Bern, 29. April 2020

Sicherheitsstandards für Internet-of-Things-Geräte (IoT)

Bericht des Bundesrates in Erfüllung der Postulate 17.4295 Glättli vom 15.12.2017 und 19.3199 Reynard vom 21.03.2019

Inhaltsverzeichnis

1 Einleitung

Das Internet der Dinge (engl.: Internet of Things, IoT) ist omnipräsent und betrifft alle Bereiche der Gesellschaft. Über IoT werden industrielle Prozesse über Firmengrenzen hinweg vernetzt. Genauso gehört es heute zum Standard, dass die verschiedensten Arten von Konsumgütern über Sensoren vernetzt und gesteuert sind: von der Einparkhilfe bei den Autos über die Drucksensoren in Zahnbürsten bis hin zum Mikrofon/Kamera bei Spielzeug für Kinder.
Das IoT birgt ein riesiges Potential, da es viele Prozesse vereinfachen und effizienter machen kann, es bringt aber auch Risiken mit sich. Wie bei vielen neuen Anwendungen stehen für die Hersteller bei der Entwicklung der Geräte nicht die Sicherheitsaspekte, sondern der Nutzen und die Kosten im Vordergrund. So erstaunt es nicht, dass sich Medienberichte zu Sicherheitsproblemen bei IoT-Anwendungen häufen und zunehmend Angriffe beobachtet werden können, bei welchen Schwachstellen bei IoT gezielt ausnutzen.
Der vorliegende Bericht beleuchtet die Sicherheit von IoT-Geräten und soll aufzeigen, wie diese besser gegen Cyberangriffe geschützt werden können. Er erklärt deshalb die besonderen Herausforderungen und Risiken von Systemen mit IoT-Komponenten, betrachtet die bekanntesten Cyberattacken im Zusammenhang mit IoT, zeigt den Stand der bereits existierenden Richtlinien zu IoT auf und beleuchtet die rechtlichen Grundlagen für den Umgang mit IoT.

1.1 Ausgangslage

Das IoT hat in den letzten Jahren stark an Bedeutung gewonnen und das Thema wird medial wie auch politisch immer mehr aufgegriffen. Es erweitert die bekannten Konzepte der digitalen Technologien von „jederzeit“ (anytime) und „an jedem Ort“ (anyplace) mit der Konnektivität von „allem“ (anything). Die IoT-Technologie verändert und verbreitet sich rasend schnell. Prognosen sagen für 2020 50 Milliarden mit dem Internet verbundene Dinge voraus. Weitere Vorhersagen gehen davon aus, dass zukünftig 200 Dinge pro Person verbunden sein werden.
Aufgrund der stetigen Verbindung zum Internet, steigt auch das Risiko für Cyberkriminalität. Die Szenarien reichen dabei von Datenmissbrauch oder Spionage über Sabotage bis hin zur illegitimen Nutzung der Rechenkapazitäten der Dinge. Der breiten Öffentlichkeit sind über die Medien inzwischen viele Cyberattacken bekannt. Die Sensibilität der Bevölkerung ist vor allem durch Vorfälle gestiegen, bei denen persönliche Daten zugänglich gemacht oder missbraucht worden sind. Besondere Beachtung verdient das Thema IoT im industriellen Umfeld. Während in einem Produktionsbetrieb bei einem Angriff beispielsweise die Produktion gestört oder unterbrochen werden kann, sind die Auswirkungen eines Angriffs bei Betreibern kritischer Infrastrukturen potentiell viel drastischer.

1.2 Auftrag

Angesichts dieser Entwicklungen muss auch für die Schweiz untersucht werden, welche Konsequenzen die Verbreitung von IoT für die Cybersicherheit hat und wie die Sicherheit von IoT-Geräten bestmöglich gewährleistet werden kann. Bundesrat und Parlament haben die Bedeutung von IoT für die Cybersicherheit erkannt und entsprechende Prüfaufträge formuliert:

- **17.4295 Po. Glättli «Sicherheitsstandards für Internet-of-Things-Geräte prüfen, weil diese eine der grössten Bedrohungen der Cybersicherheit sind»:** Der Bundesrat wird ersucht, in einem Kurzbericht aufzuzeigen, wie im rasant wachsenden Bereich der ans Internet angebundenen Geräte (Internet of Things, IoT) die Sicherheit dieser Geräte erhöht und ihr Missbrauch für Cyberkriminalität erschwert werden kann. Abzuklären und aufzuführen ist unter anderem:
  1. ein kurzer Überblick über grössere Internet-Attacken unter Verwendung von IoT-Geräten;
  2. der Stand internationaler Sicherheitsrichtlinien für IoT-Geräte (ähnlich den Zulassungsbestimmungen für elektrische Geräte) und deren Umsetzung in der Schweiz;
  3. die Einführung interner Richtlinien für den Bund und bundesnahe Betriebe mit Sicherheitsbedingungen zum Kauf und Einsatz von IoT-Geräten;
  4. die Einführung von Sicherheitsrichtlinien bei Betreibern kritischer Infrastruktur: zu erfüllende Sicherheitsbedingungen zum Kauf und Einsatz von IoT-Geräten;
  5. die Möglichkeit, durch Meldepflichten oder Anreize die Chance zu erhöhen, dass bekannte Sicherheitslücken von Geräten einer zentralen Stelle (z. B. Melani) gemeldet werden;
  6. die Möglichkeit, von den Herstellern zumindest während der Gewährleistungszeit (Garantiefrist) Sicherheitsupdates für bekanntgewordene Sicherheitslücken einzufordern.

  Der Bericht soll knapp und eingängig sein und ggf. sinnvolle Umsetzungen auf Verordnungs- oder Gesetzesstufe konkret ausführen. Dabei ist wo möglich die Unterstützung zur Schaffung internationaler Standards oder zu deren Übernahme einer schweizerischen Insellösung vorzuziehen.
- **19.3199 Po. Reynard «Verbesserung der Sicherheit von mit dem Internet verbundenen Produkten»:** Der Bundesrat wird beauftragt, einen Bericht darüber vorzulegen, wie die Sicherheit von auf dem Markt erhältlichen Produkten, die mit dem Internet verbunden sind, im Hinblick auf den Datenschutz verbessert werden kann.
- **Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS), Handlungsfeld «Standardisierung und Regulierung»:** Informations-und Kommunikationstechnologie **(**IKT)-Standardisierungen und -Regulierungen sind wichtige Instrumente zum Schutz vor Cyber-Risiken. Minimalanforderungen zu Schutzvorkehrungen stärken die Prävention und Vorgaben zum Umgang mit Vorfällen (z. B. Meldepflichten) tragen zu einer verbesserten Reaktion bei. Standardisierung und Regulierung sind auch im internationalen Umfeld wichtig, da sie mehr Transparenz und Vertrauen in der globalisierten digitalen Gesellschaft schaffen. Bei der Einführung von Standardisierungen und Regulierungen gilt es aber, die grossen Unterschiede zwischen den Wirtschaftssektoren und den Unternehmen verschiedener Grösse zu beachten. Zudem ist in jedem Fall das internationale Umfeld zu beachten. Standards und Regulierungen müssen im grenzüberschreitenden Cyber-Raum international möglichst kompatibel sein. Ebenfalls zu prüfen ist, ob und wie eine Meldepflicht für Cyber-Vorfälle eingeführt werden soll.

Der vorliegende Bericht fasst die bisherigen Arbeiten, welche im Rahmen dieser Aufträge unternommen worden sind, zusammen. Im Wesentlichen basiert er auf den Resultaten einer Auftragsstudie «Sicherheitsstandards im IoT» [1], in welcher die Bedeutung von IoT in der Cybersicherheit analysiert und damit Grundlagen zur Beantwortung der vielschichtigen Fragen liefert. Er verwendet auch die Trendanalyse des Center for Security Studies (CSS) der ETH Zürich zum Thema «The Challenges of Scaling the Internet of Things»[2], in welcher ebenfalls der aktuelle internationale Forschungsstand zum Thema reflektiert wird.

[1] Hochschule Luzern (HSLU), Sicherheitsstandards im IoT - Herausforderungen des IoT und Übersicht IT- und IoT-Richtlinien, Oktober 2019
[2] Center for Security Studies (CSS) der ETH Zürich, CYBER DEFENSE PROJECT, Trend Analysis: The Challenges of Scaling the Internet of Things, August 2019

2 Herausforderungen für die IoT-Sicherheit

Bei der Betrachtung der Sicherheit im IoT ist es sinnvoll zwischen Anwendungen des IoT für Endkunden und für die Industrie zu unterscheiden. Der Grund liegt vor allem darin, dass in den beiden Segmenten verschiedene Methoden angewendet werden, um die Sicherheit zu gewährleisten. Sind es bei Endkunden die Geräte selbst, welche eine bestimmte Sicherheit gewährleisten sollen, gilt es bei industriellen Anwendungen zusätzlich die Netzwerke entsprechend den Sicherheitsanforderungen zu segmentieren und sichern. In diesem Zusammenhang wird auch vom Industrial Internet of Things (IIoT) gesprochen.
Verglichen mit IT-Systemen (z. B. für administrative Aufgaben) gibt es für Systeme mit IoT-Komponenten besondere Herausforderungen für die Cybersicherheit. In diesem Kapitel wird zuerst verdeutlicht, welche Gefahren bei IoT-Geräten hinsichtlich der Informationssicherheit generell zu beachten sind. Im zweiten Abschnitt wird auf die spezifischen Herausforderungen und Gefahren bei industriellen IoT-Geräten eingegangen, da diese durch ihre Verbreitung bei kritischen Infrastrukturen von besonderer Bedeutung sind.

2.1 Generelle Herausforderungen: Fehlende Anreize für Sicherheit bei IoT

Kostendruck, Zeitdruck, mangelndes Bewusstsein und Verständnis darüber, wie Angreifer die Sicherheitslücken von IoT-Geräten nutzen, führen zu unterschiedlichen Schwachstellen sowie deren Ausnutzung. Nutzer von IoT-Geräten sind sich oft nicht bewusst, dass solche Geräte eine grosse Angriffsfläche bieten können. Auf der Seite der Hersteller haben viele Anbieter kein Interesse daran, Geräte mit Softwareupdates zu warten oder diese mit spezifischen Sicherheitsfunktionen auszustatten. Sie denken eher kurzfristig und wollen einfach eine möglichst grosse Anzahl an neuen IoT-Geräten verkaufen. Kommt hinzu, dass im Vergleich zur traditionellen IT in herkömmlich eingebetteten Systemen die Sicherheit keine grosse Rolle spielte. Die Geräte sind in Sachen Prozessor- und Storage-Kapazität vielfach limitiert, so dass gewisse Sicherheitsmerkmale schwierig anwendbar sind (z. B. fehlende starke Verschlüsselung wegen mangelnder Prozessorstärke).
Dies führt dazu, dass weder eine kommerziell interessante Nachfrage noch ein ausreichendes Angebot an sicheren IoT-Geräten besteht. Insbesondere bei Konsumgütern ist der Preisdruck sehr gross und das Sicherheitsbewusstsein beim Endkunden sehr klein. Generell ist nicht zu erwarten, dass ein ausreichend starker Marktdruck für die Verbesserung der Sicherheit bei IoT-Geräten entstehen wird.

2.2 Spezielle Herausforderungen und Gefahren im industriellen IoT

Industrielle Kontrollsysteme (engl. Industrial Control Systems, ICS), welche auch als IIoT bezeichnet werden, sind hoch integrierte Computersysteme, die auch in kritischen Infrastrukturen wie der Energieversorgung, dem Transportwesen oder bei der Wasseraufbereitung zur Prozesssteuerung eingesetzt werden. Seit Jahren steigt die Zahl von Cyberattacken auf diese Kontrollsysteme.
Die damit verbundenen zusätzlichen Herausforderungen und Gefahren sind:

1. Sensoren und Aktoren[3] in Industrieanlagen waren früher Teil eines separaten, eigenständigen sogenannten Sensor-Aktor-Netzwerks und nicht mit dem Internet verbunden. Das Hauptaugenmerk beim Design solcher Systeme war bis anhin eine hohe Zuverlässigkeit und Sicherheit im Sinne des Prozessablaufs. Da sie nicht mit dem Internet verbunden waren, wurden sie nicht speziell gegen Cyberangriffe gesichert. Heute sind solche IIoT-Komponenten jedoch

[3] Aktor: Elemente, die elektrische Signale und Strom in elektrische, thermische, chemische oder Strömungs-Energie transformieren

entweder direkt einem Datennetzwerk angeschlossen oder das alte Sensor-Aktor-Netzwerk wird mittels Gateways[4] mit dem Firmennetzwerk oder mit dem Internet sowie virtuellen Umgebungen (Clouds) verbunden. Sind die Netzwerkverbindungen oder Cloudspeicher schlecht gesichert, können bei einem Cyberangriff gefährliche Zustände in Industrieanlagen auftreten, welche Auswirkungen auf Leib und Leben oder Gesundheit von Personen haben können.

2. Hersteller von ICS und „Supervisory Control and Data Acquisition"-Anlagen (kurz SCADA-Systeme) implementieren immer häufiger Services, welche auf ein offenes Netzwerk sowie drahtlose Verbindungen angewiesen sind. Auch werden zunehmend Sensoren, Aktoren und Gateways direkt mit dem Internet verbunden, um so schnell und bequem auf Fehler im System reagieren zu können. Bis 2001 wurden die meisten Angriffe auf ICS von intern, vom internen Netzwerk ausgeübt. Erst mit der Vernetzung, wurden Angriffe aus dem Internet möglich.
3. Industrieanlagen haben heute dutzende Microcontroller und Prozessoren mit Millionen von Zeilen Programmcode eingebaut – auch für die Datenkommunikation ins Internet. Mit der steigenden Komplexität der Anwendungen und deren hohen Anteil an Software werden die Anlagen immer anfälliger für Fehler und Sicherheitslücken.

3 Cyberangriffe mit Bezug zu IoT-Geräten

IoT-Geräte können erstens selbst das Ziel von Cyberangriffen sein. Dies ist der Fall, wenn Angreifer versuchen direkt auf die IoT-Geräte zuzugreifen, um diese zu manipulieren, zu steuern oder zu missbrauchen. Die Beispiele reichen von Zugriffen auf Smart-Speakers oder Babyphones (um Gespräche abzuhören), bis zu Manipulationen von Drehzahlen bei Motoren in Produktionsanlagen. Zweitens können Angriffe auf IoT-Geräte dazu dienen, über diese Geräte in das lokale Netzwerk einzudringen. Es erfolgt dabei keine Manipulation an der Steuerung der Geräte selber. Drittens können Angriffe auf IoT-Geräte dazu dienen, Botnetze aufzubauen, um andere Computer oder Server anzugreifen (z. B. mittels DDoS[5] Attacke). Und viertens werden statt Daten, die Rechenkapazität der Opfersysteme zweckentfremdet, um durch Berechnungen Kryptowährungen zu erzeugen (Crypto- oder Coin-Mining).
Diese grundlegenden Möglichkeiten machen IoT-Geräte als Ziel von Cyberangriffen attraktiv. Bevor auf die wichtigsten Fälle eingegangen wird, werden einleitend die eigentlichen Ziele von Cyberattacken aufgezeigt.

3.1 IoT und die verschiedenen Ziele von Cyberangriffen

Geld verdienen
Einer der Hauptgründe für Cyberattacken ist die Möglichkeit illegal Geld zu verdienen. Wem es gelingt, ein Botnetz mit fernsteuerbaren Rechnern aufzubauen, kann dieses vermieten oder verkaufen. Die schlecht geschützten IoT-Geräte werden von Cyberkriminellen für den Aufbau solcher Botnetze[6] genutzt. Sie führen mit der Rechenleistung dieser Geräte DDoS-Attacken aus, z. B. auf Webshops, Websites oder andere online-Dienstleistungen. Auch die gezielte Verschlüsselung von IoT-Geräten durch Ransomware (auch Verschlüsselungs- oder Erpressungstrojaner genannt) wird für Angreifer zunehmend attraktiver. Da ein Ausfall von IoT-Geräte oft physische Funktionen beeinträchtigen kann, eignen sie sich aus Sicht der Angreifer für Erpressungen der Eigentümer.

[4] Gateway: Komponente (Hard- und/oder Software), welche zwischen zwei Systemen eine Verbindung herstellt.
[5] Unter DoS (Denial of Service = Verweigerung des Dienstes) versteht man einen Angriff auf Computer-Systeme mit dem erklärten Ziel, deren Verfügbarkeit zu stören. Im Fall einer durch eine Vielzahl von gezielten Anfragen verursachten, mutwilligen Dienstblockade spricht man von einer Denial-of-Service-Attacke und wenn die Anfragen von einer grossen Zahl an Rechnern aus durchgeführt werden, von einer Distributed-Denial-of-Service (DDoS) Attacke.
[6] Botnetz: Eine riesige Anzahl «gekaperter» Systeme, die vom Angreifer ferngesteuert werden können.

Sabotage
Als Sabotage wird die absichtliche Störung eines Prozessablaufs bezeichnet. Die Gefahr von Sabotage ist insbesondere bei kritischen Infrastrukturen zu beachten. Bei Sabotageakten werden die IoT-Geräte solcher Infrastrukturen gezielt angegriffen, mit der Absicht, die Versorgung mit unverzichtbaren Gütern und Dienstleistungen, wie Energie, Verkehr oder Kommunikation zu stören oder zu unterbinden und damit einen schwerwiegenden Schaden anzurichten. Aber auch das Schadenspotential bei nicht kritischen Infrastrukturen und deren Nebeneffekte sind nicht unwesentlich. So kann eine Störung in einem vermeintlich unkritischen System schlimmstenfalls ganze Produktionsanlagen von wichtigen Industriegütern zum Stillstand bringen. Oder falls es das Geschäft einer kritischen Masse an Firmen gleichzeitig betrifft, kann dies volkswirtschaftlich schwere Auswirkungen haben.

Spionage
Als Spionage wird das unbemerkte Beschaffen, das Ausspähen von Informationen für politische, wirtschaftliche oder militärische Ziele bezeichnet. Mit der zunehmenden Digitalisierung werden zur Informationsbeschaffung vermehrt intelligente Computerprogramme (Malware, Trojaner) eingesetzt, welche sich autonom in einem System einnisten und sensitive Daten abfangen und weiterleiten. Diese Schadensprogramme können entweder über die Vernetzung verteilt oder über Sicherheitslücken in ein System eingeschleust werden. Auch IoT-Geräte können zu Spionagezwecken ausgenutzt werden.

3.2 Bekannte Cyberangriffe mit Bezug zu IoT

In den vergangenen Jahren zeigte es sich, dass es für Hacker ein Leichtes ist Tausende oder gar Millionen von IoT-Geräten zu übernehmen. Die wichtigsten bekannten Vorfälle von Cyberattacken in Zusammenhang mit IoT-Komponenten sind gut dokumentiert und öffentlich zugänglich. In der Auftragsstudie der HSLU «Sicherheitsstandards im IoT» findet sich ein Überblick über die bekanntesten Cyberangriffe, an welchen das IoT wesentlich beteiligt war und sowie eine kurze Erläuterung zu den Angriffen.
Als prominente Beispiele sind, «BASHLITE», «Mirai» sowie «BrickerBot» zu nennen. Die initiale Version der Schadsoftware «BASHLITE» nutzte Schwachstellen in Geräten, vorzugsweise Routern, aus und schloss die kompromittierten Komponenten zu einem Botnetz zusammen. Mittels «BASHLITE» bzw. dessen Variationen haben Botnetz-Betreiber im 2016 über eine Million Geräte kompromittiert und für die Durchführung von DDoS-Attacken ausgenutzt. Der Botnetz-Virus «Mirai» dient zum Aufbau von Botnetzen, welches gezielte Angriffe auf IoT-Geräte wie Webcams, Router oder Digitale Video-Recorder (DVR) ausführt. «Mirai» konnte innert wenigen Wochen Millionen von Geräten infizieren. Die Auswirkungen eines Angriffs mit einer neuen Variante des «Mirai-Botnetz» hatten 2016 einen grossen Teil der Internetverfügbarkeit beeinträchtigt. «BrickerBot» ist eine IoT-Malware, welche sich in verschiedenen IoT-Geräten einnistet und diese durch überschreiben des Betriebssystems und der Systempartition zerstört. Als weiteres Beispiel ist ein Angriff aus dem Jahre 2015 zu erwähnen. Dieser wurde von Hackern angekündigt und demonstriert. Dabei konnten sie die digitalen Systeme eines Fahrzeuges übernehmen und dieses aus der Ferne übers Internet steuern. Dieser Angriff veranlasste einen der grössten Automobilhersteller der Welt zum Rückruf von 1,4 Millionen seiner Fahrzeuge. Und als wirkungsvoll ist ebenfalls der Schadcode «Triton» zu nennen, mit welchem unbekannte Angreifer im Sommer 2017 die Sicherheitssysteme der Produktionsanlagen einer petrochemischen Fabrik übernehmen konnten. Damit hätten sie lebensgefährliche Unfälle verursachen können.

3.3 Fazit aus den Cyberattacken

Diese realen Angriffe verdeutlichen das massive Potenzial, mittels oder über IoT-Geräte Störungen und sogar Zerstörungen in relativ kurzer Zeit zu verursachen. Darüber hinaus zeigen sie klar auf, dass Angreifer erfolgreich die Kontrolle über IoT-Geräte übernommen oder diese als Mittel benutzt haben, um ihre Ziele zu erreichen. Die Angriffe sind komplex und sehr vielschichtig, von gestreuten bis hin zu

gezielten und spezialisierten Angriffen. Um sich gegen diese Cyberangriffe grundsätzlich zu schützen, sollten Unternehmen bewährte Sicherheitsverfahren anwenden, einschliesslich der Kenntnis der in ihrem Netzwerk laufenden IoT-Geräte, der Änderung ihrer Standardpasswörter sowie der Sicherstellung, dass die IoT-Geräte vollständig gepatcht sind.
Was aus den verfügbaren Daten zu Cyberattacken aber kaum hervorgeht, ist der finanzielle Schaden, welchen die erfolgten Angriffe anrichten. Das liegt u. a. daran, dass die angegriffenen Firmen, aus Wahrung von Geschäftsgeheimnisses oder aus der Furcht vor Reputationsschäden, sehr zurückhaltend mit Meldungen oder Informationen darüber sind. DDoS Angriffe z. B. haben oft zeitlich begrenzte Ausfälle der IT-Infrastruktur zur Folge. Hingegen können Sabotage-Angriffe, welche kritische Infrastruktur ausser Betrieb setzen oder sogar beschädigen, zu sehr hohen finanziellen Folgekosten führen.[7] Somit muss die korrekte Abwehrstrategie gegen Cyberattacken nicht nur auf die Häufigkeit oder Reichweite der Angriffe ausgerichtet sein, sondern muss auch den potentiellen Schaden berücksichtigen, welcher aus Attacken resultieren kann. Ein entsprechendes Risikomanagement hilft Betreibern von IoT-Systemen dabei, hierzu sinnvolle Massnahmen zu definieren.

4 Stand internationale Richtlinien für IoT-Geräte

4.1 Internationale Standards und Richtlinien für IoT

Die Anzahl offizieller internationaler Standards und Richtlinien zur Informationssicherheit spezifisch für IoT-Geräte sind überschaubar. Es ist jedoch zu erwarten, dass sich diese relativ neuen Standards rasch weiterentwickeln werden und weitere Standards hinzukommen. Die Richtlinien können unterteilt werden in solche, die für Hersteller von Bedeutung sind und von diesen beachtet werden sollten, sowie Richtlinien, die den Lebenszyklus von IoT-Geräten in einer Organisation definieren und einen sicheren Betrieb gewährleisten sollen. Die letzteren beschreiben, was in den unterschiedlichen Phasen von Geräteauswahl bis Ausserbetriebnahme wichtig ist. Natürlich gibt es auch Standards oder Richtlinien welche beide Aspekte betrachten.

4.1.1 Richtlinien für Hersteller

DIN SPEC 27072: IoT-fähige Geräte – Mindestanforderungen zur Informationssicherheit
Die DIN SPEC 27072 wurde unter Beteiligung von Herstellern, dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie weiteren Prüfstellen durch den deutschen Normenverband entwickelt und im Mai 2019 veröffentlicht. Sie legt Mindestanforderungen an IoT-Geräte aus dem Small Business oder Home Umfeld fest, welche gegen elementare Angriffe aufgrund von Designschwächen (z. B. verwenden von Standardpasswörtern) schützen sollen. Fokus der Spezifikation ist die Basisabsicherung der IP-basierten Kommunikation für IoT-Geräte. Es werden IT-Sicherheitseigenschaften festgelegt, welche bei der Entwicklung von Geräten berücksichtigt werden sollen (Security-By-Design). Die Geräte sollen dadurch gegen skalierbare Cyberangriffe aus dem Internet (wie z. B. Mirai) geschützt werden.
Die Grenzen der neuen Spezifikation liegen darin, dass sie sich auf Vorgaben zu einzelnen Geräten beschränken. IoT-Geräte sind aber in der Regel keine Stand-Alone Lösung, sondern in ein IT-System eingebunden. Weitere Komponenten eines solchen Systems (zugehörige Services, Apps, Desktop-Software usw.) werden nicht betrachtet.

ETSI TS 103 645: Cyber Security for Consumer Internet of Things

[7] Für die Schweiz bieten die Resultate der Innovationserhebung der Konjunkturforschungsstelle der ETH (KOF) aus dem Jahr 2016 Anhaltspunkte für die Einschätzung der finanziellen Schäden. Die Studie hat ergeben, dass kleinere Unternehmen häufiger einen Erwerbsausfall durch Cyberangriffe als mittlere und grosse Unternehmen meldeten, aber grosse Unternehmen jedoch öfters grösseren Aufwand betreiben mussten, um Schadensfälle zu beheben. Vgl. Innovation in der Schweizer Privatwirtschaft, Ergebnisse der innovationserhebung 2016 der Konjunkturforschungsstelle der ETH (KOF) im Auftrag des Staatssekretariats für Bildung, Forschung und Innovation (SBFI).

Das Europäische Institut für Telekommunikationsnormen (ETSI) hat im Februar 2019 einen Standard zur Cybersicherheit von IoT bei Konsumgütern herausgegeben. Das Dokument beschreibt allgemein anerkannte und bewährte Verfahren zur Sicherung von IoT-Geräten mit ergebnisorientierten Bestimmungen, ohne allzu stark in technische Details zu gehen. Ziel der Spezifikation ist es, alle an der Entwicklung und Herstellung von IoT-Geräten beteiligten Parteien bei der Sicherung ihrer Produkte zu unterstützen. Der Fokus liegt auf technischen Kontrollen und organisatorischen Richtlinien, die bei der Vermeidung der wichtigsten und weit verbreiteten Sicherheitslücken berücksichtigt werden sollen.
Das Dokument enthält Bestimmungen für die Sicherheit von IoT-Geräten im Consumer Umfeld die mit dem Internet verbunden sind. Dazu gehören Geräte wie:

- Kinderspielzeug und Babyphone;
- sicherheitsrelevante Produkte wie Rauchmelder und Türschlösser;
- intelligente Kameras, Fernseher und Lautsprecher;
- tragbare Gesundheitstracker;
- Hausautomations- und Alarmsysteme;
- Haushaltgeräte (z. B. Waschmaschinen, Kühlschränke);
- Smart Home Assistenten.

Diese technische Spezifikation bietet Unternehmen, die an der Entwicklung und Herstellung von solchen Geräten beteiligt sind, grundlegende Hinweise zur Umsetzung der Bestimmungen.

IEC 62443-3-3: Security for industrial process measurement and control – Network and system security

Die International Electrotechnical Commmission (IEC) ist eine internationale Normungsorganisation im Bereich der Elektrotechnik. 2013 hat die IEC den Standard IEC 62443-3-3 veröffentlicht. Dieser beschreibt das Umfeld zur Sicherung der informations- und kommunikationstechnischen Aspekte industrieller Mess- und Regelsysteme einschliesslich ihrer Netzwerke und Geräte in diesen Netzwerken während dem gesamten Lebenszyklus der Anlage. Sie gibt Hinweise zu den Anforderungen an die Betriebssicherheit einer Anlage und richtet sich in erster Linie an die Eigentümer/Betreiber von Automatisierungssystemen, die für den Betrieb des Industrial Control System (ICS) verantwortlich sind. Die betrieblichen Anforderungen dieser Spezifikation können auch für weitere Gruppen im Umfeld des ICS von Interesse sein:

- Automatisierungssystem-Designer;
- Hersteller von Geräten, Subsystemen und Systemen;
- Integratoren von Subsystemen und Systemen.

Das Dokument berücksichtigt folgende Punkte:

- Migration/Evolution bestehender Systeme;
- Erfüllung von Sicherheitszielen mit bestehenden COTS[8]-Technologien und -Produkten;
- Gewährleistung der Zuverlässigkeit/Verfügbarkeit der gesicherten Kommunikationsdienste;
- Anwendbarkeit auf Systeme jeder Grösse und jedes Risikos (Skalierbarkeit);
- Koexistenz von Sicherheits-, Rechts- und Regulierungs- und Automatisierungsfunktionalitäten mit Sicherheitsanforderungen.

4.1.2 Richtlinien für den Betrieb

BSI IT-Grundschutzkompendium: Umsetzungshinweise zum Baustein SYS.4.4 Allgemeines IoT-Gerät

Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) hat Umsetzungshinweise für den Einsatz von IoT-Geräten veröffentlicht. Die Umsetzungshinweise beschreiben die Vorgehensweise und Massnahmen, wie IoT-Geräte während ihrem gesamten Lebenszyklus – von Planung- und Konzeptionsphase bis Ausserbetriebnahme – in einer Organisation betrieben werden sollen und was

[8] COTS steht für „commercial off-the-shelf“ bzw. „components-off-the-shelf“. seriengefertigte Produkte aus dem Elektronik- oder Softwaresektor (vgl. Standardsoftware), die in grosser Stückzahl völlig gleichartig (ugs. „von der Stange“) aufgebaut und verkauft werden

dabei speziell beachtet werden muss. Das Dokument gilt allgemein für IoT-Geräte in unterschiedlichen Einsatzgebieten.

4.2 Leitfäden zur Informationssicherheit für IoT-Geräte

Neben den wenigen offiziellen internationalen Standards und Richtlinien zur Informationssicherheit für IoT-Geräte existiert eine Vielzahl an Leitfäden und Sicherheitshinweisen für den sicheren Betrieb von IoT-Geräten und -Systemen. Dies sind «Best Practices» für den Umgang mit IoT-Sicherheit, die von staatlichen Organisationen, Allianzen oder auch Unternehmen herausgegeben werden. Solche praxisnahen Leitfäden ergänzen offizielle Standards, um die Informationssicherheit von IoT-Installationen nachhaltig zu verbessern. Oft verweisen diese «Best Practices» auf bestehende allgemeine Informationssicherheitsrichtlinien. Sie gelten für den gesamten Lebenszyklus von IoT-Geräten: Entwicklung, Produktion, Konfiguration und Installation, Wartung und Ausserbetriebnahme. Einige Beispiele von Organisationen die solche Leitfäden erarbeitet haben:

Cisco: Cisco als Hersteller von Komponenten und Dienstleister im Bereich Datennetzwerke hat das Buch «Orchestrating and Automating Security for the Internet of Things: Delivering Advanced Security Capabilities from Edge to Cloud for IoT» herausgegeben.

DHS: Die «Cybersecurity and Infrastructure Security Agency» (CISA) des us-amerikanischen «Department of Homeland Security» (DHS) hat das Dokument «Strategic principles for securing the Internet of Things» erstellt.

ENISA: Die European Union Agency for Network and Information Security (ENISA) hat viele Publikationen im Bereich Informationssicherheit erarbeitet. Einige beziehen sich speziell auf IoT-Themen wie Smart Cities, Public Transport, Hospital, Smart Home, Manufacturing, Airports, usw.

GSMA: Die GSMA repräsentiert die Interessen der Mobilfunkanbieter weltweit und hat Guidelines für IoT Security veröffentlicht.

IoTSF: Die IoT Security Foundation (IoTSF) hat als Non-Profit-Organisation eine Reihe von Publikationen im Bereich Informationssicherheit und IoT als «IoT Security best practise guidelines» veröffentlicht.

NIST: US-amerikanische National Institute of Standards and Technology (NIST).

4.3 Allgemeine Richtlinien zur Informationssicherheit

Standards und Richtlinien zur Informationssicherheit wie die ISO/IEC 27000-Familie, das NIST «Cybersecurity Framework» oder BSI IT-Grundschutz-Kompendium beschreiben, wie die benötigte Informationssicherheit in Organisationen erreicht werden kann. Unter anderem auch wie ein Information Security Management System (ISMS) implementiert werden kann. Diese allgemein gültigen Standards können selbstverständlich auch für Systeme mit IoT-Geräten angewendet werden. Bei der Adaption sowie Implementation dieser Richtlinien müssen aber die besonderen Gefahren und Herausforderungen für IoT-Geräte speziell beachtet werden.

4.4 Fazit zu den Richtlinien für IoT-Geräte

Offizielle internationale Standards und Richtlinien zur Informationssicherheit spezifisch für IoT-Geräte gibt es wenige. Studien im Zusammenhang mit Informationssicherheit und IoT zeigen folgende Problematik auf: Es existieren verschiedenste Standards und viele Leitfäden zu unterschiedlichen Themengebieten. Kein Standard hat sich bis jetzt etablieren können. Hersteller wissen nicht, an welchen Standards sie sich orientieren sollen. Zielführend wäre deshalb eine Förderung der Harmonisierung von IoT-Sicherheitsinitiativen und -vorschriften. Die «Alliance fort he Internet of Things Innovation, AIOTI» hat zu diesem Thema kürzlich zwei Berichte veröffentlicht, in denen sie

aufzeigt, welche Standards und Open-Source-Lösungen für die Entwicklung von Vorgaben im IoT genutzt werden können und welche Lücken in der Standardisierung prioritär zu schliessen sind.
Neben den Ansätzen zur Standardisierung existiert eine grosse Anzahl an Leitfäden und «Best Practices» zum Thema Informationssicherheit. Diese Leitfäden verweisen in der Regel auf allgemein gültige und bewährte Standards zum Thema Informationssicherheit für IKT. Sofern die aufgezeigten IoT-Besonderheiten beachtet werden, können diese vielfach bewährten Standards auch für IKT-Systeme mit IoT-Geräten angewendet werden. Richtlinien speziell für IoT-Geräte ergänzen diese allgemein gültigen Richtlinien zur Informationssicherheit z. B. für IoT im Consumer Bereich, industriellen Anwendungen (IIoT) oder kritischen Infrastrukturen.
Das Verfassen von Standards und «Best Practices» genügt aber nicht, um mehr Sicherheit für IoT-Anwendungen zu etablieren. Wesentlich ist deren Umsetzung in der Praxis. Die grundsätzliche Verantwortung zum Eigenschutz liegt aber bei den jeweiligen Unternehmen und Organisationen. Jedes Unternehmen ist für den sicheren Betrieb seiner IT-Infrastruktur selber verantwortlich. Interessante Ergebnisse hierzu für die Schweiz könnte auch das EU-Projekt SerIoT[9] (Secure and Safe Internet of Things) liefern, welches die Entwicklung einer IoT-Plattform mit dem Schwerpunkt Cybersicherheit und Privacy für IoT Systeme zum Ziel hat.

5 Umsetzung von Standards bei Bund und kritischen Infrastrukturen

Sicherheitsrichtlinien für Bund und bundesnahe Betriebe oder für Betreiber von kritischer Infrastruktur unterscheiden sich in Bezug auf Cybersicherheit für IoT-Geräte nicht. Standards, «Best Practices» und Prozesse um eine ausreichend hohe Sicherheit gegen Cyberangriffe zu erreichen, sind identisch. Je nach Anforderungen einer Organisation können risikobasierend unterschiedliche Sicherheitslevels eines bestimmten Standards umgesetzt werden. Für Unternehmen und insbesondere Betreiber kritischer Infrastrukturen hat das Bundesamt für wirtschaftliche Landesversorgung (BWL) den rechtlich nicht direkt verbindlichen «Minimalstandard zur Verbesserung der IKT-Resilienz» erstellt. Dieser IKT-Minimalstandard basiert auf dem NIST “Cybersecurity Framework”, mit punktuellen Ergänzungen aus weiteren international anerkannten Industriestandards wie ISO 2700x, COBIT, ENISA «NCSS Good Practice Guide» und BSI 100-2. Ziel des empfohlenen «Standards» ist es, Unternehmen und Organisationen ein Hilfsmittel zur Hand zu geben, wodurch sie individuell die Resilienz ihrer IKT-Infrastruktur verbessern können.

6 Rechtliche Aspekte im IoT

Wie bei anderen Technologien ist auch bei der Nutzung von IoT unbedingt die damit verbundene Rechtslage mit zu berücksichtigen. Folgend werden die Fragestellungen zum Umgang mit Daten sowie zur Gewährleistung und Garantie im Zusammenhang mit IoT-Geräten kurz beleuchtet. Zudem wird ebenfalls in diesem Kontext die Thematik der Meldepflicht von Cybervorfällen aufgegriffen.

6.1 Datenschutz

Eine wichtige Motivation beim Einsatz von IoT ist das Sammeln und Auswerten von Daten. Die Geräte tauschen über Netzwerke oder das Internet Informationen aus, die unter Umständen einen Bezug zu einer natürlichen Person zulassen können. Dabei genügt es, wenn der Bezug zur konkreten Person nicht unmittelbar (bestimmt), sondern erst mit einem verhältnismässigen Aufwand (bestimmbar) möglich ist. Sobald dies der Fall ist (Smartmeter, Infos aus Arealprodukten etc.), sind die

[9] https://seriot-project.eu/

Anforderungen der Datenschutzgesetzgebung zu berücksichtigen. Bei privaten Datenbearbeitern (z. B. Unternehmen) gilt, dass sie Personendaten im Prinzip ohne besondere Grundlage bearbeiten dürfen. Erst wenn eine Datenbearbeitung im konkreten Fall zu einer Persönlichkeitsverletzung führt, benötigen sie einen Rechtfertigungsgrund (Art. 12 DSG; Art. 26 E-DSG[10]). Der Rechtfertigungsgrund kann eine gesetzliche Grundlage, die Einwilligung der betroffenen Person oder ein überwiegendes privates oder öffentliches Interesse an der Datenbearbeitung sein (Art. 13 DSG; Art. 27 E-DSG). Bei Bundesorganen gilt dagegen das Legalitätsprinzip. Sie dürfen Personendaten grundsätzlich nur dann bearbeiten, wenn dafür eine gesetzliche Grundlage besteht. Ausnahmsweise kann eine Datenbearbeitung im Einzelfall unter anderem auf die Einwilligung der betroffenen Person gestützt werden (Art. 17 und 19 DSG; Art. 30 und Art. 32 E-DSG). Zu beachten ist, dass jeder Umgang mit Personendaten als Bearbeitung gilt. Im Weiteren sind alle Datenschutzanforderungen ans Managementsystem mit zu berücksichtigen. Die Datenschutzgesetzgebung regelt zwar das Bearbeiten von Daten, nicht aber die Anforderungen an das Inverkehrbringen von Produkten. Die Mindestanforderungen an die Datensicherheit werden in der Verordnung zum Datenschutzgesetz (VDSG) festgelegt (Art. 7 Abs. 2 DSG; Art. 7 Abs. 3 E-DSG). Diese Bestimmungen werden in der Folge der Totalrevision des DSG revidiert. Mit dem Entwurf zur Revision des DSG (E-DSG) wird der Grundsatz des Datenschutzes durch Technik ausdrücklich im Gesetz verankert. Nach Art. 6 Abs. 1 E-DSG ist der Datenbearbeitungsverantwortliche verpflichtet, seine Datenbearbeitungen bereits ab der Planung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden. Ausserdem soll der Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB) Verfügungskompetenzen erhalten. Danach soll der EDÖB bei einer widerrechtlichen Datenbearbeitung unter anderem die Datenbearbeitung untersagen sowie anordnen können, dass die betroffenen Personendaten vernichtet werden müssen. Er könnte auch anordnen, dass im Bereich der Sicherheit geeignete technische und organisatorische Massnahmen getroffen werden müssen (s. Art. 45 Abs. 1 und 3 in Verbindung mit Art. 7 E-DSG). Des Weiteren sieht Art. 55 Bst. c E-DSG neu eine Strafbestimmung bei der vorsätzlichen Verletzung der Mindestanforderungen an die Datensicherheit vor.

Einige der von IoT-Geräten übermittelten Informationen ohne Personenbezug lassen ebenfalls Rückschlüsse auf mögliche Geschäfts- oder Fabrikationsgeheimnisse zu. Zentral ist hier, dass sich die betroffenen Parteien gegenseitig informieren und gemeinsam vereinbaren, zu welchem Zweck (z. B. Wartung) die Informationen benötigt werden und wann sie wieder löscht werden. Fehlen derartige Vereinbarungen, besteht das Risiko der Wirtschaftsspionage oder aufgrund wettbewerbsrechtlicher Verstösse angeprangert zu werden. Führungspersonen, seien sie nun Absender oder Bezüger solcher Informationen, müssen im Rahmen ihrer Sorgfaltspflicht zwingend diese Themen als unternehmerische Handlungsfelder und auch Risiken verstehen und bearbeiten. Wird dies übersehen, so machen sie sich gegebenenfalls auch persönlich haftbar. Werden solche Informationen berechtigterweise weiterbearbeitet, ist es durchaus möglich, dass die daraus gewonnenen Resultate dem Urheberrecht unterliegen und somit deswegen wieder nur eingeschränkt weiterverwendet werden dürfen. Handelt es sich um staatliche Organisationen, so können Resultate aus Weiterverarbeitungen dem Öffentlichkeitsprinzip und/oder den Forderungen von Open Data unterliegen.

Rechtswidriger Umgang mit Daten kann verschiedene Gesetze des privaten und öffentlichen Rechtes tangieren und auch entsprechende zivilrechtliche Haftungen oder strafrechtliche Sanktionen nach sich ziehen. Es sind durchaus geltende Gesetze, die verletzt werden, der Sachverhalt findet anstatt in der realen Welt einfach in der virtuellen Welt statt. Um das Vorliegen der entsprechenden Verstösse belegen zu können, sind IT-forensisches Wissen und entsprechend spezialisierte Werkzeuge unabdingbar. Der Aufwand für die Beweisaufnahme ist in der virtuellen Welt oft signifikant höher, u. a., weil verfügbare Spuren wie IP-Adressen nicht zwangsläufig zu den verantwortlichen Personen führen.

[10] Bundesgesetz Entwurf über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (E-DSG), BBl 2017 7193

6.2 Gewährleistung, Garantie und Produktesicherheit

Der Verkäufer haftet nach den Regeln der Sachgewährleistung des Obligationenrechts (Art. 197 ff. OR) für Mängel an der Kaufsache. Ein Mangel liegt entweder vor, wenn der Wert der Kaufsache oder ihre Tauglichkeit zum vorausgesetzten Gebrauch aufgehoben oder erheblich gemindert ist, oder aber eine vom Verkäufer zugesicherte Eigenschaft nicht vorliegt (Art. 197 Abs. 1 OR). Auf Zeit zugesicherte Eigenschaften der Sache selber werden als unselbständige Garantien bezeichnet und gelten als Zusicherungen im Sinne der Sachgewährleistung.[11] Demgegenüber liegt ein selbstständiger Garantievertrag (Art. 111 OR) vor, wenn der Verkäufer einen künftigen Erfolg verspricht, der über die vertragsgemässe Beschaffenheit der Kaufsache hinausgeht, weil er wesentlich noch von anderen künftigen Faktoren abhängt, die von den Sacheigenschaften unabhängig sind und ausserhalb der Einflussmöglichkeiten des Verkäufers liegen.[12] Die Garantie stellt ein Leistungsversprechen abstrakter Natur dar; es handelt sich um eine freiwillige Verpflichtung des Verkäufers, die gesetzlich nicht näher geregelt ist.

Unklar ist, ob und unter welchen Bedingungen Sicherheitslücken in der Software von IoT-Geräten einen Sachmangel darstellen. Entscheidend ist zunächst, ob der Verkäufer sich im Kaufvertrag ausdrücklich oder stillschweigend zur Bereitstellung der Software verpflichtet hat. Beim Kauf von Geräten mit integrierter Software dürfte das in der Regel der Fall sein. Hat er sich jedoch nicht dazu verpflichtet, so kann bei einer Sicherheitslücke wohl ohnehin nicht von einem Sachmangel ausgegangen werden. Der Käufer kann sich in einem solchen Fall wohl nur an den Softwarehersteller halten. Aber auch dann, wenn der Verkäufer sich im Kaufvertrag dazu verpflichtet hat, die Software zur Verfügung zu stellen, ist unklar, ob Sicherheitslücken überhaupt je als Sachmängel qualifiziert werden können. Sicherheitslücken stellen nicht schon per se eine Einschränkung im Gebrauch dar. Als Sachmängel gelten zudem nur Mängel, welche schon im Zeitpunkt des Übergangs der Gefahr vorliegen. Fraglich ist deswegen insbesondere auch, wie es sich bei später auftretenden Sicherheitslücken verhält. Zu diesem Punkt gibt es – soweit ersichtlich – noch keine Rechtsprechung. Entdeckt die Käuferin einen Mangel, muss sie diesen unverzüglich gegenüber dem Verkäufer rügen. Sie hat dann die Wahl, vom Verkauf zurückzutreten oder eine Minderung des Kaufpreises zu verlangen. Bei vertretbaren Sachen kann sie überdies Ersatzlieferung verlangen. Für weiteren Schaden (z. B. für einen Produktionsausfall) kann sie vom Verkäufer Ersatz verlangen, sofern dieser nicht beweist, dass ihn kein Verschulden trifft. Die Mängelrechte können im Übrigen vertraglich, z. B. über AGB, eingeschränkt oder abgeändert werden. Die Ansprüche aus Sachgewährleistung verjähren zwei Jahre nach Ablieferung der Kaufsache. Im Falle von Lieferungen an Konsumenten kann der Verkäufer diese Frist bei Neuwaren nicht verkürzen; er kann sie aber um ein Jahr verkürzen, wenn es sich um gebrauchte Waren handelt. Die kurzen Fristen können bei Produkten, von welchen üblicherweise eine längere Lebensdauer erwartet wird, insofern problematisch sein, als dass für Verkäufer bzw. Hersteller unter Umständen ein geringerer Anreiz besteht, über die Verjährungsfrist hinaus Sicherheitslücken zu beheben.

Angesichts dieser unklaren gesetzlichen Situation sind Käufer gut beraten, sich vom Verkäufer Zusicherungen oder (selbständige) Garantien geben zu lassen, welche die Thematik der Softwareupdates, und Sicherheitslücken umfassend und klar regeln. Die Betriebszeiten von IoT-Geräten können insbesondere in der Industrie oder Gebäudeautomation durchaus im Bereich von 10 Jahren oder mehr liegen. Eine vertragliche Vereinbarung über eine genügend lange Wartungszeit der Software ist in solchen Fällen sehr empfehlenswert. Sollte eine Anbindung an andere Systeme wichtig sein, muss zudem vertraglich die Offenlegung von möglichen Schnittstellen während der ganzen zu erwartenden Betriebszeit des Gerätes garantiert sein. Diese Pflicht zur fortlaufenden Bereitstellung aller Funktionalitäten kann entweder als selbständiger Wartungsvertrag mit kauf-, werk-, miet- und auftragsrechtlichen Elementen oder als kaufvertragliche Nebenpflicht ausgestaltet sein.[13] Wenn eine ausdrückliche Regelung fehlt, wäre im Einzelfall zu prüfen, ob eine solche Pflicht nicht

[11] BGer 4A_220/2013 E. 4.3.1.
[12] BGE 122 III 426 E. 4 und E. 5c; BGer 4A_220/2013 E. 4.3.1.
[13] Vgl. M. EGGEN, Gewährleistung bei vernetzten Geräten, SZW 2019, 358, 364 f, m.w.N.

konkludent – als selbständiger Vertrag oder als selbständige kaufvertragliche Nebenpflicht – abgeschlossen wurde. Beim Kauf eines IoT-Gerätes einschliesslich Software kann in der Regel wohl davon ausgegangen werden, dass die Pflicht zur Systembereitstellung und –wartung Bestandteil des Kaufvertrags bildet, wenn dies nicht ausdrücklich ausgeschlossen wird. Eine gewisse Lebensdauer des Gerätes kann im Rahmen der Tauglichkeit zum vorausgesetzten Gebrauch nämlich erwartet werden. In der Lehre wird vertreten, dass für die Dauer dieser Pflicht zur Systembereitstellung und –wartung die Lebensdauer, die von Geräten dieser Art im Allgemeinen erwartet werden kann, massgeblich ist.[14] Die Verletzung einer solchen vertraglichen Pflicht könnte möglicherweise selbständig, d.h. unabhängig von den Regeln der Gewährleistung oder nur in analoger Anwendung derselben und mit einer entsprechend längeren Verjährungsfrist, geltend gemacht werden. Auch zu diesem Punkt bestehen jedoch soweit ersichtlich weder Rechtsprechung noch eine klare Mehrheitsmeinung in der Literatur.

6.3 Meldepflicht

Im Kontext des Datenschutzes ist in der Totalrevision des DSG eine Meldepflicht bei Verletzungen der Datensicherheit vorgesehen. Besteht bei einer Verletzung der Datensicherheit voraussichtlich ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen, muss der verantwortliche Datenbearbeiter inskünftig so rasch als möglich eine Meldung an den EDÖB machen (Art. 22 Abs. 1 E-DSG). Unter gewissen Umständen muss er zusätzlich auch die betroffenen Personen informieren, damit diese selber Massnahmen treffen können, um ihre Daten zu schützen (Art. 22 Abs. 4 E-DSG).
Für Cybervorfälle kennt die Schweiz aber keine generelle Meldepflicht und auch keine Pflicht zur Meldung von Verwundbarkeiten. Der Austausch zu Cybervorfällen oder von bekannten Sicherheitslücken bei kritischen Infrastrukturen wie Energieversorgung, Telekommunikation oder Finanz- und Versicherungswesen erfolgt auf freiwilliger Basis über die Melde- und Analysestelle Informationssicherung (MELANI). Angesichts der Entwicklung der Cyberrisiken stellt sich natürlich auch bei der intensiven Nutzung sowie Verbreitung von IoT die Frage, ob dieser freiwillige Austausch genügt, um Bedrohungen frühzeitig und sektorenübergreifend zu erkennen.
Diese Frage soll aber generell und nicht IoT-bezogen geprüft werden. Im Rahmen der Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) prüft der Bund, unter Einbezug der zuständigen Behörden, der Kantone und des Bundes sowie der Wirtschaft, Varianten für Meldepflichten von kritischen Infrastrukturen bei schwerwiegenden Sicherheitsvorfällen. Basierend auf diesen Ergebnissen will der Bundesrat bis Ende 2020 Grundsatzentscheide über die Einführung von Meldepflichten fällen.

6.4 Ausblick: Entwicklung des Rechtsrahmens in der EU

Viele Staaten sind daran zu prüfen, welche Anpassungen des Rechts möglich oder nötig sind, um die Sicherheit von IoT zu verbessern. Für die Schweiz besonders relevant sind die Arbeiten der EU. Im Folgenden werden relevante aktuelle Entwicklungen des Rechtsrahmens in der EU aufgezeigt. Die Auflistung erhebt keinen Anspruch auf Vollständigkeit und es sind zum gegenwärtigen Zeitpunkt auch keine Prognosen möglich, welche Schritte die EU unternehmen wird. Der Bundesrat wird die weiteren Entwicklungen verfolgen und laufend prüfen, welche Konsequenzen sich daraus allenfalls für die Schweiz ergeben.
In Bezug auf die Thematik der oben beschriebenen Fragen der Gewährleistung, Garantie und Produktesicherheit ist die revidierte Warenkaufsrichtlinie der EU wichtig (Richtlinie 2019/771 vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte des Warenkaufs). Dort ist für den Kauf von Waren mit digitalen Elementen vorgesehen, dass der Verkäufer dafür zu sorgen hat, dass der Verbraucher Sicherheitsaktualisierungen, die für den Erhalt der Vertragsmässigkeit dieser Waren

[14] Vgl. M. EGGEN, Home Smart Home – Eine privatrechtliche Einordnung von Lösungen für intelligentes Wohnen, AJP 2016, 1131 ff., 1139 m.w.N.

erforderlich sind, erhält. Wenn gemäss Kaufvertrag eine einmalige Bereitstellung von digitalem Inhalt vorgesehen ist, gilt diese Pflicht für den Zeitraum, den der Verbraucher aufgrund der Art und des Zwecks der Waren und der digitalen Elemente und unter Berücksichtigung der Umstände und der Art des Vertrags vernünftigerweise erwarten kann. Es gilt jedoch eine Gewährleistungsfrist von in der Regel zwei Jahren, wenn vertraglich nicht eine fortlaufende Bereitstellung digitaler Inhalte vereinbart wurde.[15] Die EU-Mitgliedsländer müssen diese neuen Regeln bis zum 1. Januar 2022 umsetzen.
Eine weitere interessante Entwicklung zeichnet sich im Bereich der Radio-IoT, das heisst bei IoT, welche mit mittels Funkwellen verbunden sind, ab. Die Europäische Kommission hat auf der Basis der geltenden Gesetzgebung (Funkrichtlinie RED; 2014/53/EU)[16] die Möglichkeit, zusätzliche Anforderungen durch einen einfachen delegierten Rechtsakt aufzuerlegen. Zu diesem Zweck hat die Europäische Kommission im Jahr 2019 ein öffentliches Konsultationsverfahren eingeleitet. Die Ergebnisse werden in Kürze erwartet, und die Vorbereitungen für einen delegierten Rechtsakt sind in vollem Gange. Da die Schweiz die Funkrichtlinie in ihre Gesetzgebung übernommen hat, sind diese Entwicklungen von besonderem Interesse. Durch eine Übernahme des delegierten Rechtsakts könnten verstärkte Anforderungen an die Cybersicherheit von drahtlos verbundenen IoT-Geräten gestellt werden. Die Schweiz ist über das Bundesamt für Kommunikation (BAKOM) an den Arbeiten der EU im Rahmen der Expertengruppe für die Funkrichtlinie beteiligt.

7 Fazit

Der Umstand, dass die Zahl der mit dem Internet verbundenen Geräte weiter steigen wird, legt nahe, dass auch die im Zusammenhang mit dem IoT stehenden Cyberattacken zunehmen werden. Die beschriebenen Attacken verdeutlichen das Risiko, das mit solchen Attacken einhergeht.
Zur Gewährleistung der Sicherheit von IoT zeigen sich mehrere Ansatzpunkte. Eine wichtige Erkenntnis ist, dass aufgrund dem breiten Einsatzspektrums von IoT die Nutzer und Nutzerinnen von IoT-Geräten massgeblich selbst die Sicherheit negativ beeinflussen können. Sei es, dass sie zu leichtfertig Grundsätze eines sicheren Betriebs von IoT-Geräten missachten, oder indem sie unsichere Produkte von unbekannten Herstellern betreiben. Hier gilt es die Bevölkerung weiter zu sensibilisieren und dazu zu motivieren, die grundlegenden Verhaltensmassnahmen für einen sicheren Betrieb einzuhalten.
Für den Betrieb von IoT-basierten Systemen in Unternehmen ist es entscheidend, dass IoT als integraler Bestandteil der IT-Infrastruktur erachtet wird und auch entsprechend bewährte Sicherheitsverfahren hierfür angewendet werden. Zudem lässt sich mit der Berücksichtigung des potentiellen Schadens, welcher aus Attacken resultieren kann, die passende Abwehrstrategie gegen Cyberattacken ausrichten. Ein entsprechendes Risikomanagement hilft Betreibern von IoT-Systemen hierzu sinnvolle Massnahmen zu definieren. Die bestehenden Standards und Richtlinien für die IT-Sicherheit bieten diesbezüglich bereits eine gute Grundlage. Mit Hilfe von Leitfäden und der Förderung des Austauschs unter Anwendern kann dazu beigetragen werden, deren Anwendung auf IoT zu verbreiten. Parallel dazu müssen die Hersteller ihre Verantwortung wahrnehmen und beispielsweise bei Inbetriebnahme ihrer Produkte Mindestanforderungen an die Informationssicherheit sowie den Datenschutz berücksichtigen. Obwohl viele Hersteller dieser Verantwortung nicht oder nur ungenügend nachkommen, wird die Sicherheit von verschiedenen Produzenten auch zunehmend als Chance verstanden, sich gegenüber Billigproduzenten durch erhöhte Qualitätsstandards abzugrenzen und sich in den kompetitiven Märkten zu behaupten. Diese Entwicklung kann durch die Staaten mittels Richtlinien, Leitfäden oder Vorschriften unterstützt werden. Auch dabei gilt, dass verschiedene normative Grundlagen und international etablierte Standards für Hersteller auch auf IoT anwendbar sind. Durch konsequente Umsetzung der bereits vorliegenden Richtlinien, können Hersteller und Betreiber von IoT-Geräten und IoT-Systemen bereits ein hohes Mass an Cybersicherheit erreichen.

[15] Vgl. Y. ATAMER/S. HERMIDAS, Die neue EU-Richtlinie zum Verbrauchsgüterkauf, AJP 2020, 48, 56 f.
[16] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32014L0053&from=EN

Analog gilt dies auch in rechtlicher Hinsicht. So gelten beispielsweise die Bestimmungen aus der Datenschutzgesetzgebung auch im IoT-Bereich. Wenn gezielt weitere rechtliche Vorgaben oder Richtlinien für IoT entwickelt werden sollen, so muss dies in enger internationaler Koordination geschehen. Vorschriften einzelner Staaten bleiben in ihrer Wirkung auf die Hersteller zu beschränkt und würden zu ungewollten Marktverzerrungen führen.

Die hier im Bericht aufgegriffenen Schwerpunkte zu Sicherheitsstandards für IoT-Geräte und deren Entwicklungen werden durch das Nationale Zentrum für Cybersicherheit (NCSC) im Rahmen der Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) mitberücksichtigt und weiterverfolgt. Im Speziellen gilt im Handlungsfeld «Standardisierung und Regulierung» sektoriell zu prüfen, in wie fern Lösungsansätze wirtschaftsverträglich zu realisieren sind. Diese Arbeiten erfolgen im Austausch mit allen beteiligten Departementen, den Kantonen sowie der Wirtschaft.