahr besteht, dass solche Regeln ins Leere laufen.

- **Eine Verknüpfung von Zertifikat oder Gütesiegel mit einer Haftungsregelung muss für die Wirtschaft einen Mehrwert haben**

Eine Berücksichtigung von Zertifikats- oder eine Gütesiegelregelungen, wie sie im Rahmen des Cybersecurity Act entstehen, sollte im Rahmen des Haftungsregimes auch unabhängig von der Frage, welche Form der Haftung verfolgt wird, einen Mehrwert für Unternehmen bieten. Zu diskutieren wäre hier eine Beweislastumkehr oder Haftungserleichterungen. Sollte dies ausbleiben, hätten solche meist freiwilligen Zertifikate keine positive Marktlenkungsfunktion und böten Unternehmen bestenfalls Orientierung. Nutzern und Anwendern wiederum können Zertifikate und Gütesiegel ebenfalls Orientierung und Hilfestellung bieten. Dabei sollte aber nicht der Eindruck entstehen, dass sie von eigener Sorgfalt und Verantwortung vollständig entbunden wären.

- **Verantwortung und Nachweispflichten müssen sachgerecht geregelt sein**

Die Verknüpfung von Haftungsregeln ist immer eng verbunden mit der Frage, wie Beweislast und Nachweispflichten geregelt sind. In jüngster Vergangenheit, wurde hier häufig auf das Prinzip der Beweislastumkehr gesetzt. Hersteller oder Inverkehrbringer würden damit dazu verpflichtet, den Nachweis darüber zu erbringen, dass ihre Produkte fehlerfrei sind. Solche Haftungsregeln sind für vernetzte Produkte sowie Dienste, die von Nutzern individuell konfiguriert und kombiniert werden können, nicht handhabbar. Auch die Europäische Kommission erkennt an, dass Software und IT komplex sind und es in einem sich dynamisch entwickelnden Umfeld objektiv nicht möglich ist, sie komplett ohne Sicherheitslücken auszuliefern. Diese Möglichkeiten für eine dynamische Entwicklung sollten weiterhin erhalten bleiben. Entsprechend gilt es bei der Nachweispflicht in Bezug auf die Beweislastumkehr eine umsetzbare Lösung zu erreichen, die den Ansprüchen an qualitativ hochwertige Produkte einerseits und den Anforderungen an verantwortungsbewusste Nutzer und Anwender andererseits gerecht wird.

- **Unternehmen dürfen nicht für staatliches Fehlverhalten verantwortlich gemacht werden**

Es gibt eine aktive Debatte darüber, dass Regierungsbehörden Informationen zu Schwachstellen in IT-Systemen horten, um so für geheimdienstliche Zwecke und für die Strafverfolgung Zugriff auf Endgeräte und Daten haben zu können. Eine Zuordnung von Verantwortlichkeiten und die Auflösung von Haftungsfragen vor diesem Hintergrund einseitig bei Herstellern und Produzenten zu verorten, ist nicht zielführend. Er untergräbt das Vertrauen in die allgemeine Sicherheit von IT-Systemen und schiebt die Verantwortung für den Vertrauensverlust Unternehmen zu. Dies ist abzulehnen.

**Leitlinien für eine Haftungsregelung im Bereich der IT-Sicherheit**

Folgende Aspekte sind bei der Entwicklung einer Haftungsregelung in Verbindung mit IT-Sicherheit zwingend zu berücksichtigen:

- Es bedarf vorab einer Klärung, wo exakt Haftungsbedarfe und -lücken zu verorten sind und wie diese sinnvoll durch die Zuordnung von Verantwortlichkeit oder neue Haftungsregime adressiert werden können.
- Eine Haftungsregelung in Verbindung mit einem Gütesiegel muss mit Erleichterungen bei der Haftung zwingend verbunden sein. Ansonsten fällt der objektive Mehrwert eines Gütesiegels weg.
- Bei Regelungen zur Beweislastumkehr ist darauf zu achten, dass diese auch für Hersteller und Anbieter erfüllbar ist. Entscheidend ist hier neben dem Adressaten die Frage, unter welchen Voraussetzungen sie entfällt.
- Allgemeine Auflagen und Regelungen für Haftung sollten erfüllbar, nachvollziehbar und verhältnismäßig sein - produktspezifische technische Anforderungen sind nicht hilfreich.
- Bereichsspezifischen Regeln muss Rechnung getragen werden. Es darf keinen Widerspruch zwischen bereichsspezifischen Haftungsregeln und allgemeinen Haftungsregeln für IT-Sicherheit geben. Das Zusammenwirken der verschiedenen Regime darf nicht dazu führen, dass die Verantwortung einseitig bei der IT-Branche verortet wird.
- IT-Sicherheit stellt eine komplexe Herausforderung dar. Um sie herzustellen, müssen alle Beteiligten Verantwortung übernehmen. Gleichzeitig bleiben aber immer Restrisiken bestehen. Haftungsregelungen sollten solche systemischen Risiken nicht adressieren, da dies mittel- bis langfristig im Rahmen der Digitalisierung zu einer pauschalen Benachteiligung von IT führen wird. Insbesondere bei der Herleitung von Kausalitäten und Folgeschäden sollte daher behutsam vorgegangen werden.

---

**Über eco:** Mit über 1.000 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.