Redaktion MMR-Aktuell Kurzbeiträge/Kommentare MMR-Aktuell 2012, 331642

Neuer US-Gesetzentwurf CISPA: „Kampf gegen Cyberbedrohung" - die nächste Runde

Dr. Axel Spies ist Rechtsanwalt in der Kanzlei Bingham McCutchen, Washington DC und Mitherausgeber der MMR. Mira Vinke studiert Jura an der American University.

Sowohl bei US-Unternehmen als auch bei Internetnutzern sorgten die Gesetzesentwürfe SOPA (Stop Online Piracy Act) und PIPA (Project IP Act) im Januar 2012 für viel Unruhe. Die Internetseite Wikipedia blieb damals für 24 Stunden dunkel, Google protestierte mit schwarzen Balken und auch Facebook, Twitter und eBay schlossen sich den Protesten an, da sie eine mögliche Zensur des Internet befürchteten.

Der Protest zeigte offenbar Wirkung: Nach Medienberichten stoppte der *US-Kongress* SOPA und PIPA Ende Januar 2012, da es ihnen an der erforderlichen Mehrheit fehlte. Damit wurde die Diskussion um ein bevorstehendes Anti-Piraterie-Gesetz zunächst auf Eis gelegt. Nun hat ein neuer Gesetzesentwurf die Diskussion erneut entfacht: Der Gesetzesentwurf HR 3523 mit dem Namen CISPA (Cyber Intelligence Sharing and Protection Act) wurde vom republikanischen Kongressabgeordneten *Rogers* und dem Demokraten *Ruppersberger* im *US-Repräsentantenhaus* eingebracht und soll den Austausch von Geheimdienstinformationen zwischen US-Behörden und US-Unternehmen fördern. Ziel ist, dass die Industrie und die *Regierung* Hand in Hand Cypercrime bekämpfen. Am 26.4.2012 billigte das *US-Repräsentantenhaus* den Gesetzesentwurf. Nun muss der *US-Senat* über CISPA entscheiden.

Kritiker des CISPA sehen in diesem neuen Gesetzesentwurf eine Neuauflage der SOPA. Mit SOPA wäre es sowohl dem *US-Justizministerium* als auch Urheberrechtsinhabern möglich gewesen, gerichtliche Verfügungen gegen Internetanbieter zu beantragen, die gegen Urheberrecht verstoßen haben. Im Vergleich zur SOPA hat CISPA einen anderen Anwendungsbereich und verfolgt darüber hinaus einen anderen Zweck, nämlich der Vereinfachung des Informationstauschs zwischen Firmen und US-Behörden zur Bekämpfung von Cybercrime. Anders als bei SOPA, kann mithilfe von CISPA keine Verfügung eingeholt werden, um das Anzeigen einer Webseite zu blockieren. Eine Zensur des Internet, wie von einigen Kritikern befürchtet wird, ist mit CISPA somit gar nicht möglich. Außerdem kann CISPA nach der neuen Fassung des Entwurfs infolge von Urheberrechtsverletzungen nicht angewendet werden. Deshalb ist zwischen SOPA und CISPA klar zu differenzieren.

I. Inhalt des CISPA

1. Zweck des CISPA

CISPA soll einen umfangreichen Datenaustausch zwischen den Unternehmen und den US-Behörden ermöglichen. So heißt es in der Präambel des Gesetzesentwurfes:

„To provide for the sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cybersecurity entities, and for other purposes."

Bereits der erste Satz lässt erkennen, was der Rest des Entwurfs bestätigt: Der neue Gesetzesentwurf ist sehr vage gehalten und beinhaltet keine konkreten Definitionen. So wird auch im weiteren Verlauf des Gesetzesentwurfs nicht deutlich, welchen anderen Zwecken CISPA dienen soll.

2. Betroffene

Durch Sec. 1104 (a) (1) H.R. 3523 des CISPA wird die Übergabe vertraulicher Kundendaten im Falle einer Cyberbedrohung zwischen Internetfirmen und US-Geheimdienstbehörden ermöglicht:

"(1) The Director of National Intelligence shall establish procedures to allow elements of the intelligence community to share cyber threat intelligence with private-sector entities and utilities to encourage the sharing of such intelligence."

Geheimdienstbehörden dürfen nach Sec. 1104 (a) (2) (A) H.R. 3523 nur folgenden Unternehmen Informationen mitteilen:

"(i) certified entities; or

(ii) a person with an appropriate security clearance to receive such cyber threat intelligence."

Welche Informationen im konkreten Fall ausgetauscht werden und welche staatlichen Stellen auf diese zugreifen können, ist dem Entwurf nicht zu entnehmen. Gem. Sec. 1104 (h) (2) H.R. 3523 ist eine „certified entity" definiert als:

„protected entity, self-protected entity, or cybersecurity provider that

(A) possesses or is eligible to obtain a security clearance, as determined by the Director of National Intelligence; and

(B) is able to demonstrate to the Director of National Intelligence that such provider or such entity can appropriately classified cyber threat intelligence."

3. Definition des Begriffs „Cyberbedrohung" (cyber threat)

In der ursprünglichen Version der CISPA stellt eine Information dann eine Cyberbedrohung dar, wenn sie direkt ein System oder Netz der Regierung oder eines privaten Unternehmens verletzt oder bedroht, sofern diese Informationen die Sicherheit dieses Systems oder Netzwerks betreffen. Im einzelnen gem.Sec. 1104 (h) (2) H.R. 3523:

„(A) efforts to degrade, disrupt, or destroy such system or network; or

(B) theft or misappropriation of private or government information, intellectual property, or personally identifiable information."

Doch die Formulierung „geistiges Eigentum" sorgte für einen großen Widerstand bei den Internetnutzern. Infolgedessen wurde der Gesetzesentwurf mehrmals geändert. Nach der aktuellen Fassung wird die „cyber threat information" gem. Sec. 1104 (h)(4) wie folgt definiert:

„(i) a vulnerability of a system or network of a government or private entity;

(ii) a threat to the integrity, confidentiality, or availability of a system or network of a government or private entity or any information stored on, processed on, or transiting such a system or network;

(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network of a government or private entity, or

(iv) efforts to gain unauthorized access to a system or network of a government or private entity, including to gain such unauthorized access for the purpose of exfiltrating information stored on , processed on, or transiting a system or network of a government or private entity."

Auf Grund einer erneuten Änderung ist die Anwendung von CISPA nun auch gem. Sec. 1104 (c) (D) H.R. 3523 bei Ermittlungen in Fällen von Kinderpornografie, Kidnapping und Menschenhandel erlaubt:

„(D) for the protection of minors from child pornography, any risk of sexual exploitation, and serious threats to the physical safety of such minor, including kidnapping and trafficking [...]"

Einschränkungen erfährt CISPA dadurch, dass keine Daten ausgetauscht werden dürfen, die die Steuererklärung, Ausbildung, Kauf von Büchern oder Waffen (!) oder Krankenakten betreffen.

„Protection of sensitive personal documents:

The Federal Government may not use the following information, containing information that identifies a person, shared with the Federal Government in accordance with subsection (b):

(A) Library circulation records.

(B) Library patron lists.

(C) Book sales records.

(D) Book costumer lists.

(E) Firearms sales records.

(F) Tax return records.

(G) Educational records.

(H) Medical records."

Ansonsten ist ein Austausch von Informationen mit US-Regierungsstellen nach CISPA legitimiert, solange die Weitergabe von Daten der Cybersicherheit dient.

4. Freiwillige Basis

Es besteht keinerlei Verpflichtung der Unternehmen, Kundendaten, die in Verbindung mit einer möglichen Cyberbedrohung stehen, an den US-Geheimdienst herauszugeben. Vielmehr soll dieser Austausch auf freiwilliger Basis geschehen. So heißt es in Sec. 1104 (c) H.R. 3523:

„(3) Anti-tasking restriction:

Nothing in this section shall be construed to permit the Federal Government to

(A) require a private-sector entity to share information with the Federal Government; or

(B) condition the sharing of cyber threat intelligence with a private-sector entity on the provision of cyber threat information to the Federal Government."

Praktisch gesehen haben die US-Unternehmen ein großes Interesse an dem Datenaustausch, da CISPA nicht nur angewendet wird, wenn eine Cyberbedrohung gegen die Regierung besteht, sondern auch wenn US-Firmen solchen Bedrohungen ausgesetzt sind. Daher sieht CISPA nicht nur vor, dass Firmen der Regierung Daten aushändigen, sondern auch umgekehrt. Da keine konkreten Einschränkungen für diesen Austausch in CISPA vorgesehen sind, können US-Unternehmen auf zahlreiche neue Informationen über potenzielle Bedrohungen ihrer Sicherheit hoffen.

5. Haftungsklausel für private Unternehmen

Neben der Änderung der Definition der „Cyberbedrohung" fügte das *US-Intelligence Committee* auch eine spezielle Klausel dem Entwurf hinzu, die die Haftung der privaten Unternehmen betrifft. Nach Sec. 1104 (b) (4) (A) H.R. 3523 gilt eine Haftungsbeschränkung für private Unternehmen, die „cyber threat information" entsprechend der Vorgaben des Entwurfs US-Behörden zur Verfügung gestellt haben, sofern sie im „guten Glauben" gehandelt haben:

„Exemption from liability:

No civil or criminal cause of action shall lie or be maintained in Federal or State court against a protected

entity, self-protected entity, cybersecurity provider, or an officer, employee, or agent of a protected entity, self-protected entity, or cybersecurity provider, acting in good faith."

6. Konkurrenz zu anderen Bundesgesetzen

Der Gesetzesentwurf enthält (bereits in seiner ursprünglichen Fassung) eine Klausel, die das Verhältnis von CISPA zu anderen Bundesgesetzen, die ebenfalls die Weitergabe von Informationen betreffen, regelt. Nach Sec. 1104 (b) (5) H.R. 3523 soll der Abschnitt, der die Weitergabe von Informationen betrifft, ungeachtet aller anderen Bundesgesetze gelten, die sich auf die Bereitstellung von Informationen von Personen oder Behörden an die *Regierung* beziehen:

"(5) Relationship to other laws requiring the disclosure of information:

The submission of information under this subsection to the Federal Government shall not satisfy or affect (A) any requirement under any other provision of law for a person or entity to provide information to the Federal Government [...]"

Vor solchen Formulierungen hatte jedoch der unabhängige Forschungsdienst *CRS* (*Congressional Research Service*) des *US-Kongresses* gewarnt:

„This broad phrase, however, does not specify which provisions it is meant to refer to, and may therefore have unforeseen consequences for both existing and future laws."

7. Transparenz

Gem. Sec. 1104 (e) H.R. 3523 soll ein vom Vertreter des US-Geheimdienstes verfasster Bericht an den Geheimdienst-Ausschuss des *US-Kongress* über CISPA Auskunft geben. Dieser soll zwar öffentlich zugänglich sein, er kann jedoch auch einen geheimen Anhang enthalten.

II. Kritik an CISPA

Während einige große Unternehmen CISPA unterstützen, kommt der Protest lediglich aus den Reihen der Internetnutzer. Bereits 600.000 Menschen haben die Onlinepetitionen der Organisationen Demand Progress und Avaaz.org unterstützt. Die Kritiker befürchten u.a., dass auf Grund der Datenübertragung an Regierungsstellen Onlinedurchsuchungen ohne richterliche Anordnung möglich werden. Einer der wesentlichen Kritiker der CISPA ist die *Electronic Frontier Foundation (EFF).* Sie kritisiert vor allem die unklaren und zu weit gefassten Begriffserklärung im neuen Gesetzesentwurf:

"The idea is to facilitate detection of and defense against a serious cyber threat, but the definitions in the bill go well beyond that. The language is so broad it could be used as a blunt instrument to attack websites like The Pirate Bay or WikiLeaks. Join EFF in calling on Congress to stop the Rogers' cybersecurity bill. [...] But because 'us[ing] cybersecurity systems' is incredibly vague, it could be interpreted to mean monitoring email, filtering content, or even blocking access to sites."

Die *EPIC (Electronic Privacy Information Center)* kritisiert, dass CISPA die Tür zu verstärkter Überwachung durch den Staat öffnen würde. Zudem sieht sie die Gefahr, dass die Transparenz und Rechenschaftspflicht der *Regierung* reduziert würden:

„The bill preempts established privacy protections in other federal laws and opens the door for increased surveillance of individuals in the United States. The bill also creates a new Freedom of Information Act exemption, which will reduce government transparency and accountability"

Andere Gegner der CISPA weisen darauf hin, dass es keine Einschränkungen der Informationen gibt, auf die die *Regierung* zugreifen kann. Auf Grund dessen befürchten sie, dass der *Regierung* eine sehr viel größere Rechtsbefugnis bei dem Zugriff auf personenbezogene Daten durch CISPA verliehen wird. Diese Bedenken hat auch die *ACLU (American Civil Liberties Union)*:

„We just want people to know that Congress is on the verge of giving the government incredible new authorities to collect sensitive and personal Internet information and emails."

Auch der republikanische Abgeordnete und Präsidentschaftskandidat *Ron Paul* äußerte sich in einem neuen Beitrag auf seiner Webseite kritisch zum CISPA-Entwurf und beschrieb CISPA als Neuauflage der SOPA:

„But we should never underestimate the federal government's insatiable desire to control the internet. [...] CISPA represents an alarming form of corporatism, as it further intertwines government with companies like Google and Facebook. [...] Simply put, CISPA encourages some of our most successful internet companies to act as government spies, sowing distrust of social media and chilling communication in one segment of the world economy where America still leads."

Doch gerade den Vergleich von CISPA mit SOPA weist der Initiator des Gesetzesentwurfes *Ropers* mit Entschiedenheit zurück (s. Congressional Quarterly 04 2012, Ausgabe 10). Deren Ähnlichkeit ist laut ihm mit „Äpfel und Birnen" zu vergleichen:

„They are so completely different that there is absolutely no comparison. One of the reason we're getting out

talking to people is for that very reason. This bill has nothing to do with that."

Ropers Aussage bekräftigt *Ruppersberger*. CISPA würde weder zu einer Zensur noch zu einer erweiterten Autorität der *Regierung* führen:

„There's no censorship of websites or shutting down any websites in this bill. The government doesn't have any authority to do that under the legislation."

III. Ausblick

Am 26.4.2012 stimmte das *US-Repräsentantenhaus* mit 248 gegen 168 Stimmen dem Gesetzesentwurf zur CISPA zu. Doch in trockenen Tüchern ist CISPA mit der Abstimmung noch lange nicht. Zur Umsetzung fehlt ihr noch die Zustimmung des *US-Senats* und die des *Präsidenten*, der ein Vetorecht gegen Beschlüsse des *US-Kongresses* besitzt. Ob der *US-Senat* zustimmt, ist zweifelhaft. Am vergangenen Mittwoch drohte Präsident *Barack Obama* bereits, von diesem Vetorecht Gebrauch zu machen. In einer E-Mail gab das *Weiße Haus* bekannt, dass ihrer Ansicht nach CISPA die Privatsphäre unangemessen beeinträchtige, indem es einen weitreichenden Informationsaustausch zulassen würde, ohne einen ausreichenden Schutz personenbezogener Daten zu enthalten:

„Accordingly, the Administration strongly opposes H.R. 3523, the Cyber Intelligence Sharing and Protection Act, in its current form. [...] for the reasons stated herein, if H.R. 3523 were presented to the President, his senior advisors would recommend that he veto the bill."

Weiterführende Links

Vgl. auch *Bartels*, MMR-Aktuell 2012, 328597; *EuGH* MMR-Aktuell 2012, 328643 und MMR-Aktuell 2012, 327826.