Zurück in die Zukunft bei der Gerätesicherheit

Wirksame Umsetzung von Grundsätzen für faire Informationspraktiken zur aktiven Verwaltung von Datenschutz- und Sicherheitsrisiken im Zusammenhang mit dem Internet der Dinge

Doron Rotman, CIPP, ist Geschäftsführer der KPMG LLP, nationaler Datenschutzleiter für die USA von KPMG und Mitglied des internationalen Datenschutzführungsteams von KPMG. Er verfügt über mehr als 30 Jahre Erfahrung in den Bereichen Datenschutz, Sicherheit und Informationsmanagement.

Chris Kypreos, CIPP, ist Senior Associate bei KPMG LLP und ein Mitglied der International Association of Privacy Professionals (IAPP). Kypreos hat bei mehreren Veröffentlichungen mitgewirkt sowie einige selbst verfasst und hat diese bei Fachveranstaltungen vorgestellt.

Sarah Pipes, CIPP, ist Senior Associate bei KPMG LLP und derzeit bei KPMG Belgien tätig. Pipes ist Mitglied der IAPP. Sie hat bei mehreren Veröffentlichungen mitgewirkt sowie mehrere selbst verfasst und hat bereits Vorträge auf mehreren Fachveranstaltungen gehalten.

Das Internet der Dinge (Internet of Things, IoT) birgt ungeahnte Kräfte. Eine bekannte Tatsache ist beispielsweise, dass mit dem IoT verbundene Geräte exponentiell wachsende Mengen an neuen Daten generieren, die wiederum zu wertvollen Erkenntnissen führen, neue Geschäftmöglichkeiten bieten und die Entwicklung innovativer Technologien erleichtern. Das IoT wirft jedoch auch verschiedene Bedenken zu Datenschutz und Datensicherheit auf, wenn neue Datenquellen mit veralteten Quellen kombiniert werden, um neue Erkenntnisse über Personen per Predictive Analytics zu gewinnen, die jedoch mit dem ursprünglichen Zweck der Erfassung und Verwendung unter Umständen nicht mehr übereinstimmen. Darüber hinaus kann die Verbindung neuer Technologien mit veralteten Systemen riskant sein, da viele neue IoT-Gerätehersteller nur über unzureichene Erfahrung bei Softwareentwicklung und Sicherheit verfügen.[1] Diese Risikofaktoren können die Angreifbarkeit eines Unternehmens erhöhen und das Unternehmen zu einem bereitwilligen Ziel für einen Cyberangriff machen.

Trotz der vielen Unbekannten und der daraus resultierenden Datenschutz- und Sicherheitsrisiken des IoT sind etablierte Tools erhältlich, die Führungskräfte für Datenschutz und Sicherheit verwenden können, um diesen Risikofaktoren aktiv zu begegnen. Dieser Artikel zeigt, wie Rahmenwerke, die auf fairen Informationspraktiken (Fair Information Practice Principles, FIPP) basieren,[2] angewendet werden können und stellt praktische Instrumente vor, mit denen Datenschutz- und Sicherheitslösungen in neue IoT-Geräte integriert werden können.

BEWERTUNG VON DATENSCHUTZ UND SICHERHEIT: EIN RAHMENWERK

Auch wenn das IoT sich in ständiger Veränderung und Weiterentwicklung befindet, kann eine Reihe gemeinsamer Grundsätze als Grundlage für Unternehmen dienen, die Datenschutz- und Sicherheitsaspekte bereits frühzeitig bei der Planung und in den Entwicklungsphasen neu angeschlossener Geräte verstehen und verwalten wollen. Eine Reihe von Grundsätzen sind die fairen Informationspraktiken, auf die sich das US-amerikanische Ministerium für Gesundheit, Bildung und Soziales in einem Bericht von 1973 bezieht. Diese Grundsätze wurden 1980 von der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) überarbeitet. Heute dienen diese fairen Informationspraktiken weltweit als Grundlage für verschiedene Datenschutzgesetze, Bestimmungen und Standards.[3]

FIPP-basierte Standards sind weiterhin für Datenschutz- und Sicherheitsexperten bei der Bewertung und Entwicklung ihrer IoT-Programme und -Technologien hilfreich, da diese justitiabel sind und aus risikobezogenen Kontrollen bestehen. Sie können außerdem an die besonderen Merkmale einer bestimmten Branche und die Geschäftsanforderungen eines Unternehmens angepasst werden.

Zwei FIPP-basierte Rahmenwerke sind die allgemein anerkannten Datenschutzgrundsätze (Generally Accepted Privacy Principles, GAPP)[4] und die Sonderveröffentlichung (SP) des US National Institute of Standards and Technology (NIST) 800-53, 4. Ausgabe, *Security and Privacy Controls for Federal Information Systems and Organizations*.[5]

RAHMENWERK 1: GAPP

Das GAPP-Rahmenwerk wurde von einem Team entwickelt, das vom US-amerikanischen Institut der Wirtschaftsprüfer (AICPA) und CPA Canada zusammengestellt wurde. Der Hauptzweck von GAPP ist die Unterstützung der Führungsebene bei der Erstellung eines wirkungsvollen Datenschutzprogramms, das die Pflichten zum Schutz der Privatsphäre, Risiken und Geschäftschancen berücksichtigt. Die 10 Grundsätze und 73 Kontrollkriterien innerhalb von GAPP sind daher als Unterstützung für die Umsetzung und den Nachweis guter Datenschutzmaßnahmen geeignet. Das Rahmenwerk enthält darüber hinaus ein Reifegradmodell, das Unternehmen verwenden können, um ihren Reifegrad zu bewerten.

Die 10 GAPP-Prinzipien sind:

1. **Management**–Das Unternehmen definiert, dokumentiert, kommuniziert und weist Verantwortlichkeiten für seine

Datenschutzrichtlinien und -verfahren zu.
2. **Bekanntmachung**–Das Unternehmen informiert über seine Datenschutzrichtlinien und -verfahren und legt die Zwecke fest, für die personenbezogene Informationen erfasst, verwendet, gespeichert und weitergegeben werden sollen.
3. **Auswahlmöglichkeiten und Zustimmung**–Das Unternehmen beschreibt die für die Betroffenen zur Verfügung stehenden Auswahlmöglichkeiten und holt die implizite oder ausdrückliche Zustimmung hinsichtlich der Erfassung, Verwendung und Weitergabe von personenbezogenen Informationen ein.
4. **Erfassung**–Das Unternehmen darf personenbezogene Informationen nur für die in der Bekanntmachung angegebenen Zwecke erfassen.
5. **Verwendung, Speicherung und Vernichtung**–Das Unternehmen schränkt die Verwendung von personenbezogenen Informationen auf die in der Bekanntmachung angegebenen Zwecke ein sowie auf die Zwecke, der die Person implizit oder ausdrücklich zugestimmt hat. Das Unternehmen speichert personenbezogene Informationen nur so lange wie notwendig, um die angegebenen Zwecke zu erfüllen oder solange dies gesetzlich oder durch eine Verordnung vorgeschrieben ist, und vernichtet diese Informationen anschließend ordnungsgemäß.
6. **Zugriff**–Das Unternehmen ermöglicht den Betroffenen Zugriff auf ihre personenbezogenen Informationen zwecks Überprüfung und Aktualisierung.
7. **Weitergabe an Dritte**–Das Unternehmen gibt personenbezogene Informationen an Dritte nur für die in der Bekanntmachung festgelegten Zwecke und mit der impliziten oder ausdrücklichen Zustimmung der jeweiligen Person weiter.
8. **Datensicherheit**–Das Unternehmen schützt personenbezogene Informationen vor unberechtigtem Zugriff (sowohl physisch als auch logisch).
9. **Qualität**–Das Unternehmen pflegt korrekte, vollständige und relevante personenbezogene Informationen für die in der Bekanntmachung angegebenen Zwecke.
10. **Überwachung und Durchsetzung**–Das Unternehmen überwacht die Einhaltung seiner Datenschutzrichtlinien und -verfahren und verfügt über Verfahren für den Umgang mit Beschwerden und Streitigkeiten in Bezug auf den Datenschutz.

Diese Grundsätze befassen sich nicht nur mit strengen Datenschutzpraktiken, sondern auch mit deren Umsetzung durch das Unternehmen.

RAHMENWERK 2: NIST SP 800-53 ANHANG J

Das NIST beauftragte eine Joint Task Force Transformation Initiative mit der Veröffentlichung von SP 800-53 „Security and Privacy Controls for Federal Information Systems and Organizations“ (Sicherheits- und Datenschutzkontrollen für Regierungsinformationssysteme und Organisationen), die eine Liste mit Sicherheitskontrollen enthält, die die Auswahl von Sicherheitskontrollen für Informationssysteme der US-Regierung unterstützen soll. Im Rahmen dieses größeren Standards wurde der Anhang J „Aufstellung von Datenschutzkontrollen“ entwickelt, um eine Orientierungshilfe für Unternehmen bei der Festlegung und Umsetzung von Datenschutzkontrollen zu geben, die den gesamten Lebenszyklus von personenbezogenen Daten (PII), in Papier- oder in elektronischer Form, betreffen.[6] Diese Kontrollen sind zur Verwendung durch Datenschutzbeauftragte (Chief Privacy Officer, CPO) vorgesehen, die Unternehmen bei der Erfüllung der gesetzlichen oder anderweitig geforderten Datenschutzvorgaben unterstützen. Dies wird teilweise durch eine vereinfachende Darstellung der Anforderungen in einer zentralen Liste erreicht, indem übergreifende Kontrollen, die in verschiedenen Datenschutz -und Sicherheitsanforderungen enthalten sind, einander zugeordnet werden.

Um dies zu erreichen, enthält Anhang J eine strukturierte Liste von Kontrollen über acht Kontrollgruppen. Diese Datenschutzkontrollgruppen sind:

1. **Befugnis und Zweck**–Diese Gruppe stellt sicher, dass Unternehmen:
   - die Rechtsgrundlagen angeben, die zu einer bestimmten Erfassung von personenbezogenen Daten oder einer Aktivität, die sich auf den Datenschutz auswirkt, berechtigen
   - in ihren Bekanntmachungen den Zweck angeben, für den die personenbezogenen Daten erfasst werden.
2. **Verantwortlichkeit, Prüfung und Risikomanagement**–In dieser Gruppe wird das öffentliche Vertrauen durch wirkungsvolle Kontrollen in den Bereichen Verwaltung, Überwachung, Risikomanagement und -bewertung gestärkt, um nachzuweisen, dass das Unternehmen die geltenden Datenschutzanforderungen erfüllt und das allgemeine Datenschutzrisiko minimiert.
3. **Datenqualität und Datenintegrität**–In dieser Gruppe wird das öffentliche Vertrauen dahingehend gestärkt, dass alle

personenbezogenen Daten, die von Unternehmen erfasst und gepflegt werden, korrekt, relevant, aktuell und vollständig sind für den Zweck, für den eine Verwendung vorgesehen ist (siehe öffentliche Bekanntmachungen).

4. **Datenminimierung und Datenvorhaltung**–Diese Gruppe unterstützt Unternehmen bei der Umsetzung der Datenminimierungs- und Vorhaltungsanforderungen zur ausschließlichen Erfassung, Verwendung und Speicherung von personenbezogenen Daten, die für den Zweck, für den sie ursprünglich erfasst wurden, relevant und erforderlich sind. Unternehmen speichern personenbezogene Daten so lange, wie dies für die Zwecke erforderlich ist, die in den öffentlichen Bekanntmachungen angegeben sind, und in Übereinstimmung mit den von der US-amerikanischen Behörde National Archives and Records Administration (NARA) genehmigten Fristen zur Aufbewahrung von Unterlagen.
5. **Individuelle Beteiligung und Abhilfe**–Diese Gruppe zielt auf die Notwendigkeit ab, Einzelpersonen zu aktiven Teilnehmern am Entscheidungsprozess zur Erfassung und Verwendung ihrer personenbezogenen Daten zu machen. Indem Einzelpersonen Zugriff auf ihre personenbezogenen Daten erhalten und die Möglichkeit haben, diese Daten zu korrigieren oder zu ergänzen, sofern erforderlich, stärken die Kontrollen dieser Gruppe das öffentliche Vertrauen bei betrieblichen Entscheidungen, die anhand der personenbezogenen Daten getroffen wurden.
6. **Sicherheit**–Diese Gruppe ergänzt die Sicherheitskontrollen in Anhang F, um zu gewährleisten, dass technische, physische und administrative Sicherheitsmaßnahmen vorhanden sind, um die von den Unternehmen erfassten und gepflegten personenbezogenen Daten vor Verlust, unberechtigtem Zugriff oder Weitergabe zu schützen, und darauf zu achten, dass die Behandlung von Datenschutzvorfällen mit den Richt- und Leitlinien der US-Bundesbehörde OMB übereinstimmen. Die Kontrollen in dieser Gruppe werden in Abstimmung mit dem Informationssicherheitspersonal und gemäß dem vorhandenen NIST-Risikomanagement-Rahmenwerk umgesetzt.
7. **Transparenz**–Diese Gruppe stellt sicher, dass Unternehmen ihre Informationspraktiken und die datenschutzrechtlichen Folgen ihrer Programme und Aktivitäten öffentlich bekannt geben.
8. **Nutzungsbeschränkung**–Diese Gruppe achtet darauf, dass Unternehmen personenbezogene Daten nur so nutzen, wie in den öffentlichen Bekanntmachungen angegeben und auf eine Weise, die konform mit den angegebenen Zwecken oder anderweitig gesetzlich erlaubt ist. Durch die Umsetzung der Kontrollen in dieser Gruppe wird sichergestellt, dass der Nutzungsumfang personenbezogener Daten entsprechend beschränkt ist.

GAPP und NIST SP 800-53 Anhang J basieren auf den fairen Informationspraktiken. Durch ihre Flexibilität und ihren Umfang sind diese Grundsätze zu den vorherrschenden Standards bei der Bewertung von Datenschutz und Sicherheit geworden. Beide Standards sind anpassbar und Unternehmen können diese nutzen, um neue betriebliche Prozesse umzusetzen, oder aber sie werden zur Orientierung für die Integration von Datenschutz- und Sicherheitskontrollen in neue IoT-Produkte und -Systeme verwendet. Beide sind für eine Managementanwendung entwickelt und erleichtern die Umsetzung von Datenschutzanforderungen, da nicht einfach nur Zielvorgaben genannt werden.

Jedes Rahmenwerk hat jedoch auch seine besonderen Stärken. NIST SP 800-53 Anhang J ist dafür vorgesehen, die Einhaltung von verschiedenen übergreifenden US-Bundesgesetzen, Handlungsanweisungen und Anordnungen zu unterstützen und ist somit ein rechtlich orientiertes Rahmenwerk. Während Anhang J ein nützliches Instrument für Unternehmen in vielen verschiedenen Branchen ist, sind die Hauptzielgruppe jedoch Unternehmen, die die Anforderungen der US-Bundesbehörden erfüllen müssen. Der Anhang ist daher am sinnvollsten bei der Umsetzung der IoT-Technologien in Branchen, die insbesondere US-amerikanischen Gesetzen entsprechen müssen. Umgekehrt unterstützen die allgemein anerkannten Datenschutzgrundsätze GAPP nicht die Einhaltung bestimmter Gesetze, sondern basieren eher auf bewährter Praxis auf internationaler Ebene. Sie eignen sich daher besonders für IoT-Technologien, die auf ähnliche Weise international umgesetzt und bei denen geringe Anpassungen für lokale Anforderungen vorgenommen werden sollen.

Die beiden folgenden Fallbeispiele zeigen die Effektivität der Grundsätze der jeweiligen Rahmenwerke bei der Entwicklung innovativer IoT-Produkte.

ANWENDUNGSFALL 1: INTELLIGENTE FAHRZEUGE – GAPP

Für die Automobilindustrie sind vernetzte Autos die Zukunft. Das vernetzte Fahrzeug enthält Technologien, die die Sicherheit für den Menschen erhöhen, Verkehrsstörungen verringern, die Effizienz und Leistung des Fahrzeugs steigern und wertvolle Informationsdienste bieten.[7] Analysten sagen sogar voraus, dass der weltweite Markt für vernetzte Fahrzeuge bis 2020 auf 220 Millionen Autos ansteigen wird.[8]

Auch wenn inzwischen nahezu alle großen Automobilhersteller und Kommunikationsunternehmen in den Markt der vernetzten Fahrzeuge eingestiegen sind, zeigen die Fakten, dass viele Unternehmen weiterhin Produkte entwickeln, die signifikante Datenschutzschwachstellen und Sicherheitslücken aufweisen. US-Senator Ed Markey hat einen Bericht zu den Antworten von 16 großen Herstellern in Auftrag gegeben, der aufzeigte, dass ein deutlicher Mangel an geeigneten Sicherheitsmaßnahmen besteht zum Schutz der Fahrer vor Hackern, die in der Lage wären, die Kontrolle über das Fahrzeug zu übernehmen, oder vor Personen, die personenbezogene

Informationen zum Fahrer zu erfassen und zu verwenden suchen.[9]

Automobilunternehmen haben ihr Bekenntnis zum Datenschutz nachgewiesen. Die Alliance of Automobile Manufacturers Inc. und die Association of Global Automakers entwickelten gemeinsam ein selbstregulierendes Rahmenwerk – Datenschutzgrundsätze für Verbraucher: Datenschutzgrundsätze für Dienste der Fahrzeugtechnik – um diesen Bedenken Rechnung zu tragen. Jedes teilnehmende Unternehmen verpflichtet sich zur Einhaltung der Grundsätze für neue Fahrzeuge spätestens bis zum Modelljahr 2017.[10] Auch wenn die Grundsätze den teilnehmenden Unternehmen als Orientierung bei der Erfüllung der Anforderungen dienen, können die Datenschutzbeauftragten die Kontrollen des GAPP-Rahmenwerks nutzen, um ihre Compliance-Anstrengungen zu unterstützen und künftigen Datenschutz- und Sicherheitsrisiken bereits in den Planungs- und Konstruktionsphasen entgegenzuwirken.

Hintergrund der Fallstudie

Ein Automobilhersteller (das Unternehmen) plant die Entwicklung einer Software, die im eingebauten Navigationssystem des Fahrzeugs installiert werden soll. Die Anwendung wird über Bluetooth in ein Mobilgerät integriert, um die Kontaktadressen des Nutzers mit dem Navigationssystem des Fahrzeugs zu synchronisieren. Das Unternehmen kann für den Prozess der Planung, Entwicklung und Installation der Anwendung auf das GAPP-Rahmenwerk zurückgreifen.

GAPP-Managementprinzip

Das Unternehmen sollte einen Produktmanager benennen, der für den Datenschutz verantwortlich ist und zu Beginn des Projekts eine Auswirkungseinschätzung hinsichtlich des Datenschutzes vornimmt, um die zugehörigen Risiken zu ermitteln. Die Einschätzung basiert dabei auf den erfassten, gespeicherten und übertragenen personenbezogenen Informationen. Der Datenschutzbeauftragte arbeitet eng mit mehreren Abteilungen, einschließlich der Softwareentwicklung, Rechtsabteilung und dem Kundendienst zusammen, um mit den geschäftlichen und gesetzlichen Bestimmungen vertraut zu werden und neue Verpflichtungen zu überwachen, die sich durch Änderungen im geschäftlichen und rechtlichen Umfeld ergeben.

GAPP-Bekanntmachungsprinzip

Dem Unternehmen ist bewusst, dass die Bekanntmachung ein grundlegendes Element bei Datenschutzrechten und -standards ist. Das Team ist sich auch darüber im Klaren, dass das Vornehmen einer Bekanntmachung im Zusammenhang mit vernetzten Geräten schwierig sein kann, da häufig Benutzeroberflächen fehlen oder nur begrenzt vorhanden sind. Eine Bekanntmachung wird jedoch erforderlich, wenn die Datennutzung von den Benutzererwartungen abweicht sowie im Fall von neu definierten Zwecken. Das Unternehmen kann die Bekanntmachung vornehmen, wenn ein Kunde sich erstmals für die Nutzung der Anwendung registriert, oder aber es werden Alternativen verwendet, z. B. eine Website, die Links zur Demonstration und zu Anleitungen der Softwarefunktionen enthält.

GAPP-Prinzip zu Auswahlmöglichkeiten und Zustimmung

Die Unternehmenssoftware funktioniert, indem bestimmte Elemente personenbezogener Daten mit Geo-Positionsdaten integriert werden. Ebenso wie bei der Bekanntmachung sind dem Datenschutzbeauftragten auch hier die Herausforderungen bezüglich der sachgerechten Einholung der Zustimmung bewusst, da Benutzerschnittstellen oft eingeschränkt oder nicht vorhanden sind. Das Unternehmen sollte eventuell verschiedene Serviceebenen für Kunden einrichten, die jeweils auf dem Grad der erteilten Zustimmung basieren. Fahrer könnten beispielsweise auswählen, den aktuellen Standort des Fahrzeugs mit anderen Mitgliedern ihres Netzwerks zu teilen, um eine gegenseitige Sichtbarkeit zu ermöglichen. Alternativ möchte ein Kunde seine Zustimmung vielleicht nur zur Verwendung der statischen Adressdaten geben, die im Gerät gespeichert wurden. Durch Berücksichtigung der unterschiedlichen Anwendungsfälle der Software kann das Unternehmen abgestufte Auswahlmöglichkeiten anbieten, die die Verwendung personenbezogener Informationen einschränken, gleichzeitig jedoch die Funktionalität nicht beeinträchtigen.

GAPP-Erfassungsprinzip

Dem Unternehmen ist bewusst, dass die Datenerfassung im Zusammenhang mit dem Internet der Dinge kritischer ist, da dort die meisten vernetzten Geräte ständig Daten erfassen und verarbeiten. Die Kombination großer Datensätze kann hilfreiches Wissen und Analysen bieten, jedoch kann die Datennutzung mit den ursprünglichen Zwecken der Erfassung unter Umständen eine fehlende Übereinstimmung aufweisen. Das Unternehmen sollte die Datenerfassung auf gesetzlich zulässige Verfahren beschränken und gegenüber dem Kunden Transparenz zeigen, wie personenbezogene Informationen von Dritten erfasst und verarbeitet werden. Darüber hinaus kann das Unternehmen das Risiko einer möglichen Verletzung und die damit verbundene Haftung reduzieren, indem die Datenerfassung nur auf die Elemente beschränkt wird, die für die Funktionalität entscheidend sind. Durch das Einbinden von Kontrollen zur Datenminimierung verringert sich das Risiko im Zusammenhang mit Bekanntmachung, Zustimmung und Speicherung.

GAPP-Prinzip zur Verwendung, Speicherung und Vernichtung

Die Einbindung der Unternehmenssoftware in andere Geräte und Programme kann die Kundenzufriedenheit steigern.

Dennoch sollte das Unternehmen die Verwendung der Daten auf die geschäftlichen Hauptzwecke oder die Fälle beschränken, bei denen der Kunde seine ausdrückliche Zustimmung erteilt hat. Zudem sollte sich der Datenschutzbeauftragte mit anderen Anspruchsgruppen im Unternehmen zu den geschäftlichen und rechtlichen Anforderungen für die Aufbewahrung beraten, damit diese Abteilungen Fristen für die Aufbewahrung von Unterlagen erstellen können. Anschließend setzt der Datenschutzbeauftragte Verfahren um, die das Vernichten der Daten mit Ablauf der Aufbewahrungsfristen sicherstellen. Das Unternehmen könnte z. B. alle von der Software gespeicherten Daten am Ende jeder Fahrt löschen und die Verbindung wiederherstellen, wenn der Fahrer das Fahrzeug das nächste Mal startet. Dadurch kann das Risiko einer Datenschutzverletzung verringert und die Programmfunktionalität verbessert werden. Das Unternehmen sollte regelmäßige Prüfungen durchführen, um die Einhaltung der Richtlinien und -verfahren zu testen.

GAPP-Zugriffsprinzip
Dem Unternehmen sollte bewusst sein, dass von den Kunden ein erlaubter Zugriff auf ihre Daten sowie die Möglichkeit der Aktualisierung sehr positiv aufgenommen werden wird. Die Genauigkeit und Relevanz der Daten, die dem Kunden über die Software angezeigt werden, wird erhöht. Entscheidet sich das Unternehmen dafür, Kundendaten zu speichern, kann dafür ein sicheres Webportal eingerichtet werden, auf das die Kunden zugreifen können, um ihre Daten zu aktualisieren oder zu löschen. Durch die Nutzung unterschiedlicher Technologien kann ein Unternehmen die Beschränkungen der IoT-Geräte umgehen.

GAPP-Prinzip zur Weitergabe an Dritte
Das Unternehmen kann feststellen, dass die Funktionalität der Software zunimmt, wenn eine Integration mit Drittanbietern erfolgt. Durch die Anwendung der GAPP-Prinzipien kann das Unternehmen besser verstehen, wie seine Kundendaten geschützt werden können. Dem Unternehmen ist bewusst, dass für neue Zwecke, für die die Daten vorgesehen sind, die Zustimmung des Kunden erforderlich ist. Der Datenschutzbeauftragte kann außerdem mit einem Rechtsberater zusammenarbeiten, damit gewährleistet ist, dass die entsprechenden Bestimmungen in Verträgen mit Dritten auf der Grundlage der erbrachten Dienstleistungen enthalten sind.

GAPP-Prinzip für Datensicherheit
Das Unternehmen ist sich bewusst, dass bereits in der Planungsphase Sicherheitsmaßnahmen vorgenommen werden müssen, um die Kundendaten während der Erfassung, Speicherung und Weitergabe innerhalb ihres Lebenszyklus zu schützen. Der Datenschutzbeauftragte sollte mit dem Informationssicherheitsteam zusammenarbeiten, um die Kontrollen in die IT-Infrastruktur zu integrieren. Das Unternehmen sollte die Verschlüsselung der Daten in Betracht ziehen, und zwar sowohl bei der Speicherung als auch bei der Übertragung, wenn Informationen vom Gerät an das Fahrzeug und vom Fahrzeug an im Prozess beteiligte Drittanbieter übermittelt werden. Darüber hinaus kann das Unternehmen Zugriffsmanagementlösungen auf Branchenebene einsetzen, die den Zugriff auf personenbezogene Informationen nur für autorisierte und authentifizierte Personen ermöglichen.

GAPP-Qualitätsprinzip
Das Unternehmen bietet seinen Kunden eine Leistung an, die auf dem Angebot von Echtzeitdaten basiert, die korrekt und relevant sein müssen. Es ist entscheidend, dass die erfassten Daten normalisiert sind und mit dem Ursprungsstatus übereinstimmen. Auch wenn der Kunde zunächst die Kontaktinformationen in das Mobilgerät eingibt, kann dennoch das Unternehmen die Datenqualität sicherstellen, indem einheitliche Protokolle und Kontrollen verwendet werden.

GAPP-Prinzip zur Überwachung und Durchsetzung
Das Unternehmen weiß, dass für eine gute Kundenbetreuung Mechanismen erforderlich sind, über die sich der Kunde beteiligen kann. Auch wenn dies nicht nur das Internet der Dinge betrifft, kann das Unternehmen ein Verfahren festlegen, wie Anfragen und Beschwerden zu Datenschutz und Sicherheit angenommen und beantwortet werden sollen. Zudem sollte der Datenschutzbeauftragte für die kontinuierliche Überwachung des Umfeldes in Bezug auf Compliance und neue Geschäftsrisiken verantwortlich sein.

Anwendung von GAPP
Die meisten dieser Prinzipien gelten für IoT-Gerätehersteller oder Softwareentwickler, die Datenschutz- und Sicherheitsmaßnahmen beim Entwicklungsprozess einfließen lassen. GAPP bietet jedoch auch Flexibilität: Sind spezielle Prinzipien, oder selbst Kriterien innerhalb eines Prinzips, für einen bestimmten Entwicklungsfall nicht anwendbar, können diese dokumentiert und aus dem Umfang der Datenschutzbewertung herausgenommen werden.

Auch bei der Erfolgsmessung besteht Flexibilität bei der Einhaltung der durch die GAPP-Prinzipien festgelegten Anforderungen. Das AICPA und CPA Canada schlagen die Verwendung eines Datenschutzreifegradmodells vor, das auf dem Capability Maturity Model (CMM) basiert. Dieses Modell umfasst die folgenden fünf Ebenen: *ad hoc*, definiert, wiederholbar, gesteuert und optimierend. Der entsprechende oder gewünschte Zustand wird vom Unternehmen mit dem Wissen festgelegt, dass die höchste Durchdringungsebene (optimierend) nicht für alle oder noch nicht einmal viele Situationen geeignet sein kann.

GAPP ist ein Instrument, das zur Unterstützung der Geschäftsführung bei der Erstellung eines praktischen und

wirkungsvollen Datenschutzprogramms entwickelt wurde. Anhand der 10 Prinzipien wird ein umfassendes Management-Rahmenwerk festgelegt, das die Risiken reduziert und Unternehmen gleichzeitig dabei hilft, ihren Wettbewerbsvorteil zu erhalten.

ANWENDUNGSFALL 2: VERNETZTE MEDIZINISCHE GERÄTE – NIST SP 800-53

Der Markt vernetzter medizinischer Geräte wächst rasant und eine Analyse sieht voraus, dass der Markt für Geräte zur telemedizinisch unterstützten Patientenbetreuung bis 2020 weltweit auf nahezu 1 Milliarde US $ ansteigen wird.[11] Mit steigender Anzahl von tragbaren Geräten und Überwachungstechnologien steigen jedoch auch die Bedenken im Zusammenhang mit der Erfassung und Speicherung sensibler Patientendaten. Als Folge bleibt das Gesundheitswesen weiterhin angreifbar und ein interessantes Ziel für Cyberangriffe. Tatsächlich gehen jüngste Schätzungen davon aus, dass dem Gesundheitswesen jährlich Kosten in Höhe von bis zu 5,6 Milliarden US $ entstehen, die durch Datenschutzverletzungen verursacht wurden.[12] US-amerikanische Leistungserbringer im Gesundheitswesen unterliegen datenschutz- und sicherheitsrechtlichen Anforderungen gemäß dem US-amerikanischen HIPAA-Gesetz zur Übertragbarkeit und Rechenschaftspflicht im staatlichen Krankenversicherungswesen (Health Insurance Portability and Accountability Act). Daher ist es sehr wichtig, dass Unternehmen ihre Daten und Informationssysteme sichern, um den Zugriff auf diese Systeme zu kontrollieren, Datenschutz- und Sicherheitsrisiken zu verringern und Datenqualität sicherzustellen.[13] Ein Unternehmen kann NIST SP 800-53 Anhang J aktiv einsetzen, um die Compliance-Anforderungen nach HIPAA zu erfüllen. Und bei der Bewertung neuer Informationsmanagementsysteme und anderer verbundener Geräte kann damit die Einbindung geeigneter Datenschutz- und Sicherheitskontrollen sichergestellt werden.

Die folgenden Kontrollen spiegeln die Notwendigkeit wider, den Datenschutz während des gesamten Informationslebenszyklus zu wahren: von der Datenerfassung über Verarbeitung und Wartung bis zur Datenfreigabe und Datenvernichtung. Das mit jedem Kontrollbereich verbundene Risiko wird daher durch die Art und Verarbeitung der betreffenden personenbezogenen Daten bestimmt.

Hintergrund der Fallstudie

Zur Senkung der Gesundheitskosten und zur Verbesserung der Servicequalität möchte ein Gesundheitsanbieter für die US-amerikanischen Kriegsveteranen (das Unternehmen) das Informationsmanagement seines Gesundheitswesens (Health Care Information Management, HIM) aktualisieren, um den exponentiellen Anstieg der eingegangenen Daten von medizinischen IoT-Geräten verwalten zu können. Geräte für die Gesundheitsüberwachung, die zu Hause eingesetzt werden, übertragen z. B. Vitalzeichen wie Blutdruck und Herzfrequenz und können auch Symptome im Zusammenhang mit Diabetes, Bluthochdruck, Asthma und anderen Krankheiten messen. Tragbare Geräte können einen Notfalldienst aktivieren, sofern erforderlich, während Fitnessbänder Informationen zur sportlichen Betätigung im Laufe des Tages liefern (z. B. gelaufene Stufen, Kalorienverbrauch). Das technische Personal im Gesundheitswesen weiß, dass es verschiedene Datenschutz- und Sicherheitsanforderungen gibt und versucht die entsprechenden Kontrollen vorzugsweise in den Planungs- und Entwicklungsphasen umzusetzen.

Genehmigung zur Erfassung

Das Unternehmen benötigt die Erfassung sensibler Datenelemente, um eine qualitativ hochwertige und zeitgerechte Versorgung gegenüber seinen Patienten zu erbringen. Während die Anforderungen für das Sammeln von Informationen für das neue HIM-System überprüft werden, sollte das technische Personal eine Datenschutzrisikobewertung durchführen, um die Risiken aufzuzeigen, die bei der Erfassung von bestimmten Daten auftreten, sowie die Kategorien der Informationen dokumentieren, die in der Datenschutzerklärung an die Patienten übermittelt werden.

Verantwortlichkeit, Prüfung und Risikomanagement

Das Unternehmen benennt einen Datenschutzbeauftragten, der eine Auswirkungseinschätzung hinsichtlich des Datenschutzes und eine Risikobewertung vornimmt, um die Risiken für personenbezogene Informationen aufzuzeigen, wenn ein neues HIM-System eingesetzt wird. Dieser Beauftragte und das technische Team sind sich darüber bewusst, dass sie Systeme mit automatisierten Datenschutzkontrollen entwickeln sollten, die Risiken reduzieren und die Wahrscheinlichkeit einer Datenschutzverletzung verringern. Dieser Schritt ist sehr wichtig, weil eine spätere Integration des Datenschutzes und der Sicherheit extrem aufwendig und teuer ist. Durch die Entwicklung automatisierter Kontrollen im System kann das Unternehmen seine Überwachungs- und Informationspflichten effizienter erfüllen und erhöht gleichzeitig seine Datensicherheit.

Datenqualität und Datenintegrität

Das Unternehmen ist sich bewusst, dass die Pflege korrekter Daten im Gesundheitsbereich über Leben und Tod entscheiden kann. Wenn Ärzte, Krankenschwestern und medizinische Fachkräfte mit veralteten Daten arbeiten, verschreiben sie möglicherweise falsche Medikamente, die zum Tod eines Patienten führen können. Der Datenschutzbeauftragte sollte Kontrollen bewerten, die zur Sicherstellung der Genauigkeit und Validität der Daten bei der Eingabe in das HIM-System ausgelegt sind. Darüber hinaus wird die Qualitätssicherung noch entscheidender, wenn an das System verschiedene vernetzte

Geräte angeschlossen werden, die Daten in unterschiedlichen Formaten speichern und übertragen.

Datenminimierung und Datenvorhaltung
Auch wenn Unternehmen im Gesundheitswesen geschäftliche Begründungen für die Erfassung der meisten Arten von sensiblen Daten haben, ist sich das Unternehmen bewusst, dass das Risiko einer Datenschutzverletzung reduziert werden kann, wenn die Datenerfassung nur auf die tatsächlich notwendigen Daten beschränkt wird und sensible Datensätze mit Ablauf der Speicherfristen vernichtet werden. Darüber hinaus kann sich der Datenschutzbeauftragte mit verschiedenen Abteilungen abstimmen, um die spezifischen Geschäftsanforderungen für eine verlängerte Datenspeicherung zu ermitteln. Auch wenn das Unternehmen bestimmte Daten zu Testzwecken speichert, kann der Datenschutzbeauftragte Techniken zur De-Identifikation und Aggregation prüfen, um Datenschutz- und Sicherheitsrisiken zu reduzieren. Die technischen Mitarbeiter des Unternehmens können Kontrollen mitentwickeln, um sensible Datenelemente zu markieren und Patientenaufzeichnungen zu anonymisieren. So können die Prozesse der Datenminimierung und der Unterlagenvernichtung besser unterstützt werden.

Individuelle Beteiligung und Abhilfe
Auch wenn Leistungserbringer im Gesundheitswesen geschützte Gesundheitsinformationen mit gewissen Einschränkungen weitergeben dürfen, z. B. aus Gründen, die im Zusammenhang mit Behandlung, Zahlung und Betrieb stehen, sollte dem Unternehmen bewusst sein, dass die Zustimmung und der Zugriff des Patienten grundlegende Konzepte bei der Entscheidungsfindung sind.[14] Das Unternehmen baut gegenüber seinen Patienten Vertrauen auf, wenn es den Patienten Kontrolle über ihre Informationen gibt und diesen erlaubt, die Unterlagen zu aktualisieren. Gleichzeitig wird dadurch die Datenqualität und -genauigkeit verbessert. Der Datenschutzbeauftragte sollte sicherstellen, dass Kundenportale und andere verbundene Geräte, die eine Schnittstelle mit dem HIM-System aufweisen, den Zugriff und eine gewisse Kontrolle über die Datensätze ermöglichen.

Sicherheit
Um personenbezogene Informationen über den gesamten Datenlebenszyklus wirkungsvoll zu sichern, muss das Unternehmen die unterschiedlichen Datenflüsse unbedingt dokumentieren. Bei der Entwicklung des HIM-Systems sollte der Datenschutzbeauftragte die unterschiedlichen vor- und nachgeschalteten Systeme und Anwendungen, die in diesen Systemen enthaltenden Datenelemente sowie die unterschiedlichen Datenelemente ermitteln, die von einem System auf ein anderes übertragen wurden. Dann kann der Datenschutzbeauftragte mit dem Informationssicherheitsteam zusammenarbeiten, um zu gewährleisten, dass die unterschiedlichen Systeme das jeweils erforderliche Sicherheitsniveau zugeordnet bekommen, welches anhand der Sensibilität der Daten bestimmt wurde.

Transparenz
Das Unternehmen erfasst Daten von angeschlossenen Geräten, die in das HIM-System integriert sind. Das Unternehmen sollte dafür seinen Patienten die Art der Informationen bekanntgeben, die über diese verbundenen Geräte erfasst, verarbeitet, gespeichert und übertragen werden. Wenn die tragbare Technologie über begrenzte Benutzerschnittstellen verfügt, sollte der Datenschutzbeauftragte Alternativen erwägen, um die Bekanntmachung bei diesen Geräten vorzunehmen. Das Unternehmen könnte z. B. eine Datenschutzerklärung auf einem Webportal veröffentlichen, auf das Patienten zugreifen und über das sie personenbezogene Informationen eingeben können.

Nutzungsbeschränkung
Das Unternehmen weiß, wie wichtig das Vertrauen des Patienten in die Arzt-Patienten-Beziehung ist. Der Datenschutzbeauftragte sollte Kontrollen und Überprüfungen einbinden, die die Zugriffsmöglichkeiten und Verwendungsmöglichkeiten der Informationen für neue und sekundäre Zwecke einschränken, für die die Zustimmung des Patienten nicht vorliegt. Das HIPAA-Gesetz erlaubt jedoch den Austausch bestimmter Aufzeichnungen mit anderen relevanten Einrichtungen und Geschäftspartnern, wenn die Datentransaktionen über Prüfprotokollverfahren innerhalb des HIM-Systems verfolgt werden, sowie wenn die laufende Überwachung von Datenfreigabe und Benutzerzugriff unterstützt wird.

Anwendung von Anhang J
Dieser Standard wurde entwickelt, um die wirkungsvolle Einhaltung von Datenschutzanforderungen während des gesamten Informationsmanagementzyklus zu unterstützen. Obwohl NIST SP 800-53 Anhang J nicht alle US-Gesetze berücksichtigt, insbesondere nicht diejenigen zur Lenkung von bestimmten Datentypen wie Gesundheitsinformationen, können diese zusätzlichen Gesetze in die entsprechenden Phasen des vorhandenen Rahmenwerks ganz einfach eingebunden werden. Eine entsprechende Übereinstimmung mit den Kontrollen hängt auch von zusätzlichen Anforderungen ab, die gelten können. Außerdem entscheidet sich das Unternehmen vielleicht dafür, optionale Kontrollerweiterungen umzusetzen, wenn die Notwendigkeit dafür nachgewiesen wurde.

NIST SP 800-53 Anhang J gilt für verschiedene Anwendungsfälle, um das Unternehmen beim Ausbau seines Datenschutzprogrammes zu unterstützen. Der Datenschutzbeauftragte kann das Kontrollrahmenwerk nutzen, wenn eine übergreifende Verwaltungsstruktur eingerichtet wird und wenn neue IoT-Systeme und Anwendungen in der Umgebung eingesetzt werden sollen. Das Unternehmen kann

die Kontrollen anhand betrieblicher Bedürfnisse anpassen, das Rahmenwerk bietet jedoch eine Reihe von Richtlinien, um den Datenschutz in die Umgebung einzubinden.

FAZIT

Das Internet der Dinge (IoT) steht für eine große und unvorhersehbare Veränderung, wie Daten künftig erfasst, verarbeitet, gespeichert und analysiert werden. Neue Technologien werden die Art der Geschäftsführung von Unternehmen und die Interaktion mit Kunden und anderen Unternehmen deutlich verbessern. In diesem Sinne ist das IoT sehr vielversprechend, birgt jedoch gleichzeitig auch Risiken für Datenschutz und Sicherheit, z. B. bei der Erfassung und Verarbeitung von Daten für andere Zwecke als ursprünglich festgelegt. Es liegt ein verstärktes Risiko im Zusammenhang mit unsicheren Geräten und Datenquellen, die viele Angriffsmöglichkeiten bieten, vor. Um sich diesen Fragen und Herausforderungen zu stellen, müssen Unternehmen Datenschutz- und Sicherheitsmaßnahmen von Beginn an einbinden, wenn neue vernetzte Technologien angebunden, entwickelt und eingesetzt werden sollen.

Die fairen Informationspraktiken (FIPP) bilden die Grundlagen für viele umfassende risiko- und kontrollbasierte Datenschutzrahmenwerke. Unternehmen können FIPP-basierte Rahmenwerke nutzen, darunter GAPP und NIST SP 800-53 Anhang J, um die Datenschutz- und Sicherheitsfragen zu bewerten, die durch neue IoT-Geräte entstehen. Ferner liefern die Rahmenwerke Unterstützung bei der Entwicklung und Integration sicherer Technologien und bei der Verringerung des gesamten Risikoniveaus. Auch wenn das Internet der Dinge die Art und Weise verändert, wie Daten erfasst, verarbeitet und verwendet werden, enthalten die FIPP dennoch relevante Richtlinien für Unternehmen, um Datenschutz und Sicherheit aktiv bei der Entwicklung neuer IoT-Geräte zu berücksichtigen.

FUSSNOTEN

[1] *The Economist*, „Their Own Devices“, 18. Juli 2015, *www.economist.com/news/science-and-technology/21657766-nascent-internet-things-security-last-thing-peoples*

[2] US-amerikanisches Ministerium für Gesundheit , Bildung und Soziales (Department of Health, Education and Welfare), *Records Computers and the Rights of Citizens*, USA, Juli 1973

[3] Gellman, R., „Fair Information Practices: A Basic History“, 31. Dezember 2008, *http://bobgellman.com/rg-docs/rg-FIPShistory.pdf*

[4] American Institute of Certified Public Accountants and CPA Canada, „Generally Accepted Privacy Principles“, März 2011, *www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/PRIVACY/GENERALLYACCEPTEDPRIVACYPRINCIPLES/Pages/default.aspx*

[5] National Institute of Standards and Technology, Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, USA, 30. April 2013, Anhang J

[6] *Ibid.*, S. J-1

[7] Auto Alliance, „Auto Issues–Automakers Believe that Strong Consumer Data Privacy Protections are Essential to Maintaining the Trust of Our Customers“, 13. November 2014, *www.autoalliance.org/index.cfm?objectid=46DD7290-68FD-11E4-866D000C296BA163*

[8] Greenough, J.; „The ‘Connected Car’ Is Creating a Massive New Business Opportunity for Auto, Tech, and Telecom Companies“, *Business Insider*, 19. Februar 2015, *www.businessinsider.com/connected-car-statistics-manufacturers-2015-2*. Hinweis: Die Definition von „vernetzten Fahrzeugen“, die in dieser Studie verwendet wird, lautet: „mit der notwendigen Hardware ausgerüstet, um mit dem Internet verbunden werden zu können“.

[9] Markey, E., „Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk“, Februar 2015, *www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf*

[10] *Op cit*, Auto Alliance

[11] Transparency Market Research, „Remote Patient Monitoring Devices Market—Global Industry Analysis, Size, Share, Growth, Trends and Forecast, 2014–2020“, Juni 2015, *www.pharmiweb.com/pressreleases/pressrel.asp?ROW_ID=117619#.VahJ0vlVgli#ixzz3g6TRMnS2*

[12] Ponemon Institute, „Fourth Annual Benchmark Study on Patient Privacy & Data Security“, 12. März 2014, *www.ponemon.org/blog/fourth-annual-benchmark-study-on-patient-privacy-and-data-security*

[13] Kongress, Health Insurance Portability and Accountability Act von 1996, (Veröffentl. L. 104–191), USA, 21. August 1996

[14] US-amerikanisches Gesundheitsministerium (Department of Health and Human Services), „Uses and Disclosures for Treatment, Payment, and Health Care Operations“, 45 CFR 164.506, USA, 3. April 2003, *www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/sharingfortpo.pdf*