Sicheres Internet of Things (IoT) mit AWS

Sichere Cloud-Einführung

April 2019

Mitteilungen

Dieses Dokument dient lediglich zu Informationszwecken. Es stellt die aktuellen Produktangebote und -praktiken von AWS ab dem Datum der Ausstellung dieses Dokuments dar, welche ohne vorherige Ankündigung geändert werden können. Kunden sind dafür verantwortlich, ihre eigene, unabhängige Bewertung der Informationen in diesem Dokument und jede Nutzung der Produkte oder Services von AWS durchzuführen, die jeweils im vorliegenden Fall ohne Gewährleistung jeglicher Art, sei es ausdrücklich oder stillschweigend, bereitgestellt werden. Dieses Dokument schafft keine Garantien, Erklärungen, vertraglichen Verpflichtungen, Bedingungen oder Zusicherungen von AWS, seinen verbundenen Unternehmen, Lieferanten oder Lizenzgebern. Die Verantwortlichkeiten und Verbindlichkeiten von AWS gegenüber seinen Kunden werden durch AWS-Vereinbarungen gesteuert, und dieses Dokument ist weder Bestandteil einer Vereinbarung zwischen AWS und seinen Kunden noch ändert es sie.

Inhalt

Contents

Zweck

Dieses Whitepaper gibt einen detaillierten Überblick über die sicherheitsrelevanten IoT-Services (Internet of Things), die Kunden in der AWS-Cloud nutzen können. Dieses Dokument richtet sich an Senior-Programmverantwortliche, Entscheidungsträger und Sicherheitsexperten, die die sichere Einführung von IoT-Lösungen in Unternehmen in Erwägung ziehen.

Hintergründe

IoT-Technologie ermöglicht Unternehmen, Prozesse zu optimieren, Produktangebote zu verbessern und Kundenerlebnisse auf vielfältige Weise zu transformieren. Zwar sind Führungskräfte von der Art und Weise begeistert, wie ihre Unternehmen von dieser Technologie profitieren können, aber Sicherheits-, Risiko- und Datenschutzbedenken bleiben weiterhin bestehen. Dies ist zum Teil auf den Konflikt mit ungleichen, inkompatiblen und manchmal unausgereiften Sicherheitsangeboten zurückzuführen, die Bereitstellungen nicht ordnungsgemäß absichern, was wiederum zu einem erhöhten Risiko für Kunden- oder Geschäftseigentümerdaten führt.

Unternehmen sind bestrebt, intelligente Services anzubieten, die die Lebensqualität der Bevölkerung, Geschäftsabläufe und -analytik, die Qualität der Versorgung durch Dienstleister, die Stabilität von Smart Cities, die ökologische Nachhaltigkeit und eine Vielzahl von Szenarien, die noch nicht vorstellbar sind, drastisch verbessern können. In jüngster Zeit hat AWS eine Zunahme der IoT-Akzeptanz aus dem Gesundheitswesen und Gemeinden verzeichnet, wobei in naher Zukunft weitere Branchen folgen dürften. Viele Gemeinden sind Early Adopters und übernehmen bei der Integration moderner Technologien wie IoT die Vorreiterrolle. Einige Beispiele:

- **Kansas City, Missouri:** Kansas City hat eine einheitliche Smart-City-Plattform geschaffen, um neue Systeme entlang des KC- Straßenbahnkorridors zu verwalten. Videosensoren, Fahrbahnsensoren, vernetze Straßenleuchten, ein öffentliches WiFi-Netzwerk, sowie Parkraum- und Verkehrsmanagement haben eine 40% ige Senkung der Energiekosten, die Neuentwicklung der Innenstadt im Wert von1,7 Milliarden US-Dollar und 3.247 neue Wohneinheiten ermöglicht.
- **Stadt Chicago, Illinois:** Chicago installiert Sensoren und Kameras in Kreuzungen, um Pollenzahl und Luftqualität für seine Bürger zu erkennen.
- **Stadt Catania, Italien:** Catania entwickelte eine Anwendung, um Pendler wissen zu lassen, wo sich der nächste, offene Parkplatz auf dem Weg zu ihrem Ziel befindet.
- **Stadt Recife, Brasilien:** Recife verwendet Tracking-Devices, die auf jedem Abfall-LKW und Reinigungswagen platziert sind. Die Stadt senkte die Reinigungskosten um 250.000 US-Dollar pro Monat und verbesserte gleichzeitig die Zuverlässigkeit und die Betriebseffizienz.
- **Stadt Newport in Wales, Vereinigtes Königreich:** Newport hat Smart City IoT-Lösungen eingesetzt, um die Luftqualität, den Hochwasserschutz und die Abfallwirtschaft in nur wenigen Monaten zu verbessern.
- **Jakarta, Indonesien:** Als Stadt mit 28 Millionen Einwohnern, die sich oft mit Überschwemmungen befasst, nutzt Jakarta das IoT, um Wasserspiegel in Kanälen und Tiefland zu überwachen und nutzt soziale Medien, um die Meinung der Bürger zu verfolgen. Jakarta ist auch in der Lage, Frühwarnung und Evakuierungen in möglicherweise betroffenen Gegenden bereitzustellen, sodass die Regierung und Ersthelfer wissen, in welchen Gebieten Hilfe am meisten benötigt wird, und somit der Evakuierungsprozess besser koordiniert werden kann.

Laut Machina Research wird der globale IoT-Markt bis 2024 4,3 Billionen US-Dollar erreichen.[1] Gemäß dem Bericht des britischen *Department for Business Innovation and Skills* wird der globale Markt für Smart City-Lösungen und zusätzliche Services, die erforderlich sind, um diese zu implementieren, bis 2020 auf 408 Milliarden Dollar geschätzt.[2] Darüber hinaus schätzt Forbes[3], dass »vorausschauende Wartung, selbstoptimierende Produktion und automatisiertes Bestandsmanagement die drei wichtigsten Anwendungsfälle sind, die das Wachstum des IoT-Marktes bis 2020 vorantreiben«. Forbes behauptet, dass Unternehmen etablierte und ausgereifte IT-Anbieter mit zuverlässiger Infrastruktur beim Aufbau oder der Implementierung von IoT-Lösungen nutzen wollen, da große Auswirkungen auf die Kunden bestehen.

Während Kunden bestrebt sind, geschäftliche Möglichkeiten durch das IoT zu nutzen, war in der Vergangenheit die sichere Einführung des IoTs unklar. Features und Services, die Lösungen ermöglichen, waren nicht immer standardmäßig sicher und hinterließen potenzielle Sicherheitslücken in den Architekturgrundlagen. Darüber hinaus erfolgten Aktualisierungen und Wartungen bei Hauptstrategien nicht automatisch, wie beispielsweise verschlüsselte Kommunikation und OTA-Updates (Over-the-Air). Nur wenige Anbieter unterstützten die Möglichkeit, dass Devices und Gateways nach der Bereitstellung per Fernzugriff gepatcht werden können, dadurch waren die Devices für neue Sicherheitsrisiken anfällig.

Im Gegensatz dazu, nimmt AWS Sicherheit sehr ernst und unterstützt Millionen aktiver Kunden aus einer Vielzahl von Branchen und Regionen mit unterschiedlichen Anforderungen an die Datensensibilität und Vertraulichkeit. AWS investiert erhebliche Ressourcen, um sicherzustellen, dass die Sicherheit in jede Ebene unserer Services integriert ist und erweitert diese Sicherheit auf Devices mit IoT. AWS hat Priorität, die Vertraulichkeit, Integrität und Verfügbarkeit von Kundensystemen und Daten zu schützen und gleichzeitig eine sichere und skalierbare Plattform für IoT-Lösungen bereitzustellen.

Sicherheitsherausforderungen

Sicherheitsrisiken und Schwachstellen haben das Potenzial, die Sicherheit und den Datenschutz von Kundendaten in einer IoT-Anwendung zu gefährden. In Verbindung mit der wachsenden Anzahl von Devices und den erzeugten Daten wirft das Schadenspotenzial Fragen auf, wie man mit Sicherheitsrisiken, durch IoT-Devices und Kommunikation der Devices zur und aus der Cloud heraus, umgehen kann.

Häufige Kundenbedenken, in Bezug auf Risiken, sind die Sicherheit und Verschlüsselung von Daten während der Übertragung zur und von der Cloud, oder während der Übertragung von Edge-Services zum und vom Device, das Patchen von Devices, die Device- und Benutzerauthentifizierung, sowie die Zugriffskontrolle. Die Sicherung von IoT-Devices ist unerlässlich, nicht nur um die Datenintegrität aufrechtzuerhalten, sondern auch vor Angriffen zu schützen, die die Zuverlässigkeit von Devices beeinträchtigen können. Da Devices große Mengen an sensiblen Daten über das Internet senden können und Endbenutzer die Möglichkeit haben, ein Device direkt zu steuern, muss die Sicherheit von »Dingen« jede Ebene der Lösung durchdringen.

[1] Per https://machinaresearch.com/news/the-global-iot-market-opportunity-will-reach-usd43-trillion-by-2024.
[2] Siehe https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/249423/bis-13-1217 - smart-city-market-opportunties-uk.pdf.
[3] Siehe https://www.forbes.com/sites/louiscolumbus/2017/01/29/internet-of-things-market-to-reach-267b-by - 2020 / #74c8f8c7609b.

Nachrichten über den Datenkompromiss bringen die IoT-Sicherheit unter zusätzliche Beobachtung der Kunden, bieten Erkenntnisse und fördern bessere Praktiken. Die Grundlage einer IoT-Lösung sollte mit Sicherheit beginnen und enden, zusammen mit der Verwendung von Diensten, die IoT-Konfigurationen kontinuierlich überwachen können[4], um sicherzustellen, dass sie nicht von den bewährten Sicherheitsmethoden abweichen. Sobald eine Abweichung erkannt wird, müssen Warnmeldungen ausgelöst werden, um geeignete Korrekturmaßnahmen einzuleiten - idealerweise automatisch.

Um mit dem Eintrag von Devices auf dem Markt, sowie den online kommenden Bedrohungen, Schritt zu halten, ist es am besten, Dienste zu implementieren, die jeden Teil des IoT-Ökosystems adressieren und sich in ihrer Fähigkeit zu sichern und zu schützen, zu auditieren und zu sanieren sowie Fleet-Deployments von IoT-Devices zu verwalten (mit oder ohne Verbindung zur Cloud).

Wie gehen Regierungen auf IoT-Sicherheit ein?

Während privatwirtschaftliche Organisationen das IoT aktiv in Anwendungsfällen wie Gesundheitswesen, Industriebau und Konsumgütern mit geringem Stromverbrauch einsetzen, beginnen Regierungen auf nationaler und lokaler Ebene, sich mit der Einführung und Sicherheit des IoT zu befassen (siehe Anlage 2). Zusätzlich zur Bewertung der zukünftigen Richtlinienlandschaft des IoT fügt AWS weiterhin Dienstleistungen zu verschiedenen Compliance-Frameworks hinzu, um Kunden bei der Erfüllung ihrer Compliance-Verpflichtungen zu unterstützen (siehe Anlage 3).

AWS IoT-Services und Sicherheitsfunktionen

AWS bietet eine Reihe von IoT-Services, mit denen Kunden ihre Devices, Konnektivität und Daten schützen können. Diese Services ermöglichen es Kunden, die End-to-End-Sicherheit, vom Device-Schutz bis hin zu Daten, während der Übertragung und im Ruhezustand zu nutzen. Außerdem bieten sie Sicherheitsfunktionen, welche die Anwendung und Ausführung von Sicherheitsrichtlinien ermöglichen, die zum Erreichen des Security Watermark erforderlich sind.

AWS IoT bietet eine umfassende Funktionalität; Kunden können IoT-Lösungen für virtuell jeden Anwendungsfall über eine breite Palette von Devices aufbauen. AWS IoT lässt sich mit Services für künstliche Intelligenz (KI) integrieren, sodass Kunden die Intelligenz der Devices steigern können - auch ohne Internetverbindung. Basierend auf der Nutzung der AWS-Cloud und von Millionen von Kunden in 190 Ländern, kann AWS IoT problemlos skaliert werden, wenn die Device-Fleets der Kunden wachsen und sich ihre Geschäftsanforderungen weiterentwickeln. AWS IoT bietet außerdem umfassende Sicherheitsfunktionen, damit Kunden vorbeugende Sicherheitsrichtlinien erstellen und sofort auf potenzielle Sicherheitsprobleme reagieren können.

AWS IoT bietet Cloud-Services und Edge-Software, die es Kunden ermöglichen, Devices sicher zu verbinden, Daten zu sammeln und intelligente Maßnahmen lokal durchzuführen, selbst wenn die Internetverbindung ausfällt. Cloud-Services ermöglichen es Kunden, große und vielfältige Fleets schnell einzuführen und sicher zu verbinden, den Zustand der Fleet aufrechtzuerhalten, die Sicherheit der Fleet zu bewahren, und Events über IoT-Sensoren und -anwendungen hinweg, zu erkennen und darauf zu reagieren. Um die Entwicklung von IoT-Anwendungen zu beschleunigen, können Kunden Devices und Webdienste einfach über eine Drag-and-Drop-Schnittstelle verbinden. AWS IoT kann auch verwendet werden, um Daten zu analysieren und ausgefeilte Machine Learning-Modelle (ML) zu erstellen. Diese Modelle können in der Cloud oder auf Kundendevices bereitgestellt werden, um Intelligenz der Devices zu steigern.

[4] Bei einer Konfiguration handelt es sich um eine Reihe von technischen Steuerungen, die Kunden festlegen, um Informationen sicher zu halten, wenn Devices miteinander und mit der Cloud zu kommunizieren.

Während die momentanen AWS IoT-Services[5] sehr umfangreich sind, um innovative und umfassende IoT-Lösungen zu ermöglichen, konzentriert sich dieses Whitepaper auf die folgenden fünf Services, die für die IoT-Sicherheit grundlegend sind. Service-Beschreibungen und Sicherheitsfunktionen werden nachfolgend erläutert.

- ***Amazon FreeRTOS*** ist ein Open-Source-Betriebssystem für Mikrocontroller, mit dem kleine Devices mit geringem Stromverbrauch programmiert, bereitgestellt, gesichert, verbunden und verwaltet werden können.
- ***AWS IoT Greengrass*** ist eine Software, mit der Kunden lokale Rechen-, Messaging-, Daten-Caching-, Synchronisierungs- und ML-Inferenzfunktionen auf verbundenen Devices ausführen können.
- ***AWS IoT Core*** ist ein verwalteter Cloud-Service, mit dem verbundene Devices einfach und sicher mit Cloud-Anwendungen und anderen Devices interagieren können.
- ***AWS IoT Device Management*** ist ein cloudbasierter Device-Management-Service, mit dem IoT-Devices problemlos installiert, organisiert, überwacht und remote verwaltet werden können.
- ***AWS IoT Device Defender*** ist ein IoT-Sicherheitsdienst, der die IoT-Konfigurationen von Kunden überwacht, um sicherzustellen, dass sie nicht von bewährten Sicherheitsmethoden abweichen.

Amazon FreeRTOS — Device Software

Serviceübersicht: *Amazon FreeRTOS* (a: FreeRTOS) ist ein Open-Source-Betriebssystem für Mikrocontroller,[6] mit dem kleine, energiesparende Edge-Devices einfach programmiert, bereitgestellt, gesichert, verbunden und verwaltet werden können. *Amazon FreeRTOS* basiert auf dem FreeRTOS Kernel, einem beliebten Open-Source-Betriebssystem für Mikrocontroller, und erweitert es um Softwarebibliotheken, die es ermöglichen, kleine, energiesparende Devices von Kunden zu sichern und direkt mit AWS zu verbinden, oder leistungsfähigere Edge-Devices mit AWS IoT Greengrass.

Sicherheitsfunktionen: *Amazon FreeRTOS* wird mit Bibliotheken geliefert, um Devicedaten und -verbindungen zu schützen, einschließlich Unterstützung für Datenverschlüsselung und Schlüsselverwaltung. *Amazon FreeRTOS* bietet Unterstützung für Transport Layer Security (TLS v1.2), um Devices sicher mit der Cloud zu verbinden. *Amazon FreeRTOS* verfügt außerdem über eine Code-Signaturfunktion, um sicherzustellen, dass der Devicecode des Kunden während der Bereitstellung nicht beeinträchtigt wird, sowie Funktionen für OTA- Device-Updates mit Erweiterungen oder Sicherheits-Patches.

[5] AWS IoT-Services umfassen Amazon FreeRTOS, AWS IoT Greengrass, AWS IoT Core, AWS IoT Device Management, AWS IoT Device Defender, AWS IoT Things Graph, AWS IoT Analytics, AWS IoT SiteWise und AWS IoT Events. Weitere Informationen sind unter https://aws.amazon.de/iot zu finden.

[6] Ein Mikrocontroller ist ein einzelner Chip, der einen einfachen Prozessor enthält, der in vielen Devices zu finden ist, darunter Küchengeräte, Fitness-Tracker, Sensoren für die industrielle Automatisierung und Autos. Viele dieser kleinen Devices könnten von der Verbindung mit der Cloud oder lokal mit anderen Devices profitieren. Zum Beispiel müssen intelligente Stromzähler eine Verbindung zur Cloud herstellen, um über die Nutzung zu berichten, und Gebäudesicherheitssysteme müssen lokal kommunizieren, damit sich eine Tür öffnet, wenn jemand sein Badge verwendet.

AWS IoT Greengrass - Software für Edge-Computing

Serviceübersicht: *AWS IoT Greengrass* ist eine Software, mit der Kunden lokale Rechen-, Messaging-, Daten-Caching-, Synchronisierungs- und ML-Inferenzfunktionen für angeschlossene Devices ausführen können, sodass verbundene Devices[7] auch mit intermittierender Verbindung zur Cloud betrieben werden können. Sobald das Device wieder eine Verbindung hergestellt hat, synchronisiert *AWS IoT Greengrass* die Daten auf dem Device mit *AWS IoT Core* und bietet konstante Funktionalität unabhängig von der Verbindung. *AWS IoT Greengrass* erweitert AWS nahtlos auf Devices, sodass sie lokal auf die von ihnen erzeugten Daten reagieren können, während sie die Cloud für Management, Analysen und dauerhafte Speicherung nutzen.

Sicherheitsfunktionen: *AWS IoT Greengrass* authentifiziert und verschlüsselt Devicedaten, sowohl für lokale Kommunikation, als auch für die Kommunikation der Cloud. Daten werden nie ohne nachgewiesene Identität zwischen Devices und der Cloud ausgetauscht. Der Service verwendet Sicherheits- und Zugriffsmanagement, ähnlich dem, was Kunden von *AWS IoT Core* her kennen. Beispielsweise die gegenseitige Device-authentifizierung und –autorisierung, sowie eine sichere Verbindung zur Cloud.

Insbesondere verwendet *AWS IoT Greengrass* X.509[8] Zertifikate, verwaltete Abonnements, AWS IoT-Richtlinien und *AWS Identity and Access Management* (IAM) Richtlinien und Rollen, um sicherzustellen, dass *AWS IoT Greengrass*-Anwendungen tatsächlich sicher sind. AWS IoT-Devices erfordern ein *AWS IoT Thing*, ein Device Certificate und eine AWS IoT-Richtlinie, um eine Verbindung mit dem *AWS IoT Greengrass*-Service herzustellen. Dies ermöglicht *AWS IoT Greengrass*-Core-Devices, eine sichere Verbindung mit dem AWS IoT-Cloud-Service herzustellen. Darüber hinaus kann der *AWS IoT Greengrass* Cloud-Service, Konfigurationsinformationen, AWS Lambda-Funktionen und verwaltete Abonnements für *AWS IoT Greengrass* Core-Devices bereitstellen. Des Weiteren bietet *AWS IoT Greengrass*, Hardware-Root of Trust Private Key Storage für Edge-Devices.

Weitere wichtige Sicherheitsfunktionen von *AWS IoT Greengrass* sind die Überwachung und das Logging. Die Core-Software im Service kann beispielsweise Logs in *Amazon CloudWatch*[9] (die auch für AWS IoT Core funktioniert) und in das lokale Dateisystem der Core-Devices des Kunden schreiben. Logging wird auf Gruppenebene und auf allen AWS IoTs konfiguriert. Alle Greengrass-Log-Entries enthalten einen Zeitstempel, Log-Level und Informationen zum Event. *AWS IoT Greengrass* ist in *AWS CloudTrail*[10] integriert - ein Service, der eine Aufzeichnung der Aktionen eines Benutzers, einer Rolle oder eines AWS-Services in *AWS IoT Greengrass* bereitstellt. Wenn der Kunde dies aktiviert hat, erfasst er alle API-Calls (Application Programming Interface) für *AWS IoT Greengrass* als Events. Dazu gehören Aufrufe von der *AWS IoT Greengrass* Console und Code-Calls an *AWS IoT Greengrass* API-Vorgänge. Kunden können beispielsweise einen Trail erstellen und Calls können die kontinuierliche Bereitstellung von *AWS CloudTrail*-Events an einen Amazon *Simple Storage Service* (*Amazon S3*)-Bucket ermöglichen.

---

[7] Um mit *AWS IoT Greengrass* zu beginnen, benötigen Kunden ein Device, das den *AWS IoT Greengras Core* ausführen kann. Eine vollständige Liste qualifizierter Devices und technischer Abhängigkeiten ist hier zu finden. Eine hilfreiche Anleitung bezüglich der ersten Schritte ist hier zu finden. Eine detaillierte Referenz der Entwickler ist hier zu finden.

[8] X.509-Zertifikate sind digitale Zertifikate, die den Public-Key-Infrastrukturstandard X.509 verwenden, um einen öffentlichen Key mit einer, in einem Zertifikat enthaltenen Identität, zu verbinden. X.509-Zertifikate werden von einer vertrauenswürdigen Entität ausgestellt, die als Zertifizierungsstelle bezeichnet wird. Die Zertifizierungsstelle verwaltet ein oder mehrere spezielle Zertifikate »CA-Zertifikate«, die zum Ausstellen von X.509-Zertifikaten verwendet werden. Die Zertifizierungsstelle allein, hat Zugriff auf CA-Zertifikate. Weitere Informationen sind unter https://docs.aws.amazon.com/iot/latest/developerguide/x509-certs.html zu finden.

[9] Siehe https://aws.amazon.com/cloudwatch.

[10] Siehe https://aws.amazon.com/cloudtrail.

Einschließlich Events für *AWS IoT Greengrass*. Wenn Kunden keinen Trail erstellen möchten, können sie die neuesten Events in der *AWS CloudTrail* Console im Ereignisverlauf anzeigen (falls aktiviert). Diese Informationen können für eine Reihe von Dingen verwendet werden, z. B. zur Bestimmung des Zeitpunkts einer Anfrage an *AWS IoT Greengrass* und die IP-Adresse, von der die Anfrage gestellt wurde.

Optionen für bewährte Methoden stehen zur Verfügung, um Kundendaten auf dem Device zu sichern und sollten nach Möglichkeit genutzt werden. Für *AWS IoT Greengrass* müssen alle IoT-Devices die vollständige Festplattenverschlüsselung aktivieren und bewährte Methoden für die das Key-Management befolgen. Kunden können die vollständige Festplattenverschlüsselung nutzen, indem sie AES 256-Bit-Keys verwenden, die auf NIST FIPS 140-2 validierten Algorithmen[11] basieren und bewährte Methoden für das Key-Management befolgen. Für Devices mit geringem Stromverbrauch, wie z. B. solche, die *Amazon FreeRTOS* verwenden, können Kunden NIST 8114 Lightweight Cryptography[12] Empfehlungen befolgen.

In den obigen Abschnitten wurden Mikrocontroller und Randnutzungsfälle beschrieben. Im Folgenden wird sich das Whitepaper auf IoT-Dienste konzentrieren, die in der Cloud bestehen.

AWS IoT Core - Cloud-basiertes IoT-Gateway

Serviceübersicht: *AWS IoT Core* ist ein verwalteter Cloud-Service, mit dem verbundene Devices einfach und sicher mit Cloud-Anwendungen und anderen Devices interagieren können. *AWS IoT Core* bietet sichere Kommunikation und Datenverarbeitung über verschiedene Arten von verbundenen Devices und Standorten hinweg, sodass Kunden IoT-Anwendungen mit Leichtigkeit erstellen können. Beispiele für Anwendungsfälle sind, industrielle Lösungen und vernetzte Home-Lösungen mit der Fähigkeit, Milliarden Devices und Nachrichten zu unterstützen, die verarbeitet und an AWS-Endpunkte und andere Devices weitergeleitet werden können.

Sicherheitsfunktionen: *AWS IoT Core* bietet Kunden eine Reihe von Lösungen, mit denen Sicherheit gewährleistet und aufrechterhalten werden kann. AWS Cloud-Sicherheitsmechanismen schützen Daten, wenn sie zwischen AWS IoT und anderen Devices oder AWS-Services verschoben werden. Devices können über eine Vielzahl von Identitätsoptionen (X.509-Zertifikate, IAM-Benutzer und Gruppen, Amazon Cognito-Identitäten oder benutzerdefinierte Authentifizierungstoken) über eine sichere Verbindung verbunden werden. Während Kunden die kundenseitigen Validierungen durchführen (d. h. die Validierung der Vertrauenskette, die Überprüfung des Hostnamens, die sichere Speicherung und die Verteilung ihrer privaten Schlüssel), bietet *AWS IoT Core* sichere Deliverey-Channels mit TLS. Das AWS IoT-Regelmodul leitet auch Device-Daten an andere Devices und AWS-Services, gemäß kundendefinierten Regeln, weiter. AWS-Zugriffsmanagementsysteme werden verwendet, um Daten sicher an das endgültige Ziel zu übertragen. Eine weitere AWS IoT-Autorisierungsfunktion ist AWS IoT-Richtlinienvariablen, mit der die Bereitstellung überprivilegierter Anmeldeinformationen für ein Device vermieden werden kann. Diese Funktionen, die in Verbindung mit allgemeinen bewährten Methoden für Cybersecurity verwendet werden, dienen zum Schutz von Kundendaten.

[11] NIST FIPS 140-2 Zugelassene kryptografische Algorithmen: https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402annexa .pdf.
[12] NIST 8114 — Lightweight Kryptografie: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf.

AWS IoT Device Management - Cloud-basierter IoT-Device-Management-Service

Serviceübersicht: *AWS IoT Device Management* unterstützt Kunden bei der Planung, Organisation, Überwachung und dem Remote-Management von IoT-Devices in großem Maßstab und kann in *AWS IoT Core* integriert werden, um Devices mit der Cloud und anderen Devices einfach zu verbinden, sodass Kunden ihre Device Fleets remote verwalten können. *AWS IoT Device Management* hilft Kunden, neue Devices zu integrieren, indem sie AWS IoT in der AWS Management Console oder eine API verwenden, um Vorlagen hochzuladen, die sie mit Informationen wie Devicehersteller und Seriennummer, X.509-Identitätszertifikate oder Sicherheitsrichtlinien füllen. Anschließend können Kunden die Informationen der gesamten Device Fleet in der AWS Management Console mit nur wenigen Klicks in AWS IoT konfigurieren.

Sicherheitsfunktionen: Mit *AWS IoT Device Management* können Kunden ihre Device Fleet in eine hierarchische Struktur gruppieren, die auf Funktion, Sicherheitsanforderungen oder ähnlichen Kategorien basiert. Sie können ein einzelnes Device in einem Raum, mehrere Devices auf derselben Etage oder alle Devices, die innerhalb eines Gebäudes verwendet werden, gruppieren. Diese Gruppen können dann verwendet werden, um Zugriffsrichtlinien zu verwalten, Betriebsmetriken anzuzeigen oder Aktionen über die gesamte Gruppe hinweg auszuführen. Darüber hinaus kann eine Funktion namens »Dynamic Things« automatisch Device hinzufügen, welche die vom Kunden definierten Kriterien erfüllen, und Devices entfernen, die den Anforderungen nicht mehr entsprechen. Dadurch wird der Prozess sicher optimiert und gleichzeitig die Betriebsintegrität aufrechterhalten. Dynamic Things vereinfacht auch, Device-Datensätze, basierend auf einer beliebigen Kombination von Device-Attributen, zu finden und ermöglicht es Kunden, Massenaktualisierungen durchzuführen.

Mit *AWS IoT Device Management* können Kunden Software und Firmware auch auf Devices vor Ort übertragen, um Sicherheitslücken zu patchen und die Device-Funktionalität zu verbessern, Massenaktualisierungen auszuführen, die Bereitstellungsgeschwindigkeit zu kontrollieren, Fehlerschwellenwerte festzulegen und fortlaufende Aufträge zu definieren, um die Device-Software automatisch zu aktualisieren, sodass immer die neueste Version der Software läuft wird. Kunden können remote Aktionen wie Device-Neustarts oder Werkseinstellungen senden, um Software-Probleme im Device zu beheben auf seine ursprünglichen Einstellungen zurückzusetzen. Kunden können Dateien, die an ihre Devices gesendet werden auch digital signieren, um sicherzustellen, dass die Devices nicht beeinträchtigt werden.

Die Möglichkeit, Softwareupdates zu pushen, ist nicht auf Cloud-Dienste beschränkt. OTA-Update-Jobs in Amazon FreeRTOS ermöglichen dem Kunden, Softwareupdates mithilfe des *AWS IoT Device Management* zu planen. In ähnlicher Weise können Kunden auch einen *AWS IoT Greengrass*-Core-Update-Job für ein oder mehrere *AWS IoT Greengrass* Core-Devices mithilfe von *AWS IoT Device Management* erstellen, um Sicherheitsupdates, Fehlerbehebungen und neue *AWS IoT Greengrass*-Funktionen für verbundene Devices bereitzustellen.

AWS IoT Device Defender — Cloud-basierter IoT-Device Security Service

Serviceübersicht: *AWS IoT Device Defender* ist ein vollständig verwalteter Service, der Kunden hilft, Sicherheitsfunktionen zu prüfen, die für ihre Fleet von IoT- Devices eingerichtet wurden. Der Dienst auditiert IoT-Konfigurationen kontinuierlich, um sicherzustellen, dass die Konfigurationen nicht von den bewährten Methoden für die Wartung und Durchsetzung von IoT-Konfigurationen abweichen - wie beispielsweise die Sicherstellung der Geräteidentität, die Authentifizierung und Autorisierung von Devices und die Verschlüsselung von Gerätedaten. Der Service kann eine Warnung senden, wenn es Lücken in der IoT-Konfiguration eines Kunden gibt, die ein Sicherheitsrisiko darstellen könnten, z. B. Identitätszertifikate, die über mehrere Devices verteilt werden, oder ein Device mit einem widerrufenen Identitätszertifikat, das versucht, eine Verbindung mit *AWS IoT Core* herzustellen.

Sicherheitsfunktionen: Zusätzlich zu den Überwachungsfunktionen des Service können Kunden Warnungen festlegen, die Maßnahmen ergreifen, um Abweichungen in Devices zu beheben. Beispielsweise können Spikes im ausgehenden Datenverkehr darauf hinweisen, dass ein Device an einem DDoS-Angriff (Distributed Denial of Service) beteiligt ist. *AWS IoT Greengrass* und *Amazon FreeRTOS* können auch automatisch in *AWS IoT Device Defender* integriert werden, um Sicherheitsmetriken von den Devices zur Auswertung bereitzustellen.

AWS IoT Device Defender kann Warnungen an AWS IoT, *Amazon CloudWatch* und *Amazon Simple Notification Service* (Amazon SNS) senden, wobei Warnungen in *Amazon CloudWatch*-Metriken veröffentlicht werden. Wenn ein Kunde sich entscheidet, eine Warnung zu adressieren, kann *AWS IoT Device Management* verwendet werden, um mildernde Maßnahmen, wie einen Push von Sicherheitskorrekturen durchzuführen.

AWS IoT Device Defender prüft IoT-Konfigurationen, die mit Kundengeräten verbunden sind, anhand einer Reihe von definierten bewährten Sicherheitsmethoden für IoT, sodass Kunden existierende Sicherheitslücken erkennen können und Audits kontinuierlich oder ad-hoc durchführen können. Es bestehen Sicherheitspraktiken in *AWS IoT Device Defender*, die im Rahmen der Prüfung ausgewählt und ausgeführt werden können. Dieser Service ist auch mit anderen AWS-Services wie *Amazon CloudWatch* und
Amazon SNS integrierbar, um Sicherheitswarnungen an AWS IoT zu senden, wenn eine Prüfung fehlschlägt oder Störungen erkannt werden, sodass Kunden die Ursache untersuchen und ermitteln können. *AWS IoT Device Defender* kann beispielsweise Kunden warnen, wenn Geräteidentitäten auf vertrauliche APIs zugreifen. *AWS IoT Device Defender* kann ebenfalls Aktionen vorschlagen, welche die Auswirkungen von Sicherheitsproblemen minimieren, z. B. das Widerrufen von Berechtigungen, das Neustarten eines Devices, das Zurücksetzen der Werkseinstellungen oder das Verschieben von Sicherheitskorrekturen auf die angeschlossenen Devices des Kunden.

Oft sind Kunden über schlechte Akteure besorgt, Menschliche- oder System-Fehler und autorisierte Benutzer, die böswillige Absichten haben und dies negative Auswirkungen auf die Sicherheit haben könnte. AWS IoT Core bietet Kunden die Möglichkeit, Devices sicher mit der Cloud und anderen Devices zu verbinden. Die Bausteine ermöglichen das Erzwingen von Sicherheitskontrollen wie Authentifizierung, Autorisierung, Überwachungsprotokollierung und End-to-End-Verschlüsselung. Anschließend hilft AWS IoT Device Defender bei der kontinuierlichen Prüfung von Sicherheitskonfigurationen bezüglich der Einhaltung bewährter Sicherheitsmethoden und den eigenen organisatorischen Sicherheitsrichtlinien der Kunden.

Nutzung nachweisbarer Sicherheit zur Verbesserung des IoT - ein Branchendifferenzierer

Neue Sicherheitsdienste und -technologien werden bei AWS entwickelt, um Unternehmen dabei zu unterstützen, ihre IoT- und Edge-Devices zu sichern. Insbesondere hat AWS kürzlich Prüfungen innerhalb von *AWS IoT Device Defender* gestartet, die auf AI-Technologie basieren, welche als automatisierte Argumentation bekannt ist. Diese nutzt mathematische Beweise, um zu prüfen, ob der Code der Software korrekt geschrieben wurde, und ob unbeabsichtigter Zugriff auf die Devices besteht. *AWS IoT Device Defender* ist ein Beispiel dafür, wie Kunden ihre eigenen Devices mithilfe automatisierter Argumentation direkt schützen können. Intern hat AWS automatisierte Argumente verwendet, um die Speicherintegrität von Code zu überprüfen, der auf *Amazon FreeRTOS* ausgeführt wird und, um vor Malware zu schützen. Investitionen in automatisierte Argumentation, um skalierbare Sicherheit für Software zu bieten, die als »nachweisbare Sicherheit« bezeichnet wird, ermöglichen es Kunden, vertrauliche Arbeitslasten in AWS zu betreiben.

AWS Zelkova[13] verwendet automatisierte Argumente, um zu beweisen, dass Kundendatenzugriffskontrollen, wie vorgesehen, funktionieren. Die Zugriffskontrollprüfungen in *AWS IoT Device Defender* werden von Zelkova betrieben, sodass Kunden sicherstellen können, dass ihre Daten angemessen geschützt sind. Eine AWS IoT-Richtlinie ist übermäßig permissiv, wenn sie den Zugriff auf Ressourcen außerhalb der beabsichtigten Sicherheitskonfiguration eines Kunden gewährt. Zelkova-betriebenen Kontrollen, in *AWS IoT Device Defender* prüfen, ob Richtlinien keine Aktionen zulassen, die durch die Sicherheitskonfiguration des Kunden eingeschränkt sind, und dass die beabsichtigten Ressourcen Berechtigungen zum Ausführen bestimmter Aktionen haben.

Andere Tools zur automatisierten Begründung haben dazu beigetragen, die Grundlagen der AWS IoT-Infrastruktur zu sichern. CBMC ein Open-Source-Tool wurde verwendet, um die Korrektheit von *Amazon FreeRTOS* zu beweisen, was dem Kunden mehr Vertrauen bei der Ausführung von Arbeitslasten auf Amazon IoT-Devices bietet. Hierdurch wird sichergestellt, dass Angreifer *Amazon FreeRTOS* nicht missbrauchen, oder unbefugten Zugriff erlangen können. Automatisierte Steuerungsmechanismen für die Begründung in *Amazon FreeRTOS* wurden kontinuierlich als Prüfung auf Aktualisierungen des Betriebssystems integriert. Dadurch wird sichergestellt, dass jedes Mal, wenn eine Codeänderung vorgenommen wird, Maßnahmen getroffen werden, mit denen AWS-Entwickler automatisch prüfen können, ob *Amazon FreeRTOS-Software* speichersicher ist.

Die automatisierte Argumentation wird weiterhin in einer Vielzahl von AWS-Services und -Funktionen implementiert und bietet eine erhöhte Sicherheit für kritische Komponenten der AWS-Cloud. AWS stellt weiterhin automatisierte Argumentation zur Entwicklung von Tools für Kunden, sowie zur internen Verifizierung der Infrastruktur für den AWS IoT Stack bereit.

Was sind die wichtigsten, bewährten Sicherheitsmethoden für das IoT?

Trotz der Anzahl der verfügbaren und bewährten Methoden, gibt es keinen einheitlichen Ansatz zur Minderung der Risiken für IoT-Lösungen. Je nach Device, System, Service und Umgebung, in der die Devices bereitgestellt werden, gibt es unterschiedliche Bedrohungen, Schwachstellen und Risikotoleranzen, die Kunden berücksichtigen müssen. Im Folgenden werden Empfehlungen für die Integration von End-to-End-Sicherheit über Daten, Devices und Cloud-Services hinweg empfohlen:

1. **Integrierung der Sicherheit während der Entwurfsphase**
   Die Grundlage einer IoT-Lösung beginnt und endet mit Sicherheit. Da Devices große Mengen an sensiblen Daten senden, und Endbenutzer der IoT-Anwendungen die Möglichkeit haben, ein Gerät direkt zu steuern, muss die Sicherheit von »Dingen« eine durchgängige Design-Anforderung haben. Sicherheit ist keine statische Formel. IoT-Anwendungen müssen in der Lage sein, bewährte Sicherheitsmethoden kontinuierlich zu modellieren, zu überwachen und zu iterieren.
   Eine Herausforderung für die IoT-Sicherheit ist der Lebenszyklus eines physischen Devices und die eingeschränkte Hardware für Sensoren, Mikrocontroller, Aktoren und eingebettete Libraries. Diese limitierten Faktoren können die Sicherheitsfunktionen einschränken, die jedes Device ausführen kann. Mit dieser zusätzlichen Dynamik müssen IoT-Lösungen ihre Architektur, Firmware und Software kontinuierlich anpassen, um der sich immer ändernden Sicherheitslandschaft einen Schritt voraus zu sein. Obwohl die eingeschränkten Faktoren von Devices erhöhte Risiken, Hürden und potenzielle Kompromisse zwischen Sicherheit und Kosten darstellen, muss der Aufbau einer sicheren IoT-Lösung das Hauptziel eines jeden Unternehmens sein.

[13] Weite Infoszu Zelkova sind hier zu finden: https://aws.amazon.com/blogs/security/protect-sensitive-data-in-the-cloud-with-automated - reasoning-zelkova.

2. **Aufbau auf anerkannten IT-Sicherheits- und Cybersecurity-Frameworks**
   AWS unterstützt einen offenen, standardbasierten Ansatz zur Förderung der sicheren IoT-Einführung. Wenn man die Milliarden von Devices und Anschlusspunkte berücksichtigt, die notwendig sind, um ein robustes IoT-Ökosystem für die Nutzung der Verbraucher, der Industrie und des öffentlichen Sektors zu unterstützen, ist die Interoperabilität von entscheidender Bedeutung. Daher halten sich AWS IoT-Services an Branchenstandardprotokolle und bewährte Methoden. Darüber hinaus unterstützt *AWS IoT Core* andere branchenübliche und benutzerdefinierte Protokolle, sodass Devices miteinander kommunizieren können, selbst wenn sie unterschiedliche Protokolle verwenden. AWS ist ein starker Befürworter der Interoperabilität, sodass Entwickler auf vorhandenen Plattformen aufbauen können, um verändernde Kundenanforderungen zu unterstützen. AWS unterstützt ebenfalls ein florierendes Partner-Ökosystem, um die Auswahl von Produkten und die Grenzen der Möglichkeiten für Kunden zu erweitern. Die Anwendung global anerkannter und bewährter Methoden bietet eine Reihe von Vorteilen für alle IoT-Stakeholder, darunter:
   - Wiederholbarkeit und Wiederverwendung - statt Neustart
   - Konsistenz und Konsens zur Förderung der Kompatibilität von Technologie und Interoperabilität über geografische Grenzen hinweg
   - Maximierung der Effizienz zur Beschleunigung der IT-Modernisierung und -transformation

3. **Fokussierung auf die Auswirkungen der Priorisierung von Sicherheitsmaßnahmen**
   Angriffe oder Anomalien sind nicht identisch und haben möglicherweise nicht die gleichen Auswirkungen auf Personen, Geschäftsabläufe und Daten. Das Verständnis der IoT-Ökosysteme der Kunden und der Einsatzorte der Geräte in diesem Ökosystem gibt Aufschluss darüber, wo sich die größten Risiken befinden - innerhalb des Geräts, als Teil des Netzwerks oder der physikalischen Komponente oder Sicherheit. Die Konzentration auf die Risikobewertung und die Folgen ist entscheidend für die Bestimmung, wohin die Sicherheitsbemühungen gelenkt werden sollen und wer die Verantwortung für diese Bemühungen im IoT-Ökosystem trägt.

Schlussfolgerung

Gemeinsam mit einem exponentiellen Wachstum in verbundenen Devices, kommuniziert jedes »Ding« Datenpakete in IoT, die zuverlässige Konnektivität, Speicher und Sicherheit erfordern. Mit IoT ist eine Organisation mit der Verwaltung von Überwachung und Sicherung immenser Datenmengen und Verbindungen von verteilten Devices herausgefordert. Aber diese Herausforderung muss in einer cloudbasierten Umgebung kein Hindernis sein. Neben der Skalierung und Erweiterung einer Lösung an einem Standort, ermöglicht Cloud Computing, IoT- Lösungen, die Skalierung global und über verschiedene physische Standorte hinweg, bei gleichzeitiger Reduzierung der Kommunikationslatenz und bessere Reaktionszeiten von Devices erlaubt. AWS bietet:
Eine Suite von IoT -Services mit End-to-End -Sicherheit, einschließlich Services zum Betrieb und Sicherung von Endpunkten, Gateways, Plattformen und Anwendungen, sowie den Datenverkehr, der diesen Layer durchquert. Die Integration vereinfacht die sichere Nutzung und Verwaltung von Devices und Daten, die kontinuierlich miteinander interagieren. Unternehmen profitieren von den Innovations- und Effizienzsteigerungen, die IoT bieten kann, während die Sicherheit als Priorität weiterhin gewährleistet ist.

Anlage 1 — Integration von AWS IoT-Services

AWS IoT lässt sich direkt in die folgenden AWS-Services integrieren:

- **Amazon Simple Storage Service (Amazon S3)** bietet skalierbare Speicher in der AWS-Cloud. Weitere Informationen sind unter Amazon S3 zu finden.
- **Amazon DynamoDB** stellt verwaltete NoSQL-Datenbanken bereit. Weitere Informationen sind unter Amazon DynamoDB zu finden.
- **Amazon Kinesis** ermöglicht die Echtzeitverarbeitung von Streaming-Daten in großem Umfang. Weitere Informationen sind unter Amazon Kinesis zu finden.
- **AWS Lambda** führt den Kundencode auf virtuellen Servern von Amazon Elastic Compute Cloud (Amazon EC2) als Reaktion auf Events aus. Weitere Informationen sind unter AWS Lambda zu finden.
- **Amazon Simple Notification Service (Amazon SNS)** sendet oder empfängt Benachrichtigungen. Weitere Informationen sind unter Amazon SNS zu finden.
- **Amazon Simple Queue Service (Amazon SQS)** speichert Daten in einer Warteschlange, die von Anwendungen abgerufen werden können.
  Weitere Informationen sind unter Amazon SQS zu finden.

Anlage 2 — Regierungen im IoT

Vereinigte Staaten von Amerika

National Institute of Standards and Technology (NIST) — Department of Commerce

Das United States Department of Commerce ist führend bei den vielfältigen Bemühungen, die sich IoT-Sicherheit widmen. Das National Institute of Standards and Technology (NIST) veröffentlichte ein Whitepaper[14] das Themen aufzeigt, die Kunden und Behörden bei der Bewertung der Sicherheit von Daten und Devices gleichermaßen berücksichtigen. Im Whitepaper werden die Leser aufgefordert, diese Bedenken zu bewerten und erhalten Empfehlungen zur Behebung der Probleme. NIST veröffentlichte auch den NIST Internal Report (NISTIR) 822 Bericht,[15], der Risiken identifiziert, die sich negativ auf die IoT-Einführung auswirken können. Das Dokument enthält ebenso Empfehlungen zur Minderung oder Verringerung der Auswirkungen dieser Bedenken. Das NIST beruft öffentliche und private Partnerschaften ein, bittet um Kommentare und veranstaltet Workshops zu Smart Cities und der internationalen Standardisierung des IoT, neben einer Vielzahl anderer Initiativen.[16] Obwohl die Frühindikatoren noch in den Kinderschuhen stecken, weisen sie auf potenzielle Cybersecurity- und Datenschutzrisiken als ernsthafte Herausforderungen für die Vorteile hin, die Regierungen und Verbraucher durch das IoT erzielen können.

Department of Defense

Ein weiteres Beispiel innerhalb der Regierung ist im Verteidigungsbereich zu finden. Im Jahr 2016 gab der Chief Information Officer des US Department of Defense (DoD) Empfehlungen zur Behebung der Schwachstellen und Risiken für das IoT heraus.[17] Gemäß der Richtlinienempfehlung stellt das DoD bereits Millionen von IoT-Devices und -Sensoren für DoD-Einrichtungen, Fahrzeuge und Medizinprodukte bereit und erwägt, diese in Waffen und Nachrichtensysteme einzubinden. Die Komplexität der Sicherung des IoTs beruht auf der begrenzten Verarbeitungsleistung der Devices zur Ausführung von Firewalls und Anti-Malware, sowie der großen Anzahl von Devices, die Schwachstellen auf einer anderen Ebene, als herkömmliche Mobile Devices verbinden.

Der empfohlene Ansatz und die Richtlinienmaßnahmen vom DoD zur Bewältigung von IoT-Sicherheitsrisiken umfassen: 1) Sicherheits- und Datenschutzrisikoanalyse, die jede IoT-Implementierung und damit verbundene Datenströme unterstützt, 2) Verschlüsselung an jedem Punkt, an dem die Kosten dem Risiko und dem Wert entsprechen, und 3) Überwachung von IoT-Netzwerken, um anomalen Datenverkehr und eine mögliche Bedrohung vorzeitig zu identifizieren.

Federal Trade Commission (FTC)

Die FTC war ein wichtiger Teilnehmer an IoT-Sicherheitsgesprächen und verfolgte Maßnahmen gegen Gerätehersteller, die ihre Sicherheitsverpflichtungen falsch darstellten oder nachlässig nachwiesen.

Die FTC hat ihre Messlatte auf »angemessene Datensicherheit« gesetzt. Die FTC identifizierte die folgenden, wiederholten Sicherheitslücken bei Geräteherstellern:

- Keine Sicherheitsintegration in Devices

---

[14] Jeffrey Voas (NIST), Richard Kuhn (NIST), Phillip Laplante (Penn State University) und Sophia Applebaum (MITRE), »Internet of Things (IoT) Trust Concerns« (16. Oktober 2018, https://csrc.nist.gov/publications/detail/white-paper/2018/10/17/iot-trust-concerns/draft.)

[15] NISTIR 8228, »Considerations for Managing IoT Cybersecurity and Privacy Risks Out for Public Comment« (26 September 2018, https://www.nist.gov/news-events/news/2018/09/draft-nistir-8228-considerations-managing-iot-cybersecurity-and-privacy.)

[16] Siehe https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot.

[17] Siehe https://dodcio.defense.gov/Portals/0/Documents/Announcement/DoD%20Policy%20Recommendations%20for%20 Internet% 20of% 20Things% 20-% 20White% 20Paper.pdf? ver = 2017-01-26-152811-440.

- Keine Schulungen der Mitarbeiter durch Entwickler auf gute Sicherheitspraktiken
- Keine Gewährleistung der nachgelagerten Sicherheit und Compliance (über Verträge)
- Mangelnde Defense in Depth - Strategien
- Mangel an angemessenen Zugriffskontrollen (Kunden können Standardpasswörter umgehen oder erraten)
- Keine Datensicherheitsprogramme

Bundesstaat Kalifornien

Kalifornien gehört zu den ersten Staaten in den USA, die Gesetze zum IoT erlassen haben. Die aktuellen Rechnungen befassen sich mit Problemen, wie der Sicherheit des Device Designs und des Datenschutzes, haben aber keine spezifischen Anforderungen von IoT-Herstellern. Stattdessen haben sich die Gesetzgeber in der Entwurfsphase auf die Sicherheit konzentriert und schreiben, dass der Schutz der Daten »der Art und Funktion des Geräts angemessen sein muss« und »angemessen auf die Informationen, die es sammeln, enthalten oder übertragen kann«.

Vereinigtes Königreich

Das britische Department for Digital, Culture, Media and Sport (DCMS) veröffentlichte im Oktober 2018 die endgültige Version des Code of Practice for Consumer IoT Security.[18] Dieser Code of Practice wurde gemeinsam mit dem National Cyber Security Centre erarbeitet und beinhaltete Beiträge von Verbraucherverbänden, Industrie und Wissenschaft. Das Dokument enthält 13 Leitlinien, wie ein »Secure by Design«-Ansatz für alle Unternehmen erreicht werden kann, die an der Entwicklung, Herstellung und dem Einzelhandel von Consumer-IoT-Produkten beteiligt sind.

Der Code of Practice hebt drei führende Praktiken hervor, die es Benutzern ermöglichen, die größten und unmittelbarsten Sicherheitsvorteile zu erzielen, und fordert Interessengruppen der IoT nachdrücklich auf, sie zu priorisieren: 1) Keine Standardkennwörter: Viele Benutzer ändern das Standardkennwort nicht, was die Ursache vieler IoT-Sicherheitsprobleme ist. 2) Implementierung einer Richtlinie zur Offenlegung von Sicherheitsrisiken: IoT-Devices-, Dienst- und App-Entwickler sollten eine Richtlinie zur Offenlegung von Sicherheitsrisiken und einen öffentlichen Ansprechpartner haben, um die rechtzeitige Berichterstellung (und Behebung) von Sicherheitslücken zu ermöglichen. 3) Software auf dem neuesten Stand halten: Software-Updates müssen zeitnah und einfach zu implementieren sein, und dürfen die Funktion des Devices nicht beeinträchtigen.

Ausgehend von den Bedenken und Ansätzen, die sowohl von den USA als auch von Großbritannien beschrieben wurden, wird die Sicherheit des IoTs für die Regierungen weiterhin ganz oben stehen. Nationale und internationale Normungsgremien sind ebenfalls bestrebt, Normen, Richtlinien und bewährte Verfahren zur Sicherung des IoT,[19] zu entwickeln, einschließlich der IoT-Referenzarchitektur der Internationalen Organisation für Normung (ISO) und der Arbeitsgruppe der Internationalen Fernmeldeunion (ITU) zum Thema IoT und Smart Cities.[20]

[18] Siehe https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security.
[19] Ein Kompendium aktueller Standards und Initiativen zur IoT-Sicherheit sind im Katalog des US Department of Commerce, National Telecommunications and Information Administration (NTIA) zu finden: https://www.ntia.doc.gov/files/ntia/publications/iotsecuritystandardscatalog_draft_17.pdf.
[20] Siehe https://www.itu.int/en/ITU-T/about/groups/Pages/sg20.aspx.

Im Kontext des IoT sollten Kunden die Flexibilität haben, bestehende und bewährte Praktiken zu nutzen, die bereits in der herkömmlichen Netzwerk-Cybersecurity im Einsatz sind. Zum Beispiel, wenn versucht wird, Schwachstellen zu identifizieren, Unregelmäßigkeiten zu erkennen, auf potenzielle Vorfälle zu reagieren und sich von Schäden oder Unterbrechungen an IoT-Devices zu erholen, können Kunden die Cybersecurity-Kontrollen nutzen, die dem NIST Cybersecurity Framework (CSF) zugeordnet sind.[21] Dieser grundlegende Satz von Cybersecurity-Disziplinen ist weltweit anerkannt und wurde von Regierungen und Branchen als empfohlene Basis für die Nutzung durch jede Organisation unterstützt, unabhängig von ihrer Branche oder Größe. Der Vorteil der Nutzung des NIST CSF liegt nicht nur an seinem Ruf, sondern auch in der Flexibilität, die es ermöglicht, Cybersecurity anzuwenden und gleichzeitig seine Auswirkungen auf die physische, Cyber- und Personen-Dimensionen zu berücksichtigen. Neben dem menschlichen Aspekt gilt der Rahmen für Organisationen, die sich auf Technologie verlassen, unabhängig davon, ob der Schwerpunkt in erster Linie auf Informationstechnologie, industriellen Steuerungssystemen, cyber-physikalischen Systemen oder IoT liegt.

[21] Weitere Informationen zur Ausrichtung mit dem NIST CSF, mithilfe von AWS-Services sind in diesem Whitepaper und der Kundenarbeitsmappe zu finden: https://d0.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_CSF.pdf.

Anlage 3 — AWS IoT-Services und Compliance

Als globaler Anbieter von Hyperscale-Cloud-Services verfolgt AWS einen strengen, risikobasierten Ansatz zur Sicherheit seiner IoT-Services und zum Schutz von Kundendaten. AWS erzwingt interne Sicherheitsprozesse für seine gesamten Cloud Services, um die Wirksamkeit der verwaltungstechnischen, technischen und betrieblichen Kontrollen zu bewerten, die für den Schutz vor aktuellen und neu auftretenden Sicherheitsbedrohungen, die sich auf die Sicherheit und Ausfallsicherheit auswirken, erforderlich sind. Dieser obligatorische Prozess der Sicherheitsabsicherung führt nicht nur zur Zertifizierung verschiedener Compliance-Frameworks, sondern verdoppelt auch das Engagement von AWS, Sicherheit in allen Phasen der Entwicklungs- und Betriebsprozesse des Service Lifecycles zu verankern. AWS bietet kommerzielle Cloud-Services mit Hyperscale-Standards, die nach führenden, international anerkannten Standards akkreditiert wurden, wie International Standards Organization 27001 (ISO),[22] Payment Card Industry Data Security Standard (PCI),[23] und dem Service Organization Control Reports (SOC),[24] unter anderem internationale, nationale und sektorale Akkreditierungen. AWS erfüllt außerdem die strengen Sicherheitsanforderungen im Hinblick auf die Unterstützung von klassifizierten Umgebungen bestimmter Nachrichtenagenturen. Gemeinsam erzielen Kunden in jeder Branche und jeder Größe, die AWS Cloud-Services nutzen, Sicherheitsvorteile durch Proxy, da AWS das **High Watermark** für seine Services anwendet.

AWS versteht, dass Kunden möglicherweise spezifische Compliance-Anforderungen haben, die nachgewiesen und eingehalten werden müssen. Um dies zu berücksichtigen, fügt AWS kontinuierlich Services hinzu, die auf die Kundennachfrage von Compliance-Programmen abgestimmt sind. Die im Anwendungsbereich enthaltenen IoT-Services werden nach dem Compliance-Programm auf der AWS-Website gelistet.[25]

[22] ISO 27001/27002 ist ein weit verbreiteter globaler Sicherheitsstandard, der Anforderungen und bewährte Methoden für einen systematischen Ansatz zur Verwaltung von Unternehmens- und Kundeninformationen enthält, der auf regelmäßigen Risikobewertungen basiert, die sich für ständig ändernde Bedrohungsszenarien eignen. ISO 27018 ist ein Code of Practice, der sich auf den Schutz personenbezogener Daten in der Cloud konzentriert. Es basiert auf der ISO-Informationssicherheitsnorm 27002 und bietet Implementierungshilfen für ISO 27002-Kontrollen, die für die Public Cloud Personally Identifiable Information (PII) gelten. Außerdem enthält sie eine Reihe zusätzlicher Steuerelemente und zugehöriger Anleitungen, die darauf abzielen, die Anforderungen an den Schutz öffentlicher Cloud-PII zu erfüllen, die nicht durch das bestehende Steuerungsset ISO 27002 erfüllt sind.

[23] Der Payment Card Industry Data Security Standard (PCI DSS) ist ein proprietärer Informationssicherheitsstandard, der vom PCI Security Standards Council (https://www.pcisecuritystandards.org) verwaltet wird, welcher von American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. gegründet wurde PCI DSS gilt für alle Unternehmen, die Karteninhaberdaten (CHD) und/oder sensible Authentifizierungsdaten (SAD) speichern, verarbeiten oder übermitteln, einschließlich Händler, Auftragsverarbeiter, Acquirer, Emittenten und Dienstleister.

[24] Die Berichte zur Kontrolle von Service Organization Controls (SOC 1, 2, 3) sollen eine breite Palette von Anforderungen an die Finanzprüfung für US-amerikanische und internationale Rechnungsprüfungsgremien erfüllen. Die Prüfung dieses Berichts erfolgt gemäß den International Standards for Assurance Engagements No. 3402 (ISAE 3402) und dem American Institute of Certified Public Accountants (AICPA): AT 801 (vormals SSAE 16).

[25] Siehe https://aws.amazon.com/compliance/services-in-scope.