Martin Klein-Hennig, Felix Schmidt

Zurück auf Los – Die IT-Sicherheit zurück in der Steinzeit

Haftung und Lösungen für IT-Sicherheitsmängel im Internet of Things

Keine IT ist vollständig sicher, damit hat man sich abgefunden. Trotzdem hatte man den Eindruck, dass sich die IT-Sicherheit auf einem guten Weg befindet. Unternehmen und Betroffene konnten mit einem vertretbaren Aufwand ein ebenso vertretbares Risiko erreichen. Dann kam das Internet of Things. Lampen, Waschmaschinen, Kühlschränke, Überwachungskameras und Autos werden zunehmend Teil des Internets. Die Welt scheint damit wieder zerbrechlicher.

1 Bedrohung durch das Internet of Things

„Es gibt kein Internet der Dinge. Es gibt nur viele ungepatchte, verwundbare, kleine Computer im Internet.", lautet ein provokanter Tweet[1] des Sicherheitsforschers John Adams, der für sechs Jahre Twitters Sicherheitsteam leitete. Welches Gefahrenpotential das Internet of Things für Endanwender, Firmen und das Internet selbst darstellt und wie Lösungswege aussehen, soll im Folgenden beleuchtet werden.[2]

1 „There is no Internet of Things. There are only many unpatched, vulnerable small computers on the Internet.", https://twitter.com/netik/status/765276366304489472.

Dr. Martin Klein-Hennig

ist nach Studium und Promotion an der Uni Oldenburg bei der datenschutz nord GmbH tätig und auf Penetrationstests von Netzwerken, Webapplikationen und Smartphone-Apps spezialisiert.
E-Mail: MKlein-Hennig@datenschutz-nord.de

Felix Schmidt

studierte Rechtswissenschaften an der Europa-Universität Viadrina. Danach war er als Rechtsanwalt in einer berliner Anwaltsboutique tätig bevor er Justitiar bei der datenschutz nord GmbH wurde. Felix Schmidt ist Lehrbeauftragter für Datenschutzrecht an der Europa-Universität Viadrina.
E-Mail: FSchmidt@datenschutz-nord.de

1.1 Internet of Bots

Im Jahr 2016 gab es mehrere Sicherheitsvorfälle, die durch Botnetze verursacht wurden. Bei Botnetzen handelt es sich um Netzwerke aus gekaperten Systemen, die über das Internet von einer oder mehreren Kommandozentralen (sog. Command and Control Server) Befehle eines Angreifers entgegennehmen. Der Angreifer hat also eine Vielzahl an Computern unter seiner Kontrolle, die er für seine Zwecke missbrauchen kann. Diese Zwecke sind unter anderem das Auslesen von sensiblen Daten, der Versand von Spam-Mails, die Durchführung von Distributed Denial-of-Service (DDoS)-Attacken sowie die Verbreitung von Schadsoftware und weitere Angriffe auf Systeme Dritter zur Vergrößerung des eigenen Botnetzes.

Ein vielzitiertes Beispiel ist das Mirai-Botnetz, das sich durch die gleichnamige Schadsoftware ausgebreitet hat[3]. Da der Quellcode der Schadsoftware veröffentlicht wurde, konnten Schlüsse über den Ausbreitungsweg und die betroffenen Systeme gezogen werden. Der größte Teil der Geräte im Mirai-Botnetz waren IoT-Geräte wie Netzwerkkameras und Heimrouter. Zugang zu Systemen erlangte die Schadsoftware über voreingestellte Standardkennwörter der Geräte. In den ersten 24 Stunden sollen schätzungsweise 120.000 Systeme gekapert worden sein.[4] Das Mirai-

2 Allgemeine Darstellung der Herausforderungen bei der Nutzung von IoT-Geräten, auch über IT-Sicherheit und Datenschutzrecht hinaus; siehe Schmitz/Rammos, (K)eine neue Ethik für das Internet der Dinge?, DSRITB 2015, 411.

3 Siehe z.B. Biggs, Hackers release source code for a powerful DDoS app called Mirai, https://techcrunch.com/2016/10/10/hackers-release-source-code-for-a-powerful-ddos-app-called-mirai/.

4 MalwareTech, Mapping Mirai: A Botnet Case Study, https://www.malwaretech.com/2016/10/mapping-mirai-a-botnet-case-study.html.

Botnetz nutzte die Internetanbindung seiner Bots zur Durchführung von Distributed Denial-of-Service Attacken, um Websites und Webdienste durch eine große Anzahl gleichzeitiger Anfragen zu überlasten. Zu den prominenteren Betroffenen zählen der Blog des IT-Sicherheitsjournalisten Brian Krebs, der französische Webhoster OVH, der DNS-Provider Dyn und damit indirekt die Verfügbarkeit vieler großer Internetplattformen wie GitHub, Twitter und airbnb.

Das BASHLITE Botnetz verbreitete sich bereits 2014 und wurde ebenfalls zur Durchführung von DDoS-Attacken eingesetzt. 96% der Systeme im BASHLITE Botnetz waren IoT-Geräte, 95% davon wiederum Kameras und digitale Videorecorder. Zur Verbreitung nutzte das Botnetz mehrere Schwachstellen der auf den Geräten installierten, linux-basierten Betriebssysteme und der dazugehörigen Software. Die Größe der Ausbreitung des BASHLITE-Botnetzes wird auf ca. eine Million Systeme geschätzt.[5]

Der „Linux.Darlloz"-Wurm ist eine Schadsoftware, die sich ebenfalls auf IoT-Geräten wie Routern, Kameras und Mediaplayern ausbreitet und deren Rechenkapazität verwendet, um Kryptowährungen zu „schürfen". Die Verbreitung erfolgte über eine Sicherheitslücke in PHP, einer Programmiersprache, die hauptsächlich für Webapplikationen eingesetzt wird.

1.2 IoT-Gefährdungen

Die oben genannten Beispiele zeigen, dass IoT-Geräte offenbar leicht zu kapern und daher beliebte Botnetz-Systeme sind. Dies liegt an Gefährdungen, die grundsätzlich auf alle Computersysteme mit Netzanbindung zutreffen, aber bei IoT-Geräten durch ihre Verbreitung und ihren unkritischen Einsatz besonders ins Gewicht fallen.

1.2.1 Fehlerhafte Software

Die Hauptfunktion eines IoT-Geräts ist zunächst nicht die Anbindung an Netzwerke; ein Sensor soll in erster Linie messen, eine Schließanlage soll schließen, eine Glühbirne leuchten. Ins IoT kommt das Gerät durch zusätzliche Elektronik, die das Auslesen und Steuern der eigentlichen Funktionen übernimmt, sowie Komponenten, die die Kommunikation mit anderen Geräten (z.B. über WLAN oder Bluetooth) regeln.

Zum Einsatz kommen dabei generische und günstige „System-on-a-chip"-Lösungen (SOC). Ein SOC enthält alle nötigen Computerkomponenten wie Prozessor, Arbeitsspeicher, Peripherie und Netzwerkfunktionen. Die Funktionalität erhält ein SOC über seine Firmware, also die im Gerät eingebettete und ggf. umprogrammierbare Software. Häufig handelt es sich hier aus Kostengründen um ein Open Source Betriebssystem wie z.B. Linux, das vom Hersteller mehr oder weniger gut auf den Verwendungszweck angepasst wird. IoT-Geräte sind also tatsächlich kleine Computersysteme, die immer leistungsfähiger werden.

Bei der Erstellung, Anpassung und Bereitstellung der Firmware durch den Hersteller können sowohl durch Programmierfehler als auch durch Fehlkonfiguration Sicherheitslücken entstehen. Eine Softwareentwicklung ist komplex und aufwändig. Um Entwicklungszeit zu sparen, wird auf existierende Bibliotheken (z.B. für Netzwerkfunktionen und Serverprogramme) und Betriebssysteme (z.B. Linux) zurückgegriffen, fehlende Funktionen und Anpassungen nimmt der Hersteller selber vor. Ein Sicherheits- oder Penetrationstest des Geräts ist meist nicht vorgesehen, sodass Sicherheitslücken erst bekannt werden, wenn das Gerät auf dem Markt ist.

Eine Verpflichtung zur Durchführung von Sicherheitstests könnte dazu beitragen die Sicherheit von Software für IoT-Geräte zu erhöhen.[6]

1.2.2 Versorgung mit Updates

Wird eine Sicherheitslücke in der Firmware eines Geräts bekannt, sollte diese behoben und die neue Firmware an alle Geräte ausgerollt werden. Dies ist bei PC-Betriebssystemen und -Software alltäglich. Für Hersteller von IoT-Geräten bedeutet die Entwicklung, Prüfung und Bereitstellung von Sicherheitsupdates jedoch einen erheblichen Mehraufwand. Denkbare Anforderungen an Hersteller wären hier:

- Zeitnahe Behebung von festgestellten Sicherheitslücken. Der Hersteller muss eine Anlaufstelle für die Meldung von Schwachstellen angeben und Prozesse für den schnellen Umgang mit Sicherheitsmeldungen implementieren.
- Prüfung der Software zur Verifizierung. Zur Qualitätssicherung und Verifizierung der Behebung der Schwachstelle müssen Tests durchgeführt werden, bevor ein Update verteilt wird.
- Bereitstellung der Updates über eine sichere Infrastruktur mit hoher Verfügbarkeit. Zum Schutz vor Kompromittierung muss das Update verschlüsselt und/oder mit Authentizitätsprüfung angeboten werden. Die Verfügbarkeit des Updates muss sichergestellt sein.
- Festschreibung von Mindestdauern, über die ein Produkt mit Sicherheitsupdates versorgt wird.

All diese Maßnahmen sind aufwendig und kostenintensiv. Der Durchschnittspreis und die damit einhergehende Preiserwartung der Kunden im IoT-Sektor lassen Zweifel aufkommen, ob Hersteller diesen Anforderungen gerecht werden können.

1.2.3 Fehlkonfiguration

Schwachstellen entstehen nicht nur durch Fehler in der Programmierung. Auch Fehlkonfigurationen durch Hersteller oder Anwender können ein Gerät für Angriffe verwundbar machen. So konnte sich das Mirai-Botnetz ausbreiten, weil es eine Datenbank von 61 Standardkennwörtern für unterschiedliche IoT-Geräte nutzte[7].

Einige dieser Standardkennwörter werden herstellerseitig festgelegt und sind meistens schwach (z.B. Benutzername „admin", Kennwort „admin"). Der Hersteller geht davon aus, dass der Anwender das Kennwort bei Inbetriebnahme ändert – auf eines das sicher und schwer zu erraten ist.

Eine vernünftige Lösung wäre das Setzen von individuellen, geräteabhängigen Erst-Kennwörtern ab Werk, wie es z.B. bei manchen DSL-Routern der Fall ist. Sofern sich diese nicht aus weiteren, öffentlich verfügbaren Geräteeigenschaften berechnen las-

5 Spring, BASHLITE Family of Malware Infects 1 Million IoT Devices, https://threatpost.com/bashlite-family-of-malware-infects-1-million-iot-devices/120230/.

6 Alexander Straßheim, Sebastian Schreiber, IoT-Penetrationstest, in diesem Heft, S. 623 – 627

7 Ragan, Here are the 61 passwords that powered the Mirai IoT botnet, http://www.csoonline.com/article/3126924/security/here-are-the-61-passwords-that-powered-the-mirai-iot-botnet.html.

sen, werden dadurch die Geräte abgesichert, deren Anwender sich mit der Kennwortänderung nicht beschäftigt haben. Mirai hätte wenig Chancen.

Ebenfalls denkbar ist ein durch die Software ausgeübter Zwang, das Kennwort vor der vollständigen Inbetriebnahme des Geräts zu ändern.

Ziel des Entwicklungsprozesses beim Hersteller sollte „Security by Design" sein, ein Prinzip, das verlangt, dass die Abläufe innerhalb der Software bereits bei der Planung auf Sicherheit ausgerichtet sind. Hierzu gehört auch die zwingende Verwendung von verschlüsselten Protokollen und Authentisierungsmechanismen.

1.2.4 Öffentlicher Zugang

Ein Dienst, den ein IoT-Gerät über das Netzwerk zur Verfügung stellt, muss in irgendeiner Form für den Anwender und evtl. auch weitere Systeme erreichbar und ansprechbar sein. Mit anderen Worten, eine Schnittstelle wird benötigt. Durch die Teilnahme am Netzwerk, sei es LAN oder WLAN, erhält das Gerät eine interne IP-Adresse, mit der es innerhalb des Heimnetzwerks angesprochen werden kann. Die Bereitstellung einer Schnittstelle (z.B. eine Weboberfläche zur Darstellung eines Kamerabilds und Kontrolle der Kamera) geschieht über einen oder mehrere Ports, an denen über bestimmte Protokolle Daten ausgetauscht werden können.[8]

Ein solcher Port ist zunächst nur aus dem Heimnetz zugänglich. Damit ein Gerät von außerhalb des Heimnetzes, aus dem Internet, erreichbar ist, muss der Router, über den die Internetverbindung erfolgt, entsprechend konfiguriert werden (sog. Port-Forwarding). Danach ist der Dienst über die dem Anschluss zugeordnete IP-Adresse, mit dem eingerichteten Port, für jeden Internetteilnehmer zugänglich.

Spätestens mit einer derartigen „Veröffentlichung" eines Dienstes sollte man sich als Anwender darüber im Klaren sein, dass man sein Gerät, und damit implizit sein Heimnetzwerk und ggf. Geräte Dritter, dem Risiko von Angriffen aussetzt. Hier ist Aufklärung angesagt, denn viele Anwender sind sich der Problematik nicht bewusst. Da eine eingenistete Schadsoftware möglichst lange unentdeckt bleiben soll, beeinträchtigt sie die eigentliche Funktion des Geräts gewöhnlich nicht. Wenn die Kamera weiterhin Bilder vom Hinterhof liefert, merkt der Anwender nicht, dass Kamera und Internetanschluss nebenbei noch für eine DDoS-Attacke auf eine Website genutzt werden. Vielleicht kümmert es ihn noch nicht einmal, denn er ist ja nicht unmittelbar betroffen.

Als eine technische Maßnahme wäre die Einrichtung eines VPN (Virtual Private Network), in dem die IoT-Dienste betrieben werden, empfehlenswert. Der Zugang wäre somit über die Zugangskontrolle zum VPN gesichert. Allerdings erfordert diese Maßnahme technisches Know-How, das nicht jeder Anwender mitbringt. Ebenso wie die regelmäßige Überwachung des eigenen Internetverkehrs. Diese würde zwar helfen, Schadsoftware im eigenen Netzwerk zu erkennen, ist aber nur für technisch versierte Anwender durchzuführen.

8 Für eine Zusammenfassung des technischen Hintergrunds siehe: Vogelgesang, Möllers, Hessel, Potel, Auf der Jagd nach Schwachstellen – Eine strafrechtliche Bewertung von Portscans, DuD 8, 2017.

2 Haftung für IT-Sicherheitsmängel[9]

Angenommen Ihr Onlineshop war wegen eines DDoS-Angriffs das ganze Wochenende nicht am Netz. Unabhängig von etwaigen Versicherungsansprüchen würden Sie gern den entstandenen Schaden beim Verursacher amortisieren. Gegen wen bestehen evtl. Schadensersatzansprüche?

Nicht betrachtet werden soll hierbei die Haftung des unmittelbaren Täters, dem Botnetz-Betreiber. Dieser haftet für sein Verhalten unmittelbar aus zumindest § 823 Abs. 2 BGB i.V.m. § 303b StGB und § 826 BGB. Fraglich ist vielmehr, ob auch die anderen Beteiligten, die durch den Betrieb eines unsicheren IoT-Geräts erst den Angriff ermöglicht haben, mit zur Verantwortung gezogen werden können. Dies ist vor allem aus zwei Gründen prüfenswert.

Zum einen wird der direkte Angreifer nur schwer zu ermitteln sein. Dagegen dürfte sich der Betreiber eines IoT-Geräts z.B. über die IP Adresse ermitteln lassen, und damit auch der Hersteller des eingesetzten Geräts.

Zum anderen besteht nur im Fall einer Haftung dieser weiteren am Taterfolg beteiligten Personen, die Hoffnung auf eine Verbesserung der hier skizzierten IoT-Sicherheitslage. Da der Missbrauch von IoT-Geräten als Angriffswaffe gegen Dritte die Funktionalität der Geräte nur unwesentlich beeinträchtigt, haben Nutzer von IoT-Geräten andernfalls keine unmittelbare Motivation, an der Verbesserung der Sicherheitslage mitzuwirken.

2.1 Ansprüche gegen den Hersteller/ Verkäufer

Zunächst erscheint es angemessen, den IoT-Hersteller haften zu lassen, wenn er den Missbrauch seiner in den Verkehr gebrachten Produkte durch Dritte ermöglicht, indem er bestehende Fehler in der Software nicht behebt. Leider spiegelt die deutsche Rechtslage dieses erste Judiz nicht ohne weiteres wieder.

Weder der Käufer des IoT-Gerätes, noch das Opfer haben zumeist ein direktes Vertragsverhältnis zum Hersteller des Produkts. Somit kommen nur deliktische Ansprüche in Betracht, die aber im Ergebnis nicht zum Erfolg führen.[10]

2.1.1 Das Produkthaftungsgesetz

Ansprüche aus § 1 ProdHaftG kommen nur dann in Betracht, sofern ein Produktfehler schon zum Zeitpunkt des Inverkehrbringens bekannt war. Damit wird ein Anspruch zumeist ausscheiden bzw. schwer nachweisbar sein.[11]

9 Umfassende Studie im Auftrag des BSI hierzu Spindler, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, 2007 (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gutachten_pdf).

10 Zu den Mängeln bei der Verflechtung von IT-Sicherheit und Produktsicherheit siehe Bräutigam/Kindt, Industrie 4.0, das Internet der Dinge und das Recht, NJW 2015, 1137, 1140 ff.; beide sprechen sich für einen neuen Rechtsbegriff aus, der Resilienz – die Widerstandsfähigkeit eines Systems gegen Eingriffe von außen. In dieser Frage besteht aber noch weitgehender Klärungs- und Forschungsbedarf.

11 Zudem wären durch das Produkthaftungsgesetz auch bloße Vermögensschäden nicht abgedeckt, Spreu in Palandt, § 1 ProdHaftG, 76. Aufl., 2017.

2.1.2 § 823 Abs. 1 BGB

Der Hersteller eines Produktes haftet grundsätzlich für Konstruktionsfehler und daraus entstandene Schäden.[12] Ein Hersteller darf ein Produkt nicht in den Verkehr bringen, von dem er weiß, dass dieses IT-Sicherheitsschwachstellen aufweist. Dies bedeutet aber nicht, dass der Hersteller automatisch für jeden Programmierfehler zur Verantwortung gezogen werden kann. Denn, sofern man dem Hersteller nicht nachweisen kann, dass er von der Schwachstelle wusste, als er das Produkt auf dem Markt gebracht hat, treffen diesen nur nachträgliche Produktbeobachtungs- und Warnpflichten. In diesem Bereich wird es sehr schwierig werden, dem Hersteller eine Pflichtverletzung vorzuwerfen und diese auch noch prozessual durchzusetzen.

Im Ergebnis wird auch ein erfolgreicher Anspruch hinsichtlich der Verletzung von Produktbeobachtungspflichten nicht die IT-Sicherheitslage in der Breite verbessern, da es weiterhin dem Endnutzer obliegt, bei evtl. Warnung des Herstellers, fehlerhafte Geräte vom Netz zu nehmen.

2.1.3 BSIG oder Privacy by design

Mit den Änderungen des IT-Sicherheitsgesetzes wurden auch die Softwarehersteller in den Blick genommen. Nach § 7a Abs. 1 S. 1 BSIG kann das Bundesamt für Sicherheit in der Informationstechnik zur Erfüllung seiner Aufgaben auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte und Systeme untersuchen. Das Bundesamt darf seine Erkenntnisse sogar veröffentlichen, soweit dies zur Erfüllung dieser Aufgaben erforderlich ist, § 7a Abs. 2 S. 2 BSIG. Zuvor ist dem Hersteller der betroffenen Produkte und Systeme mit angemessener Frist Gelegenheit zur Stellungnahme zu geben. Direkte Pflichten an den Hersteller finden sich im Gesetz damit nicht. So fehlt es weiterhin an allgemeingültigen und umfassenden Kriterien, die Hersteller bei der Konstruktion zu beachten haben. Bewertungen nach Common Criteria etc. sind weiterhin keine Bedingung für den Markteintritt eines Unternehmens.

Wenn schon kein allgemeiner Grundsatz von IT-Security by Design besteht, ist vielleicht ein Rückgriff auf den Grundsatz Privacy by Design zielführend. Die verantwortliche Stelle einer Datenverarbeitung ist ab 25.05.2018 verpflichtet, Datenverarbeitungsanlagen so zu gestalten, dass diese datenschutzkonform betrieben werden können, Art. 25 Abs. 1 DS-GVO. Hierbei ist unter anderem der Stand der Technik zu berücksichtigen. Für den Fall IoT führen die Überlegungen aber auch an dieser Stelle nicht weiter. Zum einen trifft diese Pflicht nicht den Softwarehersteller, sondern die Unternehmen, welche die Produkte tatsächlich einsetzen. Zum anderen verarbeitet nicht jede IoT-Anwendung auch personenbezogene Daten.

2.1.4 Mängelansprüche aus dem Kaufvertrag

Eine Überlegung ist es wert, ein unsicheres IoT-Gerät als mangelhaft nach §§ 434, 633 BGB zu bewerten, sodass der Verkäufer für evtl. Schäden aufkommen bzw. ein mangelfreies IoT-Gerät liefern müsste. Leider ist diese Konstellation aus mehreren Gründen nicht ganz passend.

Zum einen liegen Ansprüche aus dem Gewährleistungsrecht beim Käufer des IoT-Geräts und nicht bei einem potentiellen Opfer eines DDoS-Angriffs. Auch vorausgesetzt der Käufer tritt den Anspruch ab oder eine Drittschadensliquidation wird angenommen, dürfte aber kein Mangel der Software gegeben sein. Diese wäre nur der Fall, sofern die vereinbarte Beschaffenheit nicht gegeben ist oder die vorgesehene Verwendung beeinträchtigt wird. Bei dem Missbrauch von IoT-Geräten als Angriffswerkzeug liegt eine funktionale Beeinträchtigung aber unter Umständen gar nicht vor. Bloße IT-Sicherheitsmängel, die die Funktionalität nicht beeinflussen sind von der Rechtsprechung und Literatur nicht als Mangel anerkannt.[13]

2.2 Ansprüche gegen den IoT-Nutzer[14]

Der Nutzer eines IoT-Produktes kann nicht nur Opfer der IT-Sicherheitslücke sein. Vielmehr können ihn auch Verkehrssicherungspflichten treffen, Beeinträchtigungen aus seinem Netz gegenüber Dritten entgegenzuwirken.

Als Anspruchsgrundlagen kommen, wie bisher, deliktische Ansprüche in Betracht.[15]

2.2.1 § 823 Abs. 1 BGB

Als Schutzgüter des § 823 Abs. 1 BGB kommen das Eigentumsrecht am Datenbestand sowie der eingerichtete und ausgeübte Gewerbebetrieb in Frage. Bloße Vermögensschäden sind nach § 823 Abs. 1 BGB nicht erfasst, so dass zumeist nur ein geringer Teil des Schadens erfasst sein wird.[16] Dennoch lohnt sich mangels Alternativen eine genaue Prüfung.

§ 823 Abs. 1 BGB setzt neben anderen Tatbestandsmerkmalen eine Pflichtverletzung des IoT-Nutzers voraus. Äußerst fraglich ist aber, welche dies sein soll. Täter, Anstifter oder Gehilfe des IT-Angriffs war der IoT-Nutzer sicherlich nicht, so dass ihn nur allgemeine Verkehrssicherungspflichten treffen können, indem er schuldhaft gebotene IT-Sicherungsmaßnahmen unterlassen hat. Wer eine Gefahrenquelle schafft, ist grundsätzlich verpflichtet, die notwendigen und zumutbaren Vorkehrungen zu treffen, um eine Schädigung anderer zu vermeiden.

Eine Haftung wird man demzufolge annehmen können, sofern folgende Voraussetzung gegeben sind:

- Herrschaft über eine Gefahrenquelle,
- Unterlassen notwendiger Sicherungsmaßnahmen,
- Technische und wirtschaftliche Zumutbarkeit der Maßnahmen.[17]

In der Regel wird man davon ausgehen können, dass die Inbetriebnahme eines IoT-Geräts eine entsprechende Gefahrenquelle

12 Spindler: IT-Sicherheit und Produkthaftung – Sicherheitslücken, Pflichten der Hersteller und der Softwarenutzer, NJW 2004, S. 3245, 3146 f.

13 BGH 04.11.1987 – VIII ZR 314/86 und Urt. v. 05.06.2014 – VII ZR 276/13; OLG Hamburg Urt. v. 16.08.2013 – 9 U 41/11; umfassend Deusch, Eggendorfer: Softwaremängel 4.0 – zu Risiken und Nebenwirkungen fragen Sie Ihren Softwareentwickler oder Sachverständigen, DSRITB 2015, 833, 839 f.

14 Nur zur Klarstellung ist festzuhalten, dass die Betrachtungen nicht den Pflichtenkreis des IoT-Nutzers abschließend beschreiben. Geprüft wurden Ansprüche Dritter gegen den Nutzer. Unabhängig davon bestehen darüber hinaus zahlreiche andere Pflichten aus dem IT-Sicherheitsrecht, die aber nicht den hier angenommenen Fall eines DDoS-Angriffs umfassen (z.B. § 91 Abs. 2 AktG, § 130 OWiG, § 43 GmbHG).

15 Vertragliche Obliegenheiten des IoT-Nutzers zu eigenen Vertragspartners ergeben sich zumeist als Nebenpflicht aus dem Schuldverhältnis, § 241 Abs. 2 BGB.

16 Spreu in Palandt, § 823 Rdn. 9 und 11, 76. Aufl. 2017.

17 Spreu in Palandt, § 823 Rdn. 46 ff., 76. Aufl. 2017.

geschaffen hat. Fraglich ist daher vor allem, welche Sicherungsmaßnahmen das Gesetz dem IoT-Nutzer abverlangt.

Unterlassen notweniger Sicherungsmaßnahmen

Die bloße Schaffung einer Gefahrenquelle führt nicht automatisch dazu, jedwede Sicherungsmaßnahme als rechtlich geboten anzusehen. Vielmehr bleibt auch Raum, bestimmte Gefahren und hierdurch verwirklichte Schäden dem allgemeinen Lebensrisiko zuzuordnen. Die Annahme von Verkehrspflichten bedarf daher einer besonderen Begründung.

Ob und inwiefern den privaten Nutzer Maßnahmen zur Sicherung seiner IT auferlegt werden können, ist juristisch nicht geklärt. Verkehrssicherungspflichten scheiden jedenfalls nicht deshalb aus, weil eine Gefahr erst durch den unerlaubten und schuldhaften Eingriff eines Dritten entstanden ist, da der IoT-Nutzer mit solchen Angriffen rechnen muss.[18] Bei der Konkretisierung der vom IoT-Nutzer zu treffenden Sicherheitsmaßnahmen wird man auf die berechtigten Sicherheitserwartungen des betroffenen Verkehrskreises abzustellen haben. War das Sicherheitsproblem bekannt? Und welche Möglichkeiten standen dem IoT-Nutzer zur Verfügung?

Auch wenn der Verkehrskreis objektiv zu bestimmen ist, wird man sicherlich einen Unterschied machen müssen, ob es sich bei dem IoT-Betreiber um einen Verbraucher handelt oder einen Unternehmer, der evtl. IoT-Dienste sogar in die eigene Leistung eingebunden hat oder über Spezialwissen verfügt.

Verbrauchern wird man in der Regel nicht vorwerfen können, Sicherheitsprobleme nicht erkannt zu haben. Die IT-Sicherheitsprobleme im IoT-Segment sind noch nicht allgemein bekannt. Dienstleistungen in diesem Bereich sind derzeit noch neu am Markt. Zudem erhält der Verbraucher, über die bloße Funktionalität hinaus, grundsätzlich keine Informationen darüber, dass IoT-Technologie im Produkt verbaut ist, noch welche Software von welchem Hersteller, mit welcher Funktion zum Einsatz kommt. Es ist bei zunehmender Komplexität der Geräte auch nicht zu erwarten, dass der Durchschnittskunde in naher Zukunft überhaupt einen ausreichenden Wissenstand erreichen wird, um selbstständig einwirken zu können. Der eindeutige Trend ist vielmehr, Hard- und Software aus dem Einzugsbereich des Verbrauchers zu entziehen.

Anders ist die Lage bei Unternehmen und Fach-Anwendern von IoT-Geräten. Von diesen kann durchaus erwartet werden ein Grundverständnis über die eigenen IT-Systeme zu entwickeln und Gefahren zu beobachten.

Fraglich ist dann vielmehr, welche Maßnahmen technisch und wirtschaftlich zumutbar sind.

Wie bei der Feststellung der verkehrskreisspezifischen Sicherheitserwartungen, sind die Anforderungen nicht statisch. Vielmehr sind sie einem fortlaufenden technischen Wandel unterworfen. Wirtschaftlich zumutbar ist die Ergreifung von Sicherungsmaßnahmen jedenfalls dann, wenn sie nicht vollkommen außerhalb jedes vernünftigen Verhältnisses zu dem Sicherheitsgewinn stehen. Sofern der IoT-Hersteller daher Wartungsverträge für eine Software bzw. Updates zur Verfügung stellt, wird man vom IoT-Anwender verlangen können, diese auch in Anspruch

18 Vgl. BGH Urt. v. 06.02.2007 – VI ZR 274/05.

zu nehmen. Hierdurch entstehende Kosten und Aufwände müssen hingenommen werden. Das Gleiche gilt zum Beispiel für die Absicherung des Netzwerkes oder der Konfiguration der Geräte. Die Einrichtung eins VPN, das Monitoren des Netzwerkverkehrs bzw. die Implementierung von sicheren Passworten am Gerät dürfte vom Fachanwender erwartet werden können.

Sollte das IoT-Produkt keine entsprechenden IT-Sicherheitseinstellungen unterstützen, muss die Lücke außerhalb des Geräts geschlossen werden. Dies könnte über die oben genannte VPN-Lösung oder ein als „Jump Host" dazwischengeschaltetes, vertrauenswürdiges System geschehen. Andernfalls darf das IoT-Gerät nicht zum Einsatz kommen. In Erwägung zu ziehen wäre auch, den Hersteller direkt in die Pflicht zu nehmen. Dieser ist nach § 242 BGB einen gewissen Zeitraum verpflichtet, eine Wartung der Programme anzubieten, um die wirtschaftlichen Vorteile der Investition nicht unverhältnismäßig verfallen zu lassen.[19]

Somit kann im Ergebnis festgestellt werden: Nicht gewartete und mangelhaft installierte IoT-Geräte sollten von Unternehmen und Fachanwendern nicht am Netz gehalten werden, da eine Haftung für die hieraus entstanden Schäden bei Dritten nach § 823 Abs. 1 BGB droht. Gegenüber Verbrauchern wird man eine solche Haftung nicht annehmen können.

2.2.2 § 823 Abs. 2 BGB i.V.m. Art. 32 DS-GVO oder § 13 Abs. 7 TMG

Nachteilhaft aus der Sicht des DDoS-Opfers ist, dass über § 823 Abs. 1 BGB grundsätzlich nicht die Möglichkeit besteht, Vermögensschäden einzuklagen. § 823 Abs. 2 BGB eröffnet diese Möglichkeit. Hierfür ist es erforderlich, dass über § 823 Abs. 2 BGB hinaus ein Schutzgesetz verletzt wurde. Hierfür müsste das Gesetz den Zweck verfolgen, das Opfer des DDoS-Angriffs vor dem unsicheren System eines Dritten zu schützen.

In Betracht kommen hierbei die IT-Sicherheitsvorschriften des Datenschutzrechts, § 9 BDSG und bald Art. 32 DS-GVO.[20] Fraglich ist, ob diese die richtige Schutzrichtung aufweisen. Unproblematisch könnte die betroffene natürliche Person gegen die verantwortliche Stelle der Datenverarbeitung einen Schadensersatzanspruch begründen. Beispiel: Ein Online-Shop ist verpflichtet, die Daten seiner Kunden vor einem unbefugten Zugriff zu schützen. Nach Art. 32 Abs. 1 lit. b DS-GVO muss er sogar die Belastbarkeit seiner Datenverarbeitungssysteme sicherstellen. Es ist aber sehr fraglich, ob aus Art. 32 DS-GVO bzw. § 9 BDSG gleichzeitig die Pflicht erwächst, die personenbezogenen Daten einer anderen verantwortlichen Stelle zu schützen. Eine solche Pflicht ist vom Anwendungsbereich der Norm nicht mehr umfasst. Die Pflichten des Datenschutzrechtes setzen voraus, dass personenbezogene Daten betroffen sind. § 9 BDSG legt klar im ersten Satz fest, dass nur solche verantwortlichen Stellen verpflichtet sind technische und organisatorische Maßnahmen zu ergreifen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen. Ein Nutzer, der auf seinem IoT-Gerät selbst keine personenbezogenen Daten verarbeitet, kann daher nicht Verpflichteter des Gesetzes sein. Eine Haftung über § 9 BDSG kommt daher nicht in Betracht. Dies muss auch dann gelten, sofern für die verantwortliche Stelle nicht die eigenen Daten betroffen sind, sondern nur fremde Daten. Andernfalls würde ein vom Schadensereignis unabhängiges, zufälliges Ereignis die Haftung begründen. Das kann nicht Schutzzweck des Gesetzes sein.

Schadensersatzansprüche gegenüber Privatnutzern von IoT-Geräten scheitern zudem daran, dass schon der Anwendungsbereich der Datenschutzgesetze bei Datenverarbeitungsvorgängen zu persönlichen oder familiären Zwecken nicht eröffnet ist, § 1 Abs. 2 Nr. 3 BDSG, Art. 2 Abs. 2 lit. c DS-GVO.

Darüber hinaus könnte aber eine Haftung nach § 823 Abs. 2 BGB i.V.m. § 13 Abs. 7 TMG in Betracht kommen. Anders als bei Art. 32 DS-GVO ist es der ausdrückliche Wille des Gesetzgebers, den Pflichtenkreis der Norm auch über die eigenen Systeme und Daten hinaus zu erstrecken. Hierzu heißt es in der Gesetzesbegründung: „Ein wesentliches Ziel der Regelung ist es, einen der Hauptverbreitungswege von Schadsoftware einzudämmen: das unbemerkte Herunterladen allein durch das Aufrufen bzw. Nutzen einer dafür von Angreifern präparierten Website (sogenannte Drive-by-Downloads). Bereits durch eine regelmäßige Aktualisierung der für das Telemedienangebot verwendeten Software (Einspielen von Sicherheitspatches) seitens der Websitebetreiber könnten zahlreiche dieser Angriffe vermieden werden. Kompromittierungen können zudem auch durch Inhalte erfolgen, auf die der Diensteanbieter keinen unmittelbaren technischen Einfluss hat (zum Beispiel über kompromittierte Werbebanner, die auf der Webseite eingebunden sind). Dagegen sind organisatorische Vorkehrungen zu treffen. Hierzu zählt beispielsweise, Werbedienstleister, denen Werbefläche eingeräumt wird, vertraglich zu notwendigen Schutzmaßnahmen zu verpflichten. Die entsprechenden Maßnahmen sind im Rahmen der jeweiligen Verantwortlichkeit zu treffen."[21]

Nach § 13 Abs. 7 TMG sind aber nur „Diensteanbieter" verpflichtet, mit technischen und organisatorischen Vorkehrungen sicherzustellen, dass kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist.

Hierfür müsste es sich bei IoT-Geräten um einen elektronischen Informations- und Kommunikationsdienst handeln. Zumeist wird man nicht davon ausgehen können, dass das reine IoT-Gerät unter diesen Anwendungsbereich fällt. Es ist nicht Sinn und Zweck des Gesetzes ausnahmslos jede Kommunikation über das Internet unter das TMG zu fassen. Vielmehr müssen mit dem Dienst Inhalte elektronisch bereitgestellt werden.[22] Diesen inhaltlichen Außenbezug weisen IoT-Systeme nicht unbedingt auf. Unternehmen, die IoT-Geräte nur für die eigene Informationsgewinnung betreiben, z.B. Kameraüberwachung oder Energiesteuerung, fallen daher nicht unter den Anwendungsbereich. Anders liegt der Fall auch nicht, sofern IoT-Geräte von einem Unternehmen zur Information der Kunden bereitgehalten werden, z.B. IoT-Plattformen zur Steuerung der Solaranlage. Auch hier dient die Datenübermittlung der IoT-Geräte nur internen Zwecken.

Somit kommen Schadensersatzansprüche nach § 823 i.V.m. einem Schutzgesetz im Ergebnis nicht in Betracht. Wiedermal rächt sich die nur sektorspezifische und uneinheitliche Regelung der IT-Sicherheit.[23]

19 LG Köln Urt. v. 16.10.1997 – 83 O 26/97.

20 Die DS-GVO gilt ab dem 25.05.2018. Art. 32 DS-GVO wird § 9 BDSG hierbei vollständig ersetzen.

21 BT-Drucks. 18/4096, S. 34.

22 Spindler/Schuster/Ricke, 3. Aufl. 2015, TMG § 1 Rdn. 4.

23 Für den Bereich der IT-Sicherheit bei der Kommunikation im Internet der Dinge bestehen keine allgemeingültigen Vorgaben, Grünwald/ Nüßing, Machine To Machine (M2M)-Kommunikation, MMR 2015, 378, 383.

2.2.3 Durchsetzbarkeit der Ansprüche

Neben der nur in sehr engen Bereichen bestehenden Haftung stellt es ein weiteres Problem dar, dass Ansprüche nur sehr schwer durchzusetzen sein werden. Das Opfer steht vollständig in der Beweislast, dass der IoT-Nutzer Verkehrssicherungspflichten nach § 823 Abs. 1 BGB unterlassen hat. Aus der bloßen Datenübertragung kann dies nicht geschlussfolgert werden. Zudem werden IoT-Geräte weltweit als Angriffswerkzeug genutzt, so dass Ansprüche nur schwer geltend gemacht werden können. Es dürfte dem Unternehmensimage auch nicht zuträglich sein, sich an einzelnen Unternehmen in Deutschland „zu bereichern", weil diese nun mal greifbar sind.

Es bleibt auch fraglich, wie hoch der Schadensersatzanspruch gegen den einzelnen IoT-Nutzer ist, da die Pflichtverletzung nur einen Bruchteil zum tatsächlichen Schaden beigetragen hat. Zumeist wird man sogar das Fehlverhalten des einzelnen IoT-Nutzer wegdenken können, ohne dass das Schadensereignis im Ganzen entfallen würde.

3 Zusammenfassung und Lösungsansätze

Die Betrachtungen haben folgendes ergeben:

- IoT-Geräte weisen im Höchstmaß IT-Sicherheitsschwächen auf (Kein Internet of Things sondern Internet of Shit[24]).
- Risiken können sich aus der mangelhaften/ veralteten Software des Gerätes, der Implementierung und dem Netz ergeben, in welchem das Gerät betrieben wird.
- Flächendeckende und kostengünstige Lösungen sind im Markt nicht verbreitet. IoT-Nutzer müssen einen hohen Aufwand betreiben, um Risiken selbst zu erkennen und Lösungen zu entwickeln.
- Die Haftung für unsichere IoT-Geräte ist nur unzureichend geregelt.
- Eine Haftung von Hersteller und Verkäufer scheidet, insbesondere bei nicht funktionsbeeinträchtigenden Sicherheitsmängeln aus.
- Eine gesetzliche Haftung von privaten Anwendern scheidet zumeist aus, da die Intransparenz und Komplexität der Anwendungen diese überfordert.
- Eine gesetzliche Haftung von Unternehmern und anderen Fachanwendern kommt hingegen in Betracht, führt aber nicht zum Ersatz von Vermögensschäden. Einen konkreten Pflichtenkatalog beim Betrieb von IoT-Geräten gibt es nicht. Es besteht große Rechtsunsicherheit, die zu Wettbewerbsverzerrungen führen kann, indem ein erhebliches Investitionsgefälle zwischen Unternehmen entsteht.

Der Gesetzgeber ist bisher nicht tätig geworden, um die vorgenannten Probleme zu lösen. Die Regelungen des IT-Sicherheitsgesetzes (KRITIS und § 13 Abs. 7 TMG) greifen zu kurz. Manch andere Lösungen sind ein zweischneidiges Schwert: Mit der Verabschiedung des NIS Umsetzungsgesetzes vom 27. April 2017 wurde das Telekommunikationsgesetz in § 109a dahingehend erweitert, dass Telekommunikationsdienstleister wie bspw. Internetprovider bei einer Störung (z.B. durch ein mit Schadsoftware infiziertes Gerät) den Datenverkehr umleiten oder einschränken.

Um die IT-Sicherheit bei IoT-Geräten in der Breite zu verbessern gibt es nicht den einen goldenen Weg. Vielmehr sollten Stellschrauben auf mehreren Ebenen bewegt werden. Obwohl der Gesetzgeber erst vor kurzem mit dem IT-Sicherheitsgesetz einen Vorstoß gewagt hat, bleibt der Bereich praktisch ungeregelt. Wesentliche Vorgaben kommen aus dem engen Anwendungsbereich des Datenschutzrechts und schützen dabei nicht Dritte im Netz. Der Gesetzgeber ist angehalten, weiter zu konkretisieren, welche Verkehrssicherungspflichten beim Betrieb von IT, insbesondere bei IoT-Geräten bestehen (z.B. Schaffung eines weiteren Adressatenkreises über die Betreiber Kritischer Infrastrukturen hinaus – „Betreiber von Infrastruktur zu geschäftlichen Zwecken", Schaffung von Haftungsnormen einschließlich Beweislastumkehr bei DDoS-Angriffen, Mindestanforderungen hinsichtlich Updates,[25] Recht auf Fernzugriff auf Geräte, Erweiterung des Sachmangelbegriffs). Auch wenn es für Juristen und ITler wünschens- und erstrebenswert ist, mit den bestehenden rechtlichen Regelungen auszukommen und nicht immer wieder eine Konkretisierung und Verschärfung des Gesetzes zu fordern, wird man nicht umhinkommen, eine Neufassung des IT-Sicherheitsgesetzes einzufordern. Adressaten sollten dann neben Unternehmen, die IoT-Systeme einsetzen, auch IoT-Hersteller sein. Der Gesetzgeber wird dabei, Mindeststandards festlegen müssen oder sollte dies zumindest durch Rechtsverordnung zu ermöglichen. Die Entwicklung und Umsetzung von einheitlichen Standards und Zertifikaten, würde für Kunden Produkte am Markt auch erst unterscheidbar machen und professionelle Lösungen begünstigen.

Eine solche Gesetzesverschärfung nimmt Unternehmen nicht nur in die Pflicht, sondern führt auch zu Investitionssicherheit und gleichen Rahmenbedingungen im Wettbewerb. Nebenbei holt es die IT-Sicherheit der IoT-Landschaft wieder zurück aus der Steinzeit.

24 https://twitter.com/internetofshit.

25 Nicht gefolgt werden kann dem teilweise diskutierten Ansatz, bei Verstößen eine Zwangsveröffentlichung des Quellcodes vorzusehen, da hierdurch offenbarte Schwachstellen wohl schwerer wiegen, als die Ressourcen der IT-Öffentlichkeit an einer Weiterentwicklung. Dafür scheint der IoT-Markt nicht homogen genug.