Kalifornien: Neues IoT-Gesetz unterzeichnet

Dr. Axel Spies ist Rechtsanwalt in der Kanzlei Morgan Lewis & Bockius, Washington DC, und Mitherausgeber der ZD.

Ab dem 1.1.2020 müssen die Hersteller von internetfähigen (IoT-)Geräten, die in Kalifornien verkauft oder zum Verkauf angeboten werden (connected devices), die neuen gesetzlichen Vorschriften in Kalifornien für Cyber-Sicherheitsmaßnahmen einhalten. Dazu gehört die Anforderung, ihre Geräte mit angemessenen Sicherheitsmerkmalen auszustatten, um das Gerät selbst und die darin enthaltenen Informationen zu schützen.

Gouverneur *Jerry Brown* hat am 28.9.2018 die Gesetzesmaßnahme Senate Bill 327 unterzeichnet. Damit wurde Kalifornien der erste US-Bundestaat mit einem Gesetz über Cyber-Sicherheitsmaßnahmen, das von allen Herstellern von Smart-Geräten mit Internetverbindung (IoT) beachtet werden muss. Das Gesetz ergänzt den California Civil Code (Sections 1798.91.04-06) zum 1.1.2020. Es gilt für jeden „Hersteller eines verbundenen Geräts" (connected device). „Hersteller" ist definiert als derjenige, der vom Gesetz umfasste Geräte herstellt oder in Kalifornien verkauft oder zum Kauf anbietet. Ein „verbundenes Gerät" ist ein Gerät oder ein anderes physisches Objekt, das entweder direkt mit dem Internet verbunden ist oder indirekt über eine IP- oder Bluetooth-Adresse mit dem Internet verbunden werden kann. Diese Definition ist weit genug, um die meisten Geräte zu umfassen, die allgemein als Teil des IoT eingestuft werden.

Diese Gerätehersteller müssen „das Gerät mit angemessenen Sicherheitsmerkmalen ausrüsten," die „der Art und Funktion des Geräts [und] den Informationen angemessen sein müssen, die das Gerät sammelt, enthält oder überträgt." Ferner müssen die Hersteller per Design angemessene Sicherheitsmerkmale „zum Schutz des Geräts und der darin enthaltenen Informationen vor unbefugtem Zugriff, Zerstörung, Verwendung, Änderung oder Offenlegung" vorsehen. Zur Präzisierung gibt es für die Angemessenheit der Sicherheitsanforderungen einige „sichere Häfen" (Safe Harbor Provision) im Gesetz. So werden die folgenden Maßnahmen als angemessene Sicherheitsmerkmale für verbundene Geräte angesehen.

Das Gerät erhält:

- ein vorprogrammiertes, individuelles Passwort für jedes Gerät oder
- eine Sicherheitsfunktion, bei der ein Benutzer eine neue Authentifizierungsmethode generieren muss, bevor auf das Gerät zugegriffen werden kann.

Für ausländische Marktteilnehmer ist wichtig: Der Begriff „Hersteller" umfasst nicht diejenigen, die einfach ein verbundenes Gerät kaufen oder ein verbundenes Gerät schlicht weiterverkaufen. Das Gesetz schreibt dem Hersteller eines verbundenen Geräts auch keine Verpflichtung in Bezug auf Drittanbieter-Software oder Anwendungen vor, die ein Nutzer einem verbundenen Gerät mit oder ohne Zustimmung des Herstellers hinzufügt. Das IoT-Gesetz gilt auch nicht für Unternehmen, soweit sie dem Bundesgesetz über den Datenschutz bei Krankendaten von 1996 (HIPAA) oder dem kalifornischen Gesetz über die Vertraulichkeit medizinischer Informationen unterliegen.

Das IoT-Gesetz schafft auch kein privates Klagerecht. Stattdessen hat die *kalifornische Staatsanwaltschaft* mit ihren untergeordneten Stellen die „ausschließliche Befugnis", das Gesetz durchzusetzen. Die Hersteller von verbundenen Geräten müssen bis zum 1.1.2020 angemessene

Sicherheitsmerkmale in ihre Geräte einbauen, sodass das Gerät und alle auf dem Gerät gespeicherten Informationen vor unbefugtem Zugriff, Zerstörung, Nutzung, Manipulation oder Offenlegung geschützt sind. Bezeichnenderweise ist der Begriff „Information" nicht durch das IoT-Gesetz definiert. Es verwendet stattdessen allgemeine Begriffe wie „jedwede Informationen" und „die Informationen, die es sammeln, enthalten oder übertragen kann." Dementsprechend wird das Gesetz von den damit befassten Behörden und Gerichten eher weit ausgelegt werden müssen – über personenbezogene Daten hinaus.

Wenn das Gerät unter das IoT-Gesetz fällt, sollten die Hersteller von solchen Geräten, die in Kalifornien verkauft oder zum Verkauf angeboten werden, dem Gesetz schon in der Design-Phase voll Rechnung tragen. Das könnte z. B. dadurch geschehen, dass der Hersteller jedes der verbundenen Geräte mit einem eindeutigen vorprogrammierten Passwort ausstattet. Die erfassten Hersteller von IoT-Geräten können möglicherweise die Haftungsauswirkungen nach dem neuen Gesetz begrenzen, indem sie eine Zertifizierung von Drittanbietern erhalten, die Standards für die Sicherheit verbundener Geräte entwickelt haben, wie das *Underwriters Laboratory* und die *Wireless Industry Association CTIA*.

Wichtig sind auch die Handlungsempfehlungen der *Federal Trade Commission (FTC)* zu „connected devices". Wie der kürzlich verabschiedete California Consumer Privacy Act – CCPA (*Spies,* ZD-Aktuell 2018, 04318) wird das das neue IoT-Gesetz ziemlich sicher US-weite oder vielleicht sogar weltweite Auswirkungen haben, wenn man auf die Bedeutung des kalifornischen Markts abstellt.

Weiterführende Links

Vgl. auch *Determann*, ZD 2018, 443; ZD-Aktuell 2018, 06019; ZD-Aktuell 2018, 05988; ZD-Aktuell 2018, 06274 und *Hoeren/Pinelli*, MMR 2018, 711 (erscheint in MMR 11/2018).