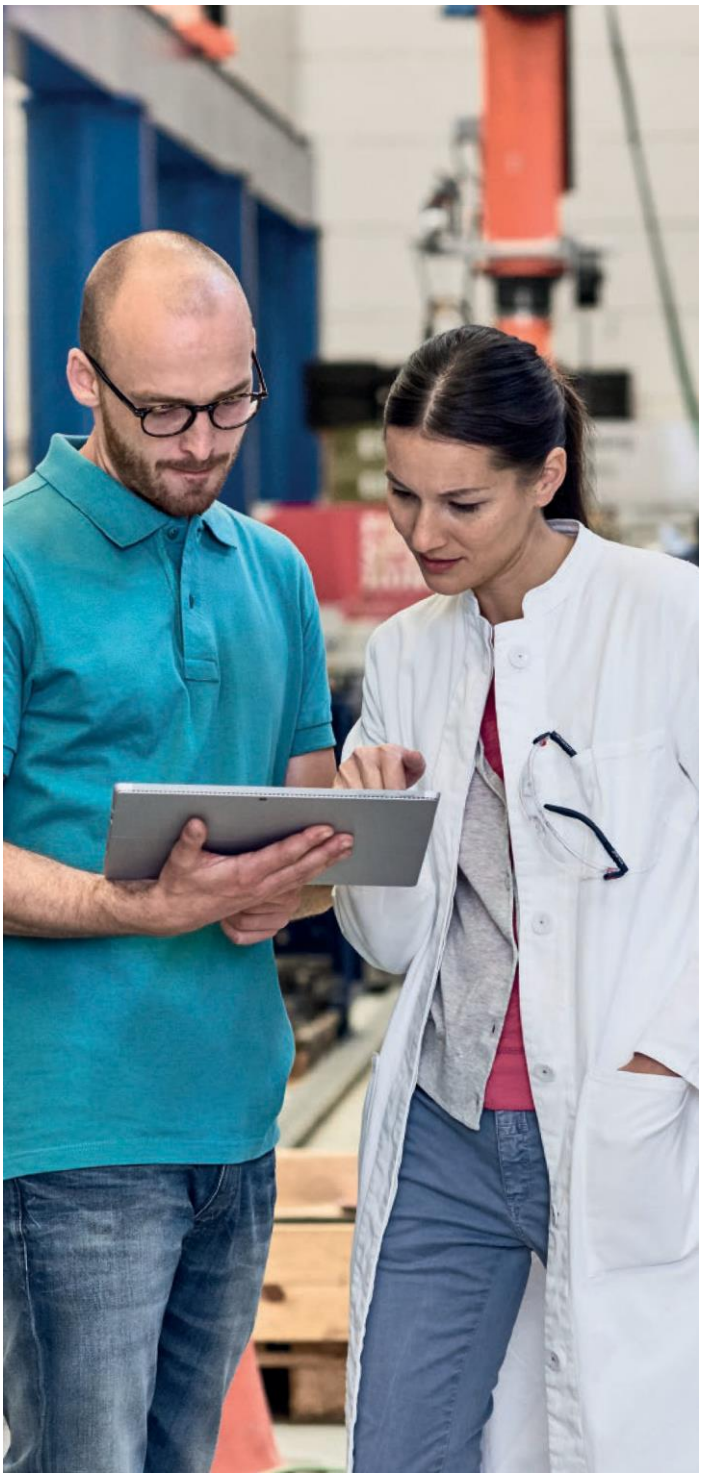
So sicher ist die Cloud of Things

Wie die Telekom Ihre IoT-Daten schützt

ERLEBEN, WAS VERBINDET.

Inhalt



1. Der sichere Einstieg ins Internet of Things

1.1 IoT, Cloud und die Sicherheit

Das Internet of Things eröffnet Unternehmen viele Möglichkeiten und macht sie fit für die Zukunft. Vorausschauende Wartung kann Personalkosten sparen und teuren Ausfällen von Maschinen vorbeugen, das Automatisieren von Prozessen beschleunigen und maschinelle Abläufe sowie Fehlerquoten senken. Zudem lassen sich mit Hilfe von Sensordaten neue Geschäftsmodelle entwickeln.

Die Telekom bietet mit der Cloud of Things die passende Plattform, mit der Kunden Maschinen und Geräte vernetzen und überwachen, Fahrzeuge lokalisieren oder den Transportweg und Zustand von Containern am Bildschirm verfolgen können. Sensordaten werden vom Gateway eingelesen, verschlüsselt an die Cloud-Plattform übermittelt und dort aufbereitet und visualisiert. Über ein beliebiges Endgerät (PC, Laptop, Tablet) erhält der Kunde Zugriff auf seine Daten.

1.2 Die Cloud of Things – Sicherheit hat hohe Priorität

Viele Unternehmen haben jedoch Bedenken, ob ihre Daten in der Cloud sicher sind. Sensible Firmendaten und Betriebsgeheimnisse sollen vor unbefugtem Zugriff geschützt, bei Kundendaten muss die Informationssicherheit gewährleistet sein. Dies sind Anforderungen, die dieTelekom ernst nimmt. Deshalb ist bei der Cloud of Things die Sicherheit oberstes Prinzip. Sie wird durch einen umfangreichen Maßnahmenkatalog gewährleistet: Sämtliche Daten werden auf Servern in sicheren Rechenzentren in Deutschland gespeichert. Übertragungen von Sensordaten erfolgen verschlüsselt. Für Sicherheit sorgen standardisierte Verfahren und Schutzkonzepte für Infrastruktur und IT-Systeme sowie die Absicherung von Netzen und Kommunikationsschnittstellen.

Plattform Management
Das Plattform Management in der Cloud of Things liefert einen Überblick über alle angeschlossenen Geräte, ihren aktuellen Betriebszustand und den Fluss der Nutzdaten. Die Ausführung von Aktivitäten erfolgt über ein umfangreiches Rollen- und Rechtekonzept, welches von einem Administrator des Kunden festgelegt wird. Wesentliche Ereignisse werden von der Plattform in Audit-Logs dokumentiert. Die Anmeldung kann optional über Zwei-Faktor-Authentifizierung erfolgen.

Aktualisierung von Firmware aus der Cloud of Things
Über die Cloud of Things lassen sich IoT-Geräte aus der Ferne warten und dadurch alle Komponenten einschließlich Firmware und Betriebssystem auf aktuellem Stand halten. Soweit erforderlich können Sicherheitsupdates aus der Cloud of Things auf die IoT-Geräte geladen werden und somit Sicherheit der Infrastruktur gewährleistet werden.

2. Sicherheit bei der Telekom

Der Cloud-Betrieb der Telekom wird regelmäßig von der Deutschen Telekom Security GmbH geprüft, die sich auf Datensicherheit spezialisiert hat. Sie legt ein angemessenes Sicherheitsniveau fest und sorgt dafür, dass es mit geeigneten Maßnahmen umgesetzt wird.

2.1 Sichere Prozesse durch das PSA-Verfahren

DieTelekom hat einen Standardprozess, Privacy Security Assessment (PSA), entwickelt. Das PSA-Verfahren gewährleistet die Integration von Sicherheit in die Produkt- und Systementwicklung und beinhaltet sowohl Beratung, Testing und Dokumentation als auch Risikobewertung und Freigaben.

Zum PSA-Verfahren gehört ein standardisiertes Sicherheits- und Datenschutzkonzept (SDSK) mit sechs Modulen:

- Systembeschreibung
- Datenschutzinformation
- Berechtigungskonzept
- Anforderungskataloge
- Maßnahmenplan
- Systemkategorisierung

2.2 Sichere Rechenzentren

Der Zugriff auf die bauliche Infrastruktur eines Rechenzentrums oder gar die Hardware würde einem Angreifer einen aussichtsreichen Ansatzpunkt zur Spionage von Daten oder zur Manipulation von Diensten liefern. Ein Angreifer könnte so z. B. über Ein-/Ausgabe-Schnittstellen oder USB-Ports Daten auslesen und kopieren, Schadcode einbringen oder Dienste abschalten. Ein wichtiger Aspekt des IT-Grundschutzes ist deshalb die Absicherung der Infrastruktur. Dazu zählt ebenso der Schutz vor unvorhergesehenen Ereignissen, die zum Ausfall von Diensten führen könnten. Für die Cloud-Infrastruktur arbeitet dieTelekom mit Microsoft als erfahrenem Partner zusammen. Microsoft hat geeignete Maßnahmen zum Schutz Ihrer Informationen umgesetzt und schützt diese vor versehentlichem, unbefugtem oder rechtswidrigem Zugriff.

Umfassender Gebäudeschutz
Die Gebäudekomplexe in eingesetzten Rechenzentren sind daher abgeschottet; höchste Sicherheitsvorkehrungen schützen die Daten vor unberechtigtem Zugriff. Das Betriebsgelände, die Gebäude und Räume sind vor unbefugtem Zugang und Einbruch geschützt und können ausschließlich durch autorisiertes Personal betreten werden. Die Zugänge werden überwacht und je nach Sicherheitsstufe wird gespeichert, welche Person zu welchem Zeitraum Zugang hatte.
Der Schutz vor Bränden und Blitzeinschlag sowie vor Wasser- und Hochspannungsschäden gehört ebenfalls zum umfassenden Sicherheitspaket der Infrastruktur. Außerdem ist die Stromversorgung ausfallsicher gegen Spannungsschwankungen, Über- oder Unterspannung gesichert.

Cloud-Rechenzentren für die Cloud of Things sind nach der internationalen Norm ISO / IEC 27001 zertifiziert. Dieses in regelmäßigen Abständen überprüfte Zertifikat bescheinigt, dass Standards bezüglich Sicherheitsrichtlinien, Schutzbedarf und Risiken erfüllt sind.

Das „Zero Outage“-Prinzip
DieTelekom verfolgt das Zero Outage Prinzip, um Ausfällen von IT-Systemen vorzubeugen..

Die durchschnittliche Plattformverfügbarkeit der Cloud of Things liegt bei 99,95% je Kalenderjahr.

3. Sicherheit in der Cloud of Things

Zusätzlich zu den konzernweiten Sicherheitsstrategien bei der Deutschen Telekom wird die IoT-Plattform Cloud of Things durch weitere, im Folgenden beschriebenen Maßnahmen vor potenziellen Risiken geschützt.

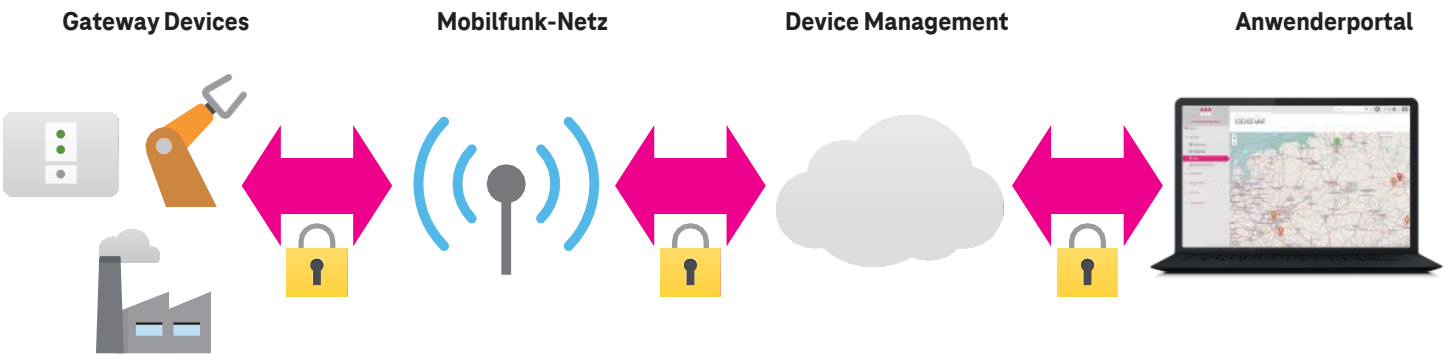
3.1 IT-Systeme

Die in den IT-Systemen der Telekom verwendeten Betriebssystemkerne und Softwarekomponenten unterliegen hohen Anforderungen an die Pflege von Softwareständen und den Schutz vor Viren und Malware.

Überlastschutz
Die IT-Systeme der Cloud of Things sind vor Überlast geschützt. So ist die Plattform gegen den Versuch abgesichert, durch massenhafte Anfragen eine Blockade von Diensten zu erreichen (DDoS-Attacken) oder das System aus der Balance zu bringen.

Freigabe der IT-Systeme
Vor jeder Freigabe neuer Cloud of Things Releases überprüfenauf das Testen spezialisierte Experten diese auf die Einspielung der neuesten Softwarestände und -patches. Im Anschluss an die Überprüfung simulieren sie mit Penetrationstests gezielt Angriffe, um in der Vorgehensweise eines potenziellen Angreifers zu versuchen, in die Systeme einzudringen.

3.2 Sicherheit im Netz



Ein potenzielles Angriffsziel für Cyberattacken sind die Netzwerkverbindungen zwischen dem Browser des Kunden und der Cloud of Things sowie die Funkstrecken zwischen den Geräten und der Plattform als Server. Die Infiltration einer Funk- oder Netzwerkstrecke könnte dann der Ausgangspunkt für weiterführende Spionage- oder Sabotageversuche sein: Hat der Angreifer einmal Nutzungs- und Positionsdaten ausgespäht, Webcamvideos mitgeschnitten oder ein Smart Home manipuliert, kann er durch Sabotage ganze Produktfamilien und das Image des Produkts oder Anbieters zerstören – oder den Hersteller erpressen. Dem beugt die Telekom durch einen umfangreichen Maßnahmenkatalog vor.

TLS-Authentifizierung vor jeder HTTPS-Kommunikation
Die Verwendung eines anerkannten und standardisierten Authentifizierungsmechanismus gewährleistet, dass sich kein Dritter in die HTTPS-Kommunikation zwischen einem IoT-Gerät oder dem Browser des Kunden und der Cloud of Things einschalten kann. Vor jeder Kommunikation über ein Netzwerk weist die Cloud of Things ihre Identität durch ein Zertifikat nach. Zertifikate gewährleisten, dass der Kommunikationspartner derjenige ist, der er vorgibt zu sein – einer Quelle, die kein akzeptiertes Zertifikat liefern kann, wird prinzipiell nicht vertraut. So wird bei Änderungen an der Firmware oder anderem Datenverkehr mit dem Gerät die Authentizität der Plattform nachgewiesen.

Bei der Cloud of Things kommt das Protokoll Transport Layer Security (TLS) zum Einsatz. In TLS überprüfen die Kommunikationspartner ihre Authentizität über Zertifikate und stellen eine verschlüsselte Verbindung her. Jetzt können Daten sicher ausgetauscht werden: Die Verbindung ist gegen Attacken geschützt, in denen ein Angreifer eine falsche Identität vortäuscht, sich zwischen Sender und Empfänger schaltet und den Datenverkehr abhört (sogenannte „Man in the Middle"-Attacken). Für die Kommunikation mit der Cloud of Things werden die Versionen TLS 1.2 und TLS 1.3 unterstützt.

Verschlüsselung mit AES
Die gesamte Datenkommunikation der Cloud of Things wird verschlüsselt durchgeführt. Dies gilt nicht nur für die Zugriffe über das Cockpit, sondern auch für die gesamte Kommunikation zwischen den IoT-Geräten und der Plattform in beiden Richtungen. Dazu unterstützt die Cloud of Things den sicheren Algorithmus Advanced Encryption Standard (AES). Dieser Algorithmus wurde vom amerikanischen National Institute of Standards and Technology (NIST) als Standard bekannt gegeben. Er gilt als so sicher, dass die Verwendung in den USA sogar für staatliche Dokumente mit höchster Geheimhaltungsstufe zugelassen ist. Für Kunden, deren Geräte kein AES unterstützen und deren Geheimhaltungsstufe dies nicht erfordert, unterstützt die Cloud of Things weitere Verschlüsselungsverfahren.

Die starke Verschlüsselung gewährleistet, dass niemand Unternehmens- oder Kundendaten entschlüsseln kann, wenn er diese zufällig oder illegal erhält oder ausspioniert, um sie für eigene Zwecke zu missbrauchen, zu verkaufen beziehungsweise an anderer Stelle zu veröffentlichen. Veränderungen an den Daten, auch als Spoofing bekannt, sind ebenfalls nicht möglich. Somit ist es beispielsweise einem Angreifer nicht möglich, Positionsdaten zu überschreiben und virtuell die Position eines LKWs zu verändern, Messwerte von Sensoren in einem Kühlcontainer zu manipulieren oder im Smart Home das Signal eines Garagentors zu reproduzieren und das Tor zu jeder beliebigen Zeit zu öffnen.

Netzwerktrennung
Der Kern der Cloud of Things ist in mehrere Teilbereiche mit unterschiedlichen Funktionen aufgeteilt. Die einzelnen Module dieser Teilbereiche arbeiten in eigenen Zellen, die wiederum unabhängige Netzwerkkonfigurationen mit eigenen Adressbereichen nutzen. Diese virtuellen Netzwerke (VLAN) sind so gegeneinander abgeschottet, dass ein Einbruch in eines der VLANs keinen Zugriff auf ein anderes VLAN bietet und folglich nicht auf andere Zellen ausgeweitet werden kann.

Firewalls
Die Cloud of Things verwendet ein umfangreiches Firewallkonzept, das Zugänge aus unsicheren Netzwerken in die Plattform absichert. Alle eingehenden Anfragen müssen die Firewall passieren: Dies gilt für Zugriffe von der Webseite genauso wie für Anfragen von IoT-Geräten über die Softwareschnittstellen der Cloud of Things. Die Sicherheitsexperten der Deutschen Telekom überprüfen die Firewalls regelmäßig mit Penetrationstests: So werden Schwachstellen aufgedeckt und geschlossen.

3.3 Zusätzliche Maßnahmen für erhöhten Schutz

Eine weitere Angriffsfläche bieten die Schnittstellen zur Cloud of Things. Sie sind für das Gerätemanagement und die Datenhaltung notwendig und dienen mitunter auch zur Übermittlung von Alarmen. Da sie über das Internet erreichbar sind, sichert die Telekom sie mit speziellen Konzepten.

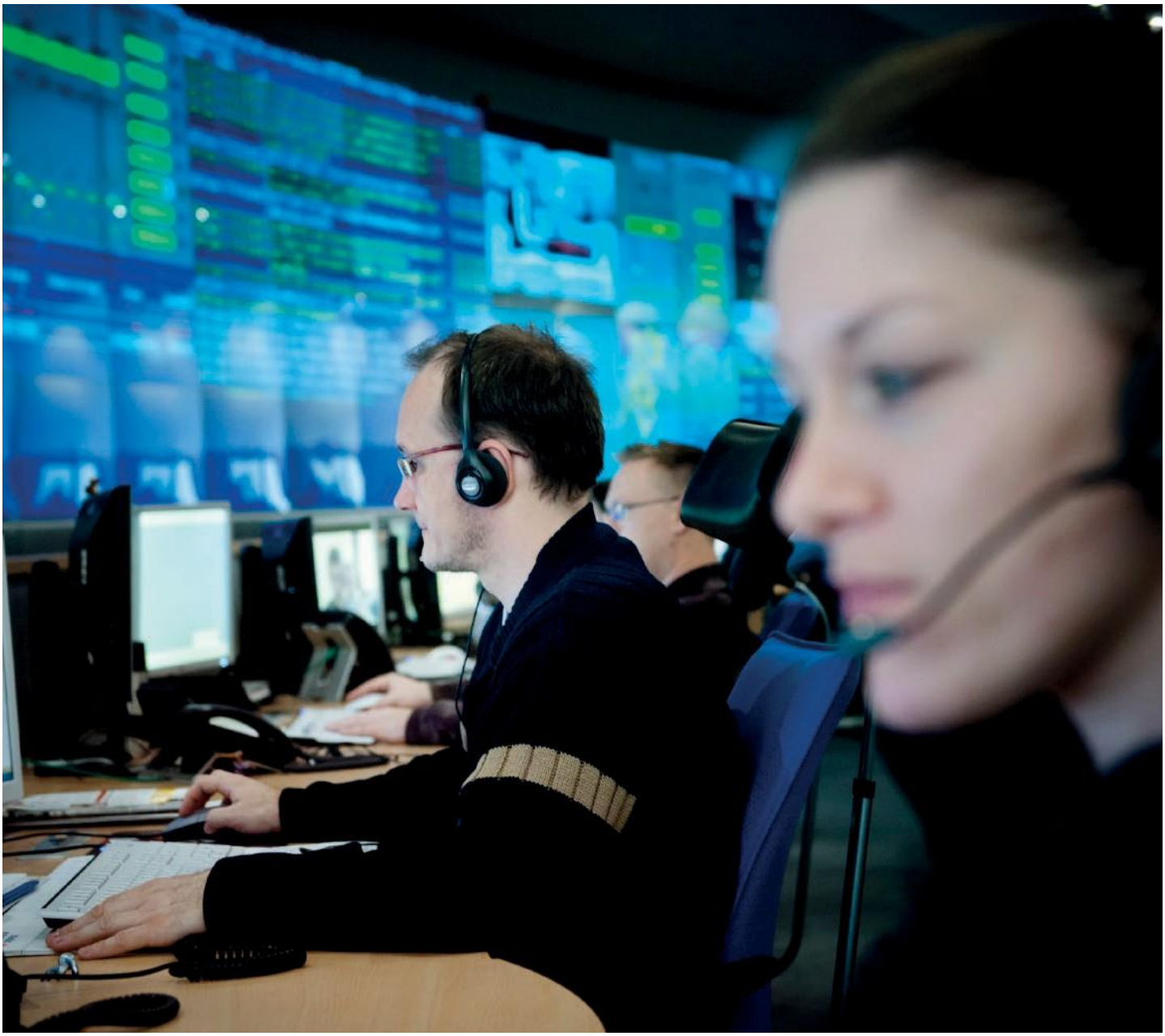
Multi-Tenancy
Die Cloud of Things ist multi-tenant (mandantenfähig) aufgebaut: Unterschiedliche Kunden (Tenants) verfügen auf der Plattform über getrennte Nutzerbereiche und teilen sich keine Administrator- oder Datenbereiche mit anderen Kunden. Es besteht keine Möglichkeit, Kunden-, Nutzer- oder Nutzdaten eines anderen Tenants auszuspähen. Ein Logistikunternehmen beispielsweise hat keinen Zugriff auf die Kundendaten oder LKW-Positionsdaten eines Konkurrenten. Auch Administratoren der Deutschen Telekom haben nur Zugriff auf die Daten in den Kundenmandanten nach expliziter Freigabe durch den Kunden für maximal 24 Stunden.

Trennung von Nutzerdaten und Nutzdaten
Eine zweite Trennung schützt vor Datenspionage oder -manipulation: Innerhalb eines jeden Tenants werden Kunden- und Nutzerdaten getrennt von den Nutzdaten der IoT Geräte verwaltet und abgelegt.
Das bedeutet, dass IoT Geräte auch nicht mit krimineller Energie dazu verwendet werden können, um an persönliche oder betriebliche Daten zu gelangen.

Berechtigungskonzept
Kunden können unterschiedliche Benutzerrollen wie Administrator, Standardnutzer oder Business User definieren und autorisieren, die mit verschiedenen Berechtigungen und Privilegien verknüpft sind. Entsprechend können Anwender nur Inhalte einsehen, für die ihnen Rechte in den Benutzerrollen zugewiesen wurden. Das Berechtigungskonzept definiert, wer Daten erzeugen, lesen, verändern und löschen darf. Privilegierte Berechtigungen werden nur solchen Rollen, Gruppen oder Personen zugewiesen, die überwiegend mit der Administration betraut sind.

Freigabe durch Securityexperten vor jedem Release
Bei jeder Neuentwicklung oder Änderung überprüfen Experten der Deutschen Telekom, ob das Projekt alle Anforderungen an technische Sicherheit erfüllt. Die Freigabe durch die Sicherheitsexperten, die organisatorisch und prozessual außerhalb der Projekt- und Entwicklungsteams stehen, ist verpflichtend vor jedem Release der Cloud of Things. Eine Veröffentlichung ohne diese Freigabe ist nicht möglich.

Zertifizierungsprozess für IoT-Geräte
Businesspartner können ihre IoT-Geräte von den Experten der Deutschen Telekom prüfen und zertifizieren lassen, die für die Nutzung in der Cloud of Things infrage kommen. Für diese Geräte ist gewährleistet, dass sie die Anforderungen an technische Sicherheit erfüllen.
Kunden, die eigene Geräte und eigene Lieferanten einbeziehen, können die entsprechenden Testkriterien anfordern oder eine Beratung und Überprüfung durch die Telekom in Anspruch nehmen.
Jedes Gerät verfügt über einen bei der Registrierung in der Cloud of Things festgelegten Autorisierungsschlüssel, der eindeutig ist und nicht auf andere Geräte übertragen werden kann. So wird gewährleistet, dass sich keine Geräte in die Kommunikation einklinken können.



4. Tipps für sicheres Arbeiten im Internet of Things

DieTelekom sorgt mit einem umfangreichen Maßnahmenkatalog für Sicherheit in der Cloud of Things. Doch eine sichere Plattform nützt nichts, wenn die IT- Umgebung des Kunden nicht ausreichend geschützt ist. Die Punkte in den folgenden Kapiteln sollen helfen, typische Versäumnisse in puncto Sicherheit zu vermeiden.

4.1 Prinzipien und Richtlinien

Formale Prozesse und Richtlinien sind ein wichtiger Baustein – es hilft, einen Plan zu haben!

- **Risikoanalyse durchführen:** Sicherheitsrisiken identifizieren, mögliche Schadenszenarien abschätzen, vorbeugende Maßnahmen treffen
- **Anforderungen definieren:** Anforderungskataloge und Checklisten erstellen, Messgrößen und Testkriterien festlegen
- **Auf Sicherheit testen:** Gezielte Angriffsversuche durch eigenes Sicherheitspersonal simulieren, Penetrationstests durchführen, Testkatalog erstellen, Testfälle generieren, Tester finden, Zeitpunkte für Tests und Audits festlegen, Testautomatisierung verwenden
- **Abnahmestrategien festlegen:** Gates und Zeitpunkte festlegen, Auditoren benennen, Ergebnisse dokumentieren
- **Notfallplan entwickeln:** Abläufe für den Fall der Fälle festlegen, Abschalten /Herunterfahren von Modulen und Systemen regeln, Betriebskontinuität sicherstellen, Sicherheitsreserven anlegen, Kommunikation und Pressearbeit regeln

4.2 Gerätesicherheit

Auch die Software und Daten auf vernetzten Geräten außerhalb der Cloud of Things – also beispielsweise auf dem Rechner, mit dem Anwender auf das Webportal zugreifen – müssen sicher sein, um nicht als Einfallstor für Angriffe missbraucht zu werden. Die Telekom empfiehlt folgende Maßnahmen:

- **Updates einspielen:** Updates vorsehen, Sicherheitslücken im Betriebssystem schließen, Firmware aktualisieren, Aktualisieren von Zertifikaten ermöglichen
- **Passwörter ändern:** Alle Standardpasswörter durch eigene Passwörter ersetzen, starke Passwörter verwenden, nach im Hintergrund installierten Komponenten suchen
- **Autorisierung stärken:** Autorisierung am Server überprüfen (nicht am Client), Passwortänderungen ermöglichen, Zugangsdaten zu anderen Systemen änderbar machen, Löschen von Zugangsdaten vorsehen, LDAP oder vergleichbare Standard-Autorisierungsbackends verwenden
- **Standard-PKI verwenden:** Standardisierte Public-Key-Infrastruktur (PKI) mit Zertifikatsprüfung vor jeder Datenkommunikation einsetzen, TLS (Client prüft Zertifikat des Servers) oder IPsec (beide Seiten prüfen Zertifikate des jeweils anderen) verwenden, gerätespezifische Zertifikate nutzen, Teilen oder gemeinsames Verwenden von Zertifikaten mit anderen vernetzten Geräten vermeiden
- **Vor Malware schützen:** Antivirenschutz einsetzen und aktuell halten
- **Datenspeicher verschlüsseln:** Alle lokalen Datenträger verschlüsseln
- **Vor Überlast schützen:** Nicht autorisierten Datentransfer am Eingang abweisen, Überlastsituation durch massenhafte Anfragen (DDoS) erkennen und reagieren, Systeme vor Eintreten von unstabilem oder unvorhergesehenem Verhalten kontrolliert herunterfahren
- **Außerbetriebnahme ordnen:** Geräte und Dienste bei Verlust / Diebstahl /Verkauf /Ende des Produktlebenszyklus außer Dienst stellen, Zugangsdaten sperren, Zugänge löschen, Zertifikate und Lizenzen kündigen, Software deinstallieren, Speicher löschen, Einträge in Whitelists aktualisieren, Geräte und Dienste herunterfahren, Hardware entfernen, Entsorgung regeln

4.3 Eigene Fähigkeiten weiterentwickeln

Es ist empfehlenswert, nicht nur in Technik und Sicherheitskonzepte zu investieren, sondern parallel die eigenen Fähigkeiten ständig zu erweitern sowie Trends und notwendige Anpassungen zu verfolgen. DieTelekom unterstützt Sie bei folgenden Maßnahmen:

- **Briefing:** Mitarbeiter informieren, auf Gefahren hinweisen, Verantwortlichkeiten benennen, Techniken vorstellen, Material zur Verfügung stellen
- **Schulung:** Weiterbildungsbudget bereitstellen, Konzepte und Techniken schulen, Beratung und Know-how einkaufen, Wissenstransfer fördern
- **Zertifizierung:** externe Prüfung durchführen und Prozesse zertifizieren lassen, Mitarbeiter zertifizieren

5. Zusammenfassung

Sicherheit hat für das Internet of Things der Deutschen Telekom hohe Priorität. Unternehmen wollen einerseits die Vorteile einer cloudbasierten IoT-Plattform nutzen, um ihr Geschäftsmodell zukunftsfähig zu machen. Andererseits wollen sie aber sicher gehen, dass Firmen-, Kunden- und Sensordaten nicht in falsche Hände geraten.

Sicherheit bei der Deutschen Telekom

DieTelekom hat deshalb auch für ihre IoT-Plattform Cloud of Things die Sicherheit zu einem hohen Prinzip erhoben. Konzernweit sorgt das Privacy and Security Assessment für die Integration von Datensicherheit in die System- und Produktentwicklung. Die Zusammenarbeit mit Microsoft Azure gewährleistet hohe Sicherheitsstandards für die Rechenzentren, aus der die Cloud of Things bereitgestellt wird: Die Infrastruktur ist durch einen umfassenden Gebäudeschutz sowohl vor unberechtigtem Zugriff als auch vor unvorhergesehenen Ereignissen wie Brand, Wassereinbruch oder Stromausfall geschützt. Mit einem Frühwarnsystem werden die Rechenzentren zudem vor Cyberattacken geschützt.

Das Sicherheitskonzept für die Cloud of Things

Die Systeme haben keine ungeschützte Verbindung zum Internet; alle Daten werden Ende-zu-Ende verschlüsselt übertragen. Vor jeder Netzwerkkommunikation findet eine Authentifizierung in beide Richtungen statt. Die IT ist gegen DDoS-Angriffe gewappnet; Datenbanken und Server werden aktiv gemanaged. Außerdem ist die Plattform durch eine mehrstufige Firewall vor unbefugtem Zugriff geschützt.

Durch die unabhängige Verarbeitung können Attacken auf ein Modul nicht auf andere Module übergreifen. Jeder Vorgang durchläuft eigene Endpunkte, wobei jeder Endpunkt durch eine separate Authentifizierung und Zugriffskontrolle abgedeckt ist, um die Identität, den Mandantenbereich und die Zugriffsrechte zu bestätigen. Ein direkter Zugriff auf die Datenbank ist auch für die Mitarbeiter im Betrieb und für Dienstleister nicht zulässig. Administratoren der Deutschen Telekom können eine Freigabe durch den Kunden für maximal 24 Stunden zu Diagnosezwecken erhalten. Die Informationssicherheit ist somit stets gewährleistet. Mit diesem umfangreichen Sicherheitspaket ebnet dieTelekom den Weg von Unternehmensanwendungen ins Internet of Things.

Glossar

AES – Advanced Encryption Standard: Verschlüsselungs- verfahren mit einem sehr hohen Maß an Sicherheit.

Camellia: Ein symmetrisches Blockverschlüsselungs-verfahren mit ähnlichen Parametern wie AES, aber einem anderen Verschlüsselungsalgorithmus.

DDoS – Distributed Denial of Service: Nichtverfügbarkeit eines Dienstes infolge von Überlastung durch einen gezielten Angriff auf einen Server oder eine andere Netzkomponente, der von einer großen Zahl anderer Systeme geführt wird.

Firewall: Ein Sicherheitsgateway aus Soft- und Hardware, um IP-Netze sicher zu koppeln.

IDS – Intrusion Detection System: System zur Erkennung von Angriffen gegen ein Computersystem oder Rechnernetz.

M2M – Machine-to-Machine-Kommunikation: Automatisierter Datenaustausch zwischen Maschinen, Geräten, Automaten, Fahrzeugen und anderen Endgeräten oder mit einer zentralen Leitstelle über Internet, Mobilfunk- und andere Zugangsnetze.

„Man in the Middle"-Attacke: Zwischenschalten eines Angreifers in die Kommunikation zwischen zwei Partnern.

Multi-Tenancy: Mandantenfähigkeit, d. h. Fähigkeit eines Computersystems, unterschiedliche Mandanten (Tenants) mit jeweils eigenständiger Datenhaltung, Konfiguration und Präsentation zu verwalten.

Penetrationstest: Simulierter Versuch, in der Vorgehensweise eines potenziellen Angreifers gezielt in das eigene IT-System einzudringen.

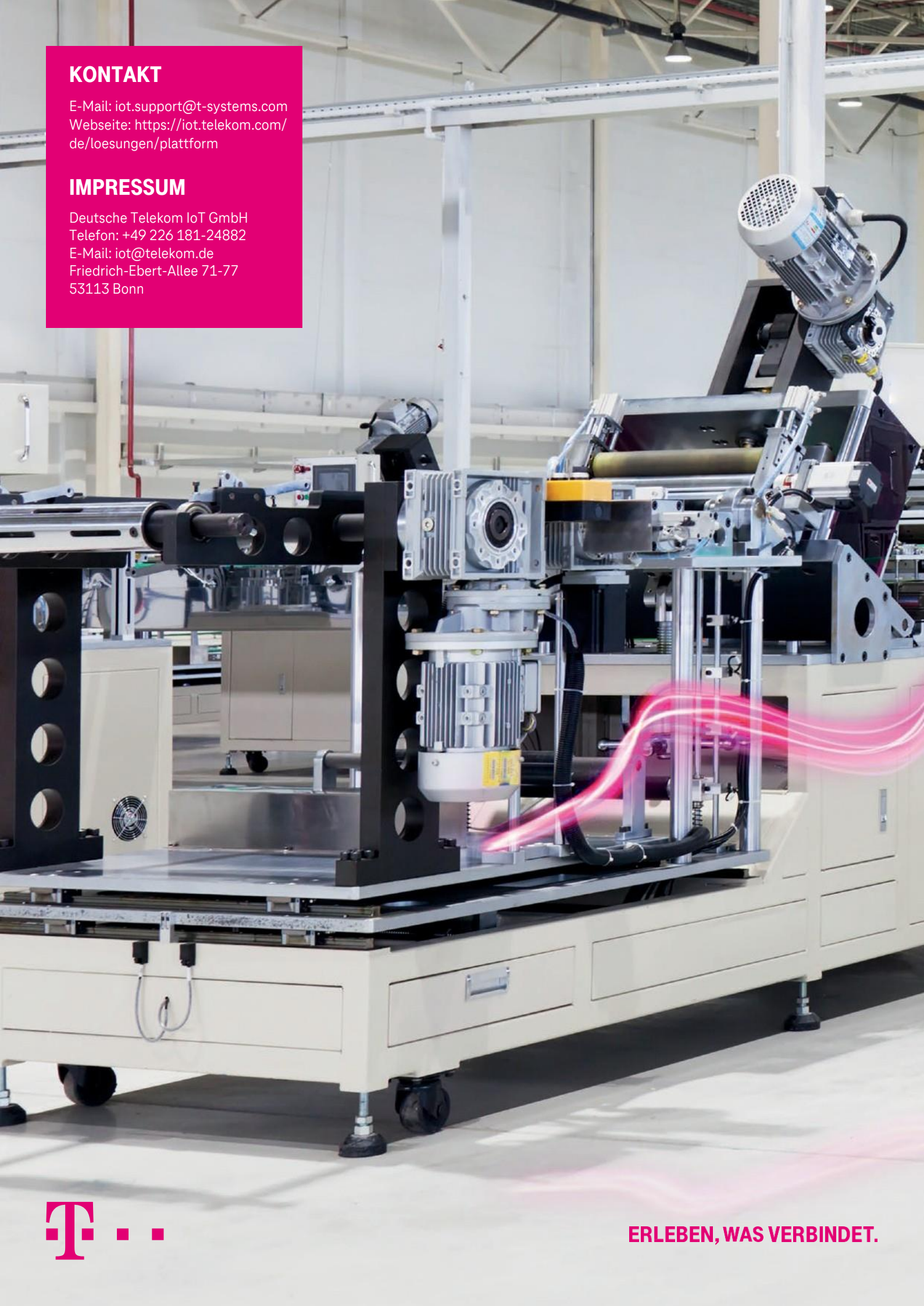
PKI – Public Key Infrastructure: Ein System zum Ausstellen, Verteilen und Überprüfen von digitalen Zertifikaten zur Authentifizierung mithilfe eines Paares von öffentlichen und privaten Kryptographieschlüsseln.

PSA – Privacy and Security Assessment: Standardprozess der Deutschen Telekom zur Sicherstellung von Sicherheit und Datenschutz in allen Telekom-Produkten.

Tenant: Mandant, d. h. eine datentechnisch abgeschlossene Gruppe von Nutzern eines Computersystems mit eigenen Zugriffsberechtigungen.

TLS – Transport Layer Security: Verschlüsselungsprotokoll für die Datenübertragung, Weiterentwicklung von Secure Socket Layer (SSL).

VPN – Virtual Private Network: Virtuelles privates Netzwerk; in sich geschlossenes Kommunikationsnetz, das ein anderes Kommunikationsnetz als Transportmedium verwendet, etwa in Form eines VPN-Tunnels durch das öffentliche Internet.



KONTAKT

E-Mail: iot.support@t-systems.com
Webseite: https://iot.telekom.com/de/loesungen/plattform

IMPRESSUM

Deutsche Telekom IoT GmbH
Telefon: +49 226 181-24882
E-Mail: iot@telekom.de
Friedrich-Ebert-Allee 71-77
53113 Bonn

ERLEBEN, WAS VERBINDET.