Spies: USA: Totgesagte leben länger – Cyber Intelligence Sharing and Protection Act (CISPA) ZD-Aktuell 2013, 03457

USA: Totgesagte leben länger – Cyber Intelligence Sharing and Protection Act (CISPA)

Dr. Axel Spies ist Rechtsanwalt in der Kanzlei Bingham McCutchen LLP in Washington DC und Mitherausgeber der ZD.

Der umstrittene Cyber Intelligence Sharing and Protection Act (CISPA) ist wieder in der Diskussion. In seiner Form gleicht er dem CISPA-Entwurf aus der letzten Legislaturperiode vom April 2012. Eines der Schlüsselprinzipien von CISPA ist es, den US-Unternehmen Immunität gegen Strafverfolgung und Schutz vor einer möglichen Haftung zu gewähren, wenn sie Informationen an Regierungsbehörden in Bezug auf „Bedrohungen" im Cyberbereich weiterleiten. Besonders in der Schusslinie dieser Maßnahmen ist China, von dem in letzter Zeit angeblich einige Angriffe auf die Cyber-Security ausgegangen sind, wie die US-Presse berichtet. Andere befürchten Cyber-Security-Angriffe aus dem Iran und aus Nordkorea.

Unklar ist weiterhin in diesem von den Kongressabgeordneten *Rogers* (Republican/Michigan), Vorsitzender des House Permanent Select Committee on Intelligence, und *Rupperberger* (Democrat/Maryland) über die Parteigrenzen hinweg gesponserten Entwurf von CISPA, zu welchen Zwecken die Behörden die von den Unternehmen übermittelten Informationen verwenden dürfen. Das nach EU-Verständnis bestehende Prinzip der Zweckbindung der Datenerhebung gibt es in dieser Form in den USA nicht. Zahlreiche Privacy-Gruppen in den USA befürchten deshalb, dass die nationalen Sicherheitsbehörden auf diese Weise an alle Arten von vertraulichen Informationen, wie Nutzungsdaten und E-Mail-Inhalte, kommen könnten, die ihnen ansonsten nicht zur Verfügung stünden. Die Autoren von CISPA betonen, dass diese Daten nach dem Gesetzentwurf nur auf freiwilliger Basis erhoben würden, und „ermutigen" die Unternehmen, nur anonymisierte Daten zur Verfügung zu stellen. Allerdings dürfte der faktische Druck auf die Unternehmen zur Bereitstellung der personenbezogenen Daten, sofern sie in den Unternehmen gespeichert sind, groß sein. Es gibt auch Bedenken gegen die in dem Gesetzentwurf vorgesehenen Immunitätsvorschriften gegen die Unternehmen: Einigen gehen sie nicht weit genug (nur „good faith immunity"), andere meinen, sie sind zu weit gefasst.

Der CISPA-Gesetzentwurf von 2012 wurde nach Medienberichten von vielen als so belastend im Hinblick auf den Schutz der Privatsphäre angesehen, dass ein Veto des *Präsidenten* drohte. Das *Repräsentantenhaus* hatte den Entwurf im April 2012 mehrheitlich verabschiedet. Der *Senat* hat dem Entwurf allerdings nie zugestimmt, sondern arbeitete an einem eigenen Entwurf. Der „Cyber-Security-Zirkus", so die Presse, war am Ende der Legislaturperiode im Dezember 2012 in vollem Gange.

In der Rede zur Nation des *Präsidenten* v. 12.2.2013 heißt es zur Cyber-Security: „We know hackers steal people's identities and infiltrate private e-mail. We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."

Um diese Initiative zu untermauern, hat der *Präsident* ebenfalls am 12.2.2013 eine Executive Order zur Cyber-Security wenige Stunden vor seiner Rede veröffentlicht. Diese Executive Order weist als Verwaltungsanweisung zahlreiche Behörden an, in einer kurzen Frist Maßnahmen zur Verbesserung der Cyber-Security zu ergreifen: Kernstück der Initiative ist ein neuer Rahmen für die Bekämpfung der Cyber-Risiken: In der Executive Order heißt es dazu in Sec. 7 (a): „Der *Secretary of Commerce* leitet den *Direktor des National Institute of Standards and Technology* an, um einen Rahmen zur Bekämpfung von Cyber-Risiken für kritische Infrastrukturen zu entwickeln („Cyber-Security Framework"). Das Cyber-Security Framework umfasst eine Reihe von Standards, Methoden, Verfahren und Prozessen, die sich an Politik, Wirtschaft und technologische Stellen wenden, um Cyber-Risiken zu begegnen. Das Cyber-Security Framework beruht auf der Grundlage eines freiwilligen Konsens, Standards und Best Practices der Branche, um diese so weit wie möglich zu integrieren."

Die Executive Order des *Präsidenten* sieht auch eine Ausweitung des Defense Industrial Base (DIB) Information-sharing Program auf andere US-Behörden vor. Die DIB wurde 2011 eingerichtet und erlaubt dem *US-Department of Defense* und dem *US-Department of Homeland Security* den Austausch von nicht geheimen Informationen bei Bedrohungen der Cyber-Security, die z. B. von Zulieferern (Contractors) stammen (DIB partner companies).

Im Unterschied zu CISPA sieht die Executive Order allerdings nicht vor, dass die Unternehmen von sich aus Daten bei Bedrohungen der Cyber-Security an die Regierungsstellen übermitteln und ihnen im Gegenzug Immunität gewährt wird. Dies wird von Vertretern der Privacy-Gruppen begrüßt.

Weiterführende Links

Vgl. zu den Maßnahmen der EU zur Cyber-Security MMR-Aktuell 2013, 342694 und *Nüßing*, MMR-Aktuell 2013, 342689.