Editorial – Grußwort des Forschungsprojektleiters von »BayWiDI« Prof. Dr. Dirk Heckmann

Sehr geehrte Leserinnen und Leser,

herzlich willkommen zur elften Ausgabe des BayWiDI-Newsletters.

Diese Ausgabe steht ganz unter dem Stern eines Phänomens, welches sich seit einigen Jahren steigender Beliebtheit erfreut, dem Internet of Things, kurz IoT. Die Vorteile, die diese Technologie bietet, scheinen unerschöpflich. Allzu schnell gerät dabei jedoch in Vergessenheit, dass diese vernetzten Geräte nicht immer ausreichend stark gegen das Eindringen oder die Beeinflussung durch Dritte gesichert sind. Dieser Newsletter widmet sich daher insbesondere dem Thema der IT-Sicherheit von IoT-Geräten.

Im ersten Beitrag dieses Newsletters unter dem Titel „Internet of Things als ernsthafte Bedrohung?“, werden die Grundlagen des IoT beschrieben und eine definitorische Einordnung des Begriffs vorgenommen. Mit Blick auf die Frage nach der IT-Sicherheit von IoT-Geräten, werden die derzeit bekannten Lücken in der technischen Konzeption der Geräte beschrieben. Selten werden diese zwar vom Durchschnittsnutzer als Bedrohung empfunden, nichtsdestotrotz liegt hier ein Gefahrenpotenzial, wenn Angreifer sich aufgrund mangelnder Sicherheitsvorkehrungen bereits bei leichtem Aufwand Zugang zu den Geräten verschaffen können. Aufgrund der zunehmenden Verbreitung von IoT-Geräten, kann davon ausgegangen werden, dass der Handlungsbedarf hinsichtlich der IT-Sicherheit weiter zunehmen wird.

Zwei gesetzgeberische Handlungsansätze in diesem Kontext werden im Folgenden gegenübergestellt. Vor kurzem wurde in Kalifornien, USA, ein Gesetz erlassen, welches die IT-Sicherheit speziell bzgl. der IoT-Geräte regelt. Hersteller der Geräte werden in die Pflicht genommen, bestimmte Minimalstandards bzgl. der Sicherheit der technischen Konzeption einzuhalten. Einen anderen Ansatz verfolgt die Europäische Union. Ein derzeit diskutierter Gesetzesvorschlag sieht die Zertifizierung von IoT-Geräten als den richtigen Regulierungsansatz. Vorteil dieser Maßnahme wäre eine bessere Informiertheit von IoT-Nutzern sowie der Anreiz für Hersteller, den Sicherheitsstandard ihrer IoT-Geräte zum Erreichen der Zertifizierungen zu erhöhen. Der Beitrag „Ansätze für eine staatliche Regulierung der Sicherheit von IoT-Geräten – Eine Gegenüberstellung“ stellt beide Ansätze vor und unternimmt einen ersten Bewertungsversuch.

14. Internationales For..Net Symposium „Digitale Bildung. Digitale Haltung“

Auch im 21. Jahrhundert soll Bildung Menschen befähigen, sich als selbstbestimmte Persönlichkeiten in einer sich stetig wandelnden Gesellschaft zurechtzufinden und verantwortungsvoll ihre Lebensentwürfe zu verwirklichen. Doch stellen sich im Zuge des digitalen Wandels Fragen: Was ist Wissen noch wert, wenn es jederzeit abrufbar ist? Welche Fähigkeiten gilt es in einer digitalen Welt zu entwickeln? Bemerkenswert ist, dass Vorreiter bei der Digitalisierung – wie Finnland und Estland – in Bildungsrankings oft Spitzenplätze einnehmen. Digitale Kompetenz ist also von entscheidender Bedeutung: zum einen für den einzelnen Menschen, um in einer digitalen Welt selbstbestimmt und verantwortungsvoll leben zu können und um gute Chancen auf dem Arbeitsmarkt zu haben; zum anderen für die Gesellschaft, um Demokratie und Wohlstand auch in Zukunft zu erhalten. All dies setzt voraus, dass Menschen befähigt werden, komplexe, vernetzte und automatisierte Technologien, das Internet der Dinge oder die Mensch-Maschine-Interaktion unter den Bedingungen maschinellen Lernens zu begreifen sowie sicher und verantwortungsbewusst einzusetzen. Angesichts dessen ist die im Digitalpakt Schule vorgesehene Verbesserung der digitalen Infrastruktur an Schulen zu Recht das zentrale bildungspolitische Projekt der Bundesregierung. Das 14. Internationale For..Net Symposium am 25. und 26. April 2019 widmet sich den hiermit verbundenen Fragen unter dem Generalthema „Digitale Bildung. Digitale Haltung“ und knüpft dabei an die Erkenntnisse der Datenethikkommission und der Enquete Kommission Künstliche Intelligenz des Deutschen Bundestages an. Schirmherrin des Symposiums ist wieder die Staatsministerin für Digitalisierung im Bundeskanzleramt, Dorothee Bär.

Nun wünsche ich Ihnen eine interessante Lektüre. Genießen Sie die kommenden Weihnachtstage und kommen Sie gut ins neue Jahr!

Ihr Prof. Dr. Dirk Heckmann,
Leiter des Forschungsprojekts »BayWiDI«

Inhalt

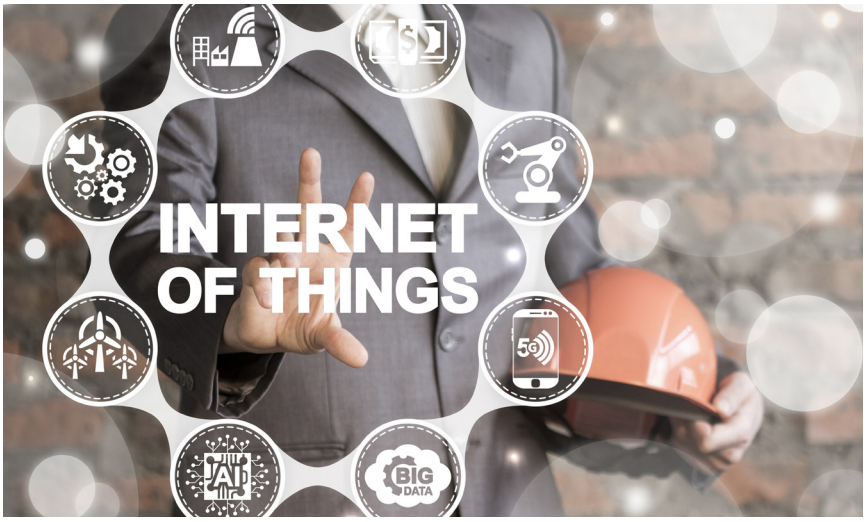
Internet of Things als ernsthafte Bedrohung?

Die Nutzung des Internet of Things (IoT) im industriellen und privaten Sektor nimmt seit Jahren stetig zu. Bereits im Jahr 2020 werden laut Experten über 30 Milliarden Geräte weltweit vernetzt sein.[1] Dies schafft für Privatanwender und Unternehmen große Chancen. Nicht nur im privaten Bereich bietet IoT diverse Annehmlichkeiten, sondern es erleichtert auch in vielfältiger Weise die Unternehmensführung.

Allerdings verkennen die meisten Anwender die von dieser Entwicklung ausgehenden Gefahren und nicht zu unterschätzenden Risiken. Im Folgenden soll daher ein Überblick über die Entwicklungen im Internet of Things gegeben werden, mit einem wesentlichen Schwerpunkt auf die Risiken bei dessen Anwendung im privaten und industriellen Sektor.

Vernetzte Geräte

Unter dem Internet of Things („Internet der Dinge" oder auch „Allesnetz") versteht man die Vernetzung von Gegenständen mit dem Internet in einer Weise, dass diese Gegenstände über das Internet selbstständig kommunizieren und einen Material- oder Produktionsfluss festlegen. Die Verbindung der am Produktionsfluss beteiligten Systeme mit softwaretechnischen Komponenten nennt man „cyber-physische Systeme".[2] Im privaten Bereich gibt es bereits jetzt diverse Anwendungsformen, zumeist ist sich der User nicht einmal bewusst, welche Vernetzungen sich hinter teils einfach anmutenden Geräten verborgen halten. Von Sprachassistenten wie Alexa, per App gesteuerten Waschmaschinen, smarten Heizungen[3], Parkraumüberwachung über Paketverfolgung bis hin zu kurios anmutenden Errungenschaften wie intelligenten Mülleimern, die den Füllstand anzeigen[4] oder gar appgesteuerten Vibratoren mit Videofunktion[5] sind nahezu alle Lebensbereiche mittlerweile vom Internet of Things umfasst.



Auch Unternehmen setzen zunehmend auf diese Technologie, um Produktions- und Unternehmensabläufe zu optimieren. Dies umfasst unter anderem die Möglichkeit von Datenanalysen in Echtzeit, das frühzeitige Erkennen und Beheben von Fehlern, sowie eine, über Unternehmensgrenzen hinausreichende, Automatisierung von Produktionsprozessen.[6]

Eklatante Sicherheitslücken

Als Sicherheitslücke wird eine Fehlfunktion in einem Betriebssystem oder Anwendungsprogramm definiert, durch die ein potentieller Angreifer Daten von einem Personalcomputer, Server oder Netzwerkgerät stehlen oder das Gerät unter seine Kontrolle bringen kann. Teilweise wird die Hardware missbraucht, wenn ein Standardservicepasswort festgelegt und nicht geändert wurde oder eine andere Hintertür zu Servicezwecken eingebaut wurde. Softwarelücken sind entweder auf klare Fehler des Programmierers zurückzuführen oder entstehen durch eine unübliche Nutzung der Software, die der Programmierer nicht vorhersehen konnte. Auch durch Add-Ons bei Internet-Browsern werden solche Sicherheitslücken geschaffen, da die zusätzlichen Funktionen auf Ressourcen des Hostcomputers zugreifen können.[7]

Bei der raschen technischen Entwicklung und der immer größer werdenden Palette an Anwendungsmöglichkeiten achten die Anwender sowohl privat

1 *Franke*, heise, https://www.heise.de/newsticker/meldung/Sicherheit-Internet-of-Things-wird-Angriffsziel-Nummer-Eins-4106314.html?view=print, abgerufen am 14.11.2018; https://www.consilium.europa.eu/de/policies/cyber-security/, abgerufen am 15.11.2018.

2 *Steinhoff*, Wissenschaftliche Dienste Deutscher Bundestag, https://www.dieter-stier.de/cms/wp-content/uploads/2013/06/industrie-4-0-data.pdf, abgerufen am 14.11.2018.

3 *Klaus*, IT-Service.Network, https://it-service.network/blog/2018/11/04/das-internet-der-dinge-sicherheit/, abgerufen am 14.11.2018.

4 *Briegleb*, heise, https://www.heise.de/newsticker/meldung/Vodafone-Schmalbandnetz-fuer-das-Internet-der-Dinge-steht-4190141.html, abgerufen am 14.11.2018.

5 *Scherschel*, heise, https://www.heise.de/newsticker/meldung/Svakom-Siime-Eye-Vernetzter-Kamera-Vibrator-ist-ein-Sicherheitsalptraum-3674827.html, abgerufen am 14.11.2018.

6 *Diedrich*, iX Magazin, https://www.heise.de/ix/meldung/IBM-warnt-vor-dem-Internet-of-Threats-3992680.html, abgerufen am 14.11.2018.

7 Heise, https://www.heise.de/thema/Sicherheitslücken#liste, abgerufen am 15.11.2018.

als auch bei der industriellen Verwendung des Internet of Things kaum auf die Sicherheit der Geräte, die sich etwa in Form von Zertifizierungen und Updatemöglichkeiten zum Schließen von Sicherheitslücken weitgehend herstellen ließe.[8]

Wesentliche Sicherheitslücken

- Standardservicepasswörter
- Programmierfehler
- Unvorhergesehene Nutzung der Software
- Add-Ons in Internet-Browsern

Für die Hersteller ist es nach den bisherigen Entwicklungen stets von oberster Priorität gewesen, eine möglichst große Gewinnmarge zu erhalten.[9] Dies geht meist auf Kosten der Sicherheit der Produkte und etwaiger Updatemöglichkeiten. Das ist auch auf den Endverbraucher zurückzuführen, der sich nur selten um eine ausreichende Zertifizierung seines Produktes bemüht; ihm geht es zumeist darum, bei vergleichbaren Produkten das möglichst günstigste zu erwerben. Daher sparen die meisten Hersteller zuerst an Updatemöglichkeiten und einer ausreichenden Zertifizierung, um die Preise gegenüber anderen vergleichbaren Produkten niedrig zu halten.[10]

Hohes Gefahrenpotential

In den Hintergrund rücken dabei allzu oft die Risiken der digitalen Vernetzung. Diese bleiben von den meisten Usern unbeachtet, bis sie sich realisiert haben. Von Persönlichkeitsverletzungen durch Spionage im privaten Bereich über Webcams bis hin zum „Gläsernen Bürger“[11]

können wirtschaftlich gravierende Folgen für Unternehmen, Industriezweige oder sogar ganze Staaten drohen.

Dramatische Auswirkungen kann ein Angriff über das Internet bei Industrie und Versorgungsunternehmen haben. 30 Prozent der Cyberattacken zielen auf Betriebstechnik ab, im Nahen Osten richten sich 50 Prozent der Angriffe gegen die Öl- und Gasindustrie. Daraus ergeben sich fatale Konsequenzen; von Betriebsspionage über Produktionsausfälle bis hin zu Umweltkatastrophen und Todesfällen.[12]

Die wenigsten Unternehmen haben dabei technische Vorkehrungen zur Absicherung ihrer IoT-Netzwerke getroffen, lediglich 21 Prozent der Unternehmen verschlüsseln den IoT-Datenverkehr; über ein zentralisiertes Patch-System verfügen gerade einmal 15 Prozent der Unternehmen; ebenso authentifizieren gerade einmal 15 Prozent ihre IoT-Geräte. Angriffe simulieren sogar nur 14 Prozent der Unternehmen und lediglich 10 Prozent überwachen den IoT-Netzwerkverkehr, um Anomalien zu entdecken. 45 Prozent der Unternehmen gleichen dies durch Versicherungen aus, die vermeintliche Sicherheit nach einem Sicherheitsvorfall versprechen oder zumindest den finanziellen Schaden beschränken.[13] Insbesondere drohen beim Einsatz vernetzter Geräte Denial of Service (DoS)- und Distributed Denial of Service (DDos)-Attacken über Botnetze. Bei DoS-Angriffen werden Infrastrukturelemente durch Überlastung lahmgelegt. Dies geschieht meist durch eine Attacke auf den Server, einen Rechner oder sonstige Teile des Datennetzwerks. Bei einem DDoS-Angriff wird der Angriff nicht von einem einzelnen Rechner aus durchgeführt, sondern gleichzeitig im Verbund mit mehreren Rechnern. Dadurch wird ein Vielfaches an Datenverkehr erzeugt und es ist schwieriger den Ursprung eines Angriffs auszumachen.[14]

Schneck, Ass. Jur.

8 *Diedrich*, iX Magazin, https://www.heise.de/ix/meldung/IBM-warnt-vor-dem-Internet-of-Threats-3992680.html, abgerufen am 14.11.2018.

9 *Klaus*, IT-Service.Network, https://it-service.network/blog/2018/11/04/das-internet-der-dinge-sicherheit/, abgerufen am 15.11.2018.

10 *Ross*, heise, https://www.heise.de/newsticker/meldung/Kommentar-zur-IoT-Sicherheit-Europas-Verordnung-ist-zahnlos-4208938.html?view=print; abgerufen am 14.11.2018.

11 *Franke*, heise, https://www.heise.de/newsticker/meldung/Sicherheit-Internet-of-Things-wird-Angriffsziel-Nummer-Eins-4106314.html?view=print, abgerufen am 15.11.2018.

12 *Diedrich*, heise, https://www.heise.de/ix/meldung/IBM-warnt-vor-dem-Internet-of-Threats-3992680.html, abgerufen am 15.11.2018.

13 *Diedrich*, heise, https://www.heise.de/ix/meldung/IBM-warnt-vor-dem-Internet-of-Threats-3992680.html, abgerufen am 15.11.2018.

14 *Vistola*, Computerwoche, https://www.computerwoche.de/a/so-funktionieren-ddos-angriffe,3329263, abgerufen am 06.12.2018.

Ansätze einer staatlichen Regulierung zur Verbesserung der Sicherheit von IoT-Geräten – Eine Gegenüberstellung

Wie im vorigen Beitrag bereits dargestellt, scheitert die Sicherheit von IoT-Geräten oft am mangelnden Interesse der Nutzer, bzw. einer mangelnden Kenntnis, dessen, welche Daten diese Geräte überhaupt erheben und verarbeiten. Ein rechtlicher Rahmen könnte daher für einen besseren Sicherheitsstandard sorgen. Wie aber sähe dieser Rechtsrahmen aus, um am wirkungsvollsten die IT-Sicherheit von IoT-Geräten zu gewährleisten? Zwei unterschiedliche Ansätze sollen hier dargestellt und diskutiert werden: Auf Ebene der Europäischen Union wird derzeit die Idee einer regulierten Zertifizierung von IoT-Geräten diskutiert.[1] In Kalifornien wurde kürzlich bereits ein Gesetz zur Regelung von IoT-Geräten verabschiedet, welches einen Mindeststandard an Sicherheitsmaßnahmen seitens der Hersteller fordert.

EU-Verordnung zur „Zertifizierung der Cybersicherheit"

Der Europarat hat kürzlich einen EU-Verordnungsentwurf zur „Zertifizierung" der Cybersicherheit" erlassen, welches das Europäische Parlament passieren müsste, um rechtlich verbindlich zu werden. Die Verhandlungen hierzu zwischen dem Europäischem Rat und dem Europäischem Parlament wurden am 13. September 2018 aufgenommen.[2] Geplant ist, die Verordnung bis Ende 2018 verbindlich werden zu lassen.[3]

Die Verordnung ist bereits vor In-Kraft-treten massiv in die Kritik geraten. Die Zertifizierung ist danach nur für Produkte verpflichtend, die innerhalb „kritischer Infrastrukturen" eingesetzt werden. Bei anderen IoT-Produkten wird auf Freiwilligkeit seitens der Hersteller gesetzt. Dabei können diese zwischen „niedriger, mittlerer und hoher" Zertifizierungsstufe wählen. Dies soll die Abwehrfähigkeit der Produkte bei Angriffen für den Verbraucher greifbar machen, in Form einer „Konformitätsbewertung".[4]

Die EU-Verantwortlichen erhoffen sich über die Freiwilligkeit eine große Beteiligung der Hersteller an der Zertifizierung. Jedoch wird dabei verkannt, dass dies ja bereits zur verheerenden aktuellen Sicherheitssituation geführt hat. So lange die Nutzer zum Teil wenig auf die Sicherheit bedacht sind, sondern lediglich stets das günstigste Produkt erwerben wollen, werden die Hersteller weiterhin an der Zertifizierung Kosten sparen. Außerdem sollte bedacht werden, dass auch viele Geräte außerhalb der EU hergestellt werden, was sicherheitstechnisch vom Nutzer hinterfragt werden sollte.

Ein weiteres ungelöstes Problem wird darin liegen, dass die EU-Zertifizierung immer auf dem aktuellen Stand der Technik erfolgen muss, was bei dem sich rasant entwickelnden Markt im IoT-Bereich kaum realisierbar sein wird. Die Möglichkeit zur Zertifizierung ist immer nur vorab auf dem technischen Standard bei der Produkteinführung gegeben und kann etwaige Veränderungen von Umwelt und Technik nicht vorhersehen. Für Unternehmen gilt es deshalb ein besonderes Augenmerk darauf zu haben, ihre IoT-Umgebung im Rahmen von beschleunigten Zertifizierungsverfahren so sicher wie möglich auszugestalten. Neben einer höheren Produktqualität kann dadurch auch eine wesentliche Verbesserung der IT-Sicherheit erreicht werden. Die Einführung eines europäischen Zertifizierungsstandards darf allerdings nicht dazu führen, dass Unternehmen mit bereits hohen Sicherheitsstandards auf den Minimalstandard zurückfallen.[5] Ob der EU-Gesetzgeber die Situation noch einmal überdenken wird und strengere, verpflichtende und vor allem wirksamere Regelungen in Betracht zieht, bleibt abzuwarten.

Kalifornischer Vorstoß im Bereich der gesetzlichen Regelung zur IoT-Sicherheit

Kalifornien hat als erster[6] US-Amerikanischer Bundesstaat ein Gesetz[7] erlassen, das die Sicherheit von IoT-Geräten regulieren soll. Mit Wirkung zum 1. Januar 2020 wird es Herstellern künftig auferlegt, einen gewissen Sicherheitsstandard für IoT-Geräte einzuhalten. Dem Gesetz wird eine hohe Bedeutung für die Rechtsentwicklung im IoT-Bereich zumindest für die USA zugesprochen.[8] Aufgrund der Aufmerksamkeit, die das Gesetz bereits auch in deutschen Fachmedien[9] er-

1 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die „EU-Cybersicherheitsagentur" (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit") COM/2017/0477 final/2 - 2017/0225 (COD), https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A52017PC0477R%2801%29, abgerufen am 14.11.2018.

2 https://www.consilium.europa.eu/de/policies/cyber-security/, abgerufen am 15.11.2018.

3 *Klaus*, IT-Service.Network, https://it-service.network/blog/2018/11/04/das-internet-der-dinge-sicherheit/, abgerufen am 15.11.2018.

4 *Klaus*, IT-Service.Network, https://it-service.network/blog/2018/11/04/das-internet-der-dinge-sicherheit/, abgerufen am 15.11.2018.

5 *Ritter*, bitkom, https://www.bitkom.org/sites/default/files/file/import/2017-12-20Stellungnahme-Cybersecurity-Act.pdf, abgerufen am 07.12.2018.

6 *Spies*, ZD-Aktuell 2018, 06313.

7 Senate Bill 327, Chapter 886.

8 *Hawkins*, Washington Post, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/09/17/the-cybersecurity-202-california-s-internet-of-things-cybersecurity-bill-could-lay-groundwork-for-federal-action/5b9e6e331b326b47ec959638/?noredirect=on&utm_term=.5a4e93af9275, zuletzt abgerufen am 06.12.2018.

9 Vgl. etwa *Böck*, Golem, https://www.

langt hat, ist auch eine Beeinflussung des deutschen und/oder europäischen Rechtsraums nicht auszuschließen.

1. Inhalt des Gesetzes

Das am 29. September 2018 von Gouverneur Jerry Brown unterzeichnete Gesetz regelt zwar keine spezifischen Schritte, welche Hersteller künftig unternehmen müssen. Es wird jedoch klargestellt, dass erfasste Geräte künftig einen angemessenen Sicherheitsstandard hinsichtlich des Schutzes von persönlichen Informationen bieten müssen.[10]

a. Hersteller

Hersteller definiert das Gesetz als diejenigen, die die erfassten Geräte herstellen oder mit Dritten die Herstellung in Auftragsarbeit vereinbaren. Bezogen auf den Anwendungsbereich des Gesetzes setzt dieses allerdings zusätzlich voraus, dass die Geräte in Kalifornien verkauft werden oder zum Verkauf angeboten werden.

b. Erfasste Geräte

Das Gesetz erwähnt IoT-Geräte nicht unter dieser Bezeichnung, sondern spricht stattdessen von verbundenen Geräten. Damit soll jedes Gerät umfasst sein, welches die Eigenschaft hat, sich mit dem Internet direkt oder indirekt verbinden zu können und dem darüber hinaus entweder eine IP- oder Bluetooth-Adresse zugeordnet ist. Darunter können sowohl moderne Fernseher, Telefone, Spielzeuge sowie Haushaltsgeräte fallen.[11]

c. Maßnahmen und Verpflichtungen

Die einzurichtenden Maßnahmen werden dahingehend konkretisiert, dass die Geräte mit Sicherheitsfunktionen versehen werden, welche für die jeweilige Funktion und die von dem Gerät verarbeiteten Daten angemessen sind.[12] Aufgrund des unbestimmten Begriffs der Angemessenheit wird dem Rechtsanwender hier ein recht weiter Interpretationsspielraum gelassen. Allerdings wird ausdrücklich darauf hingewiesen, dass das Design der Sicherungsmaßnahmen das Gerät und die hierin gespeicherten Informationen sowohl vor unautorisierten Zugriffen als auch vor der unbefugten Zerstörung oder Benutzung und Modifikation schützen muss.

Unter anderem verbietet das kalifornische Gesetz, dass IoT-Hersteller ihre Geräte mit simplen Standard-Passwörtern ausstatten.[13] Anlass zu dieser Regelung mag das sog. Mirai-Botnetz gewesen sein, welches aus massenhaft gehackten IoT-Geräten bestand, die nur mit Standardpasswörtern gesichert waren.[14] Dieses Botnetz wurde 2016 zu zahlreichen Denial-of-Service-Attacken eingesetzt.[15] Die neuen Vorschriften geben daher vor, dass bereits die voreingestellten Standard-Passwörter individuell und sicher sein müssen. Alternativ sind Nutzer dazu zu zwingen, vor der ersten Anwendung des Geräts ein individuelles Passwort festzulegen. Dies gilt für all diejenige IoT-Geräte, welche auch außerhalb eines lokalen Netzwerks erreichbar sind. Auch dies kann den Router bis hin zur smarten Glühbirne betreffen.[16]

Standardpasswörter zukünftig zu untersagen, soll bewirken, dass sich Angreifer nicht mehr durch einfaches Erraten der Passwörter Zugriff auf die Geräte verschaffen können.[17] Denn auch wenn bei standardisierten Passwörtern den Nutzern die Möglichkeit eingeräumt wird das Passwort zu ändern, so tun dies viele oft nicht.[18] Der Aufwand, die Geräte zur Einbindung in sog. Bot-Netze zu kapern, wird somit durch die neue Gesetzeslage in Kalifornien wohl deutlich erhöht werden.

d. Durchsetzung

Die Durchsetzung des kalifornischen Gesetzes, wenn auch insbesondere die Daten Privater geschützt werden sollen, wird ausschließlich von staatlicher Seite aus stattfinden. Ein privates Klagerecht wurde nicht geschaffen. Stattdessen soll die kalifornische Staatsanwaltschaft die ausschließliche Befugnis erhalten, für die Durchsetzung der Bestimmungen zu sorgen.[19] Ob sich das Ausbleiben privater Durchsetzungsmöglichkeiten als sinnvoll erweisen wird, bleibt abzuwarten.

2. Kritik

Ob das Gesetz eine Besserung der IT-Sicherheit von IoT-Geräten schafft, ist unter Experten umstritten.[20] Unter anderem wird angemerkt, dass die geregelten Inhalte nicht weit genug gehen, und der starke Fokus auf die Passwortsicherung das Problem nicht richtig greift, da die IoT-Geräte mit unterschiedlichen

golem.de/news/iot-sicherheitsluecken-kalifornien-verbietet-standard-passwoerter-1810-136988.html, zuletzt abgerufen am 06.12.2018; *Sokolov*, heise, https://www.heise.de/newsticker/meldung/Kalifornien-verlangt-einzigartige-Passwoerter-fuer-vernetzte-Geraete-4182625.html, zuletzt abgerufen am 06.12.2018.

10 *Miller*, Legaltechnews, https://www.law.com/legaltechnews/2018/10/01/hey-alexa-californias-new-iot-law-requires-data-protections-397-12036/?slreturn=20181106043246, zuletzt abgerufen am 06.12.2018.

11 *Kovacs*, SecurityWeek, https://www.securityweek.com/california-iot-cybersecurity-bill-signed-law, zuletzt abgerufen am 06.12.2018.

12 *Böck*, Golem, https://www.golem.de/news/iot-sicherheitsluecken-kalifornien-verbietet-standard-passwoerter-1810-136988.html, zuletzt abgerufen am 06.12.2018.

13 *Köver*, heise, https://netzpolitik.org/2018/internet-der-dinge-kalifornien-verbietet-standardpasswoerter-ein-modell-fuer-deutschland/, zuletzt abgerufen am 05.12.2018.

14 Vgl. etwa *Böck*, Golem, https://www.golem.de/news/iot-sicherheitsluecken-kalifornien-verbietet-standard-passwoerter-1810-136988.html, zuletzt abgerufen am 06.12.2018.

15 *Kühl*, Zeit, https://www.zeit.de/digital/internet/2017-12/ddos-attacke-mirai-botnet-minecraft, zuletzt abgerufen am 06.12.2018; vgl. hierzu auch vorigen Newsletter Beitrag.

16 *Köver*, Netzpolitik.org, https://netzpolitik.org/2018/internet-der-dinge-kalifornien-verbietet-standardpasswoerter-ein-modell-fuer-deutschland/, zuletzt abgerufen am 06.12.2018.

17 *Köver*, heise, https://netzpolitik.org/2018/internet-der-dinge-kalifornien-verbietet-standardpasswoerter-ein-modell-fuer-deutschland/, zuletzt abgerufen am 05.12.2018.

18 *Böck*, Golem, https://www.golem.de/news/iot-sicherheitsluecken-kalifornien-verbietet-standard-passwoerter-1810-136988.html, zuletzt abgerufen am 06.12.2018.

19 Vgl. auch *Spies*, ZD-Aktuell 2018, 06313.

20 *Köver*, Netzpolitik.org, https://netzpolitik.org/2018/internet-der-dinge-kalifornien-verbietet-standardpasswoerter-ein-modell-fuer-deutschland/, zuletzt abgerufen am 05.12.2018.

Authentifizierungsebenen und -schnittstellen funktionieren.[21] Die Regelung sei daher auf ein typischerweise nur oberflächliches Verständnis von Cybersecurity und Hacking zurückzuführen.[22]

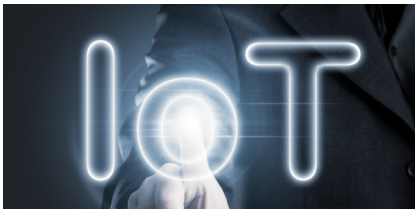
Auch wird bemängelt, dass die Regelungen zu unbestimmt gefasst sind und damit an Effektivität und Wirkung einbüßen. Stattdessen würden die Regelungen nur unnötige Kosten verursachen und Innovation hemmen.[23]

3. Denkbares Konzept auch in Deutschland?

Frank Rieger, Sprecher des Chaos Computer Club (CCC) ist der Auffassung, dass es ein erster richtiger Schritt wäre, auch in Deutschland Minimalstandards für die IT-Sicherheit festzulegen. Verwunderlich sei allerdings, dass Selbstverständlichkeiten wie die sichere Passwortregelung gesetzlich vorgegeben werden müssen.[24] Auch das Bundesministerium für Justiz und Verbraucherschutz (BMJV) scheint die Einführung von Regelungen für vernetzte Geräte entweder auf nationaler oder europäischer Ebene zu begrüßen. Allerdings ist ebenso die Variante wie sie in Form eines „Cybersecurity Acts“[25] derzeit diskutiert wird, denkbar.

Zusammenfassung

Das kalifornische Gesetz zur Regelung der IT-Sicherheit von IoT-Geräten trägt einen ersten Ansatz, den Sicherheitslücken im Bereich der IoT-Geräte Einhalt zu gebieten. Anders als der europäische Ansatz, welche Hersteller zu einer freiwilligen Verbesserung ihrer Standards führen will, erwartet das kalifornische Gesetz einen angemessenen Mindeststandard und macht diesen verpflichtend. Auch in Deutschland wäre ein solcher Ansatz denkbar. Einigkeit dürfte allerdings dahingehend herrschen, dass der Gesetzgeber gehalten ist, sich um einen verbesserten Schutz persönlicher Daten bereits im Rahmen der Herstellung datenverarbeitender IoT-Geräte zu bemühen. Bei entsprechender Umsetzung der geplanten EU-Verordnung könnte man allerdings den Vorteil darin sehen, dass eine gewisse Freiwilligkeit im Gegensatz zum kalifornischen verpflichtenden Modell auch eine höhere Sicherheitsstufe zur Folge haben kann. Während bei verpflichtenden Vorgaben zumeist nur der Mindeststandard eingehalten wird, ist beim europäischen Lösungsansatz für die Hersteller die Möglichkeit gegeben entsprechend höhere Sicherheitsstandards einzusetzen und somit durch eine über dem Minimum liegende Zertifizierung die Endkunden zu überzeugen.



Schneck, Ass. Jur./Zerbst, L.L.M. (VUW)

Designed by Tobias Springer und Florian Jurina

21 *Hawkins*, Washington Post, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/09/17/the-cybersecurity-202-california-s-internet-of-things-cybersecurity-bill-could-lay-groundwork-for-federal-action/5b9e6e331b326b47ec959638/?noredirect=on&utm_term=.812039cfeb99, zuletzt abgerufen am 05.12.2018; Errata Security, https://blog.erratasec.com/2018/09/californias-bad-iot-law.html#.XAgH1WhKiUm, zuletzt abgerufen am 05.12.2018.

22 Errata Security, https://blog.erratasec.com/2018/09/californias-bad-iot-law.html#.XAgH1WhKiUm, zuletzt abgerufen am 06.12.2018.

23 *Hawkins*, Washington Post, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/09/17/the-cybersecurity-202-california-s-internet-of-things-cybersecurity-bill-could-lay-groundwork-for-federal-action/5b9e6e331b326b47ec959638/?noredirect=on&utm_term=.5a4e93af9275, zuletzt abgerufen am 06.12.2018.

24 *Köver*, Netzpolitik.org, https://netzpolitik.org/2018/internet-der-dinge-kalifornien-verbietet-standardpasswoerter-ein-modell-fuer-deutschland/, zuletzt abgerufen am 05.12.2018.

25 Rat der Europäischen Union, https://www.consilium.europa.eu/de/policies/cyber-security/, zuletzt abgerufen am 06.12.2018.

Der nächste Newsletter erscheint am 15. März 2019. Sie finden den Newsletter und die Möglichkeit, sich an- und abzumelden, unter www.baywidi.de

Hinweise, Anregungen, Lob und Kritik sind herzlich willkommen. Schreiben Sie uns einfach unter baywidi@uni-passau.de

Impressum

Universität Passau
Innstraße 41
94032 Passau
Telefon: 0851/509-0
Telefax: 0851/509-1005
E-Mail: praesidentin@uni-passau.de
Internet: www.uni-passau.de
USt-Id-Nr.: DE 811193057

Organisation

Gemäß Art. 11 Abs. 1 BayHSchG ist die Universität Passau als Hochschule des Freistaates Bayern eine Körperschaft des öffentlichen Rechts und zugleich staatliche Einrichtung. Aufsichtsbehörde ist das Bayerische Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst in München (Anschrift: Salvatorstraße 2, 80333 München).

Vertretung

Die Universität Passau wird von der Vorsitzenden des Leitungsgremiums, Präsidentin Prof. Dr. Carola Jungwirth, gesetzlich vertreten. Verantwortliche im Sinne des § 5 TMG (Telemediengesetz) ist die Präsidentin. Für namentlich oder mit einem gesonderten Impressum gekennzeichnete Beiträge liegt die Verantwortung bei den jeweiligen Autorinnen und Autoren.