SO SICHER IST DIE CLOUD DER DINGE

WIE DIE DEUTSCHE TELEKOM KUNDENDATEN SCHÜTZT

ERLEBEN, WAS VERBINDET.

INHALT

1. DER SICHERE EINSTIEG INS INTERNET DER DINGE 3

1.1 M2M, IoT, Cloud und die Sicherheit 3

1.2 Die Cloud der Dinge – Sicherheit hat oberste Priorität 3

2. SICHERHEIT UND DATENSCHUTZ BEI DER DEUTSCHEN TELEKOM 4

2.1 Sichere Prozesse durch das PSA-Verfahren 4

2.2 Standardisiertes Sicherheits- und Datenschutzkonzept 6

2.3 Sichere Rechenzentren 6

3. SICHERHEIT IN DER CLOUD DER DINGE 8

3.1 IT-Systeme 8

3.2 Sicherheit im Netz 9

3.3 Zusätzliche Maßnahmen für erhöhten Schutz 10

4. TIPPS FÜR SICHERES ARBEITEN IM INTERNET DER DINGE ...12

4.1 Prinzipien und Richtlinien 12

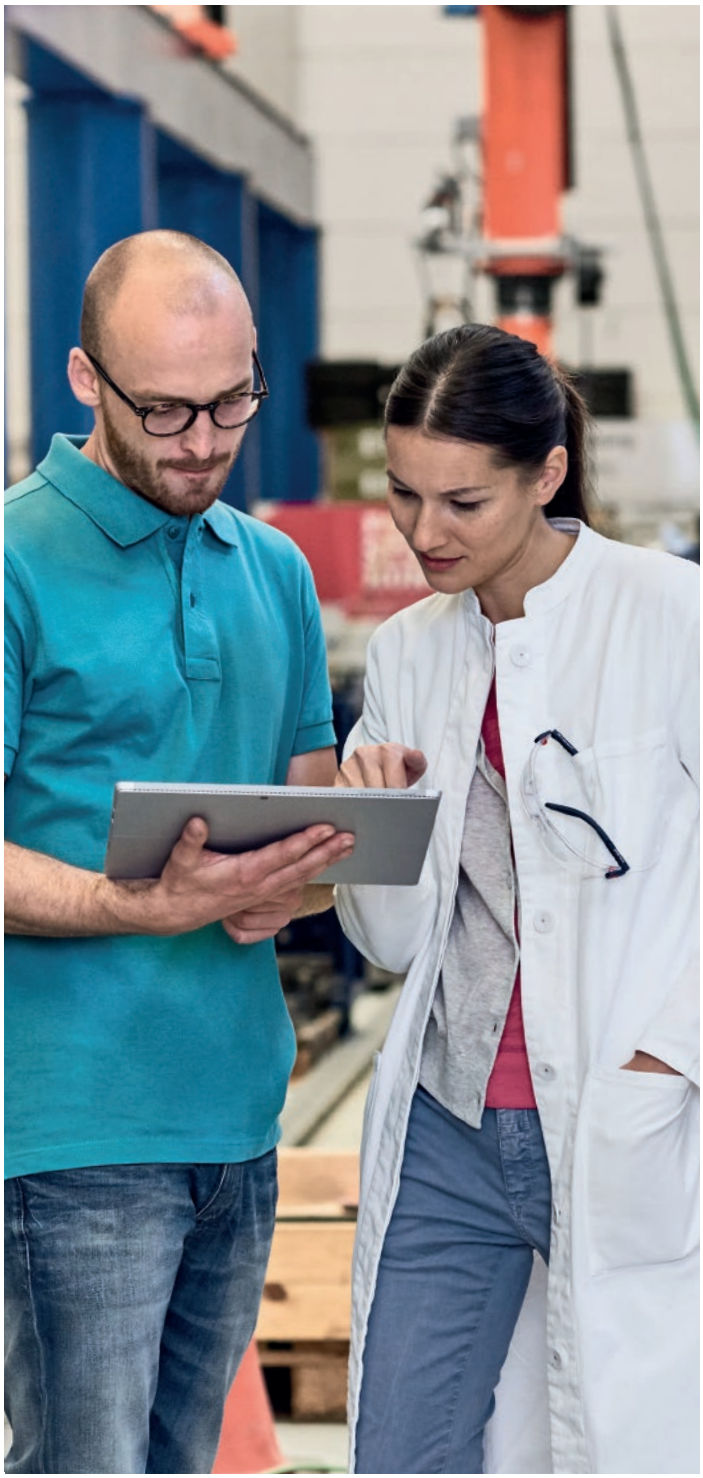
4.2 Gerätesicherheit 13

4.3 Eigene Fähigkeiten weiterentwickeln 13

5. ZUSAMMENFASSUNG 14

GLOSSAR 15

KONTAKT / IMPRESSUM 16



1. DER SICHERE EINSTIEG INS INTERNET DER DINGE

1.1 M2M, IOT, CLOUD UND DIE SICHERHEIT

Das Internet der Dinge eröffnet Unternehmen viele Möglichkeiten und macht sie fit für die Zukunft. Vorausschauende Wartung spart Personalkosten und beugt teuren Ausfällen von Maschinen vor, das Automatisieren von Prozessen beschleunigt maschinelle Abläufe und senkt die Fehlerquote, aus Sensordaten lassen sich neue Geschäftsmodelle entwickeln.

Die Deutsche Telekom bietet mit der Cloud der Dinge die passende Managementplattform, 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 nur der Kunde Zugriff auf seine Daten.

1.2 DIE CLOUD DER DINGE – SICHERHEIT HAT OBERSTE PRIORITÄT

Viele Unternehmen haben jedoch Bedenken, ob ihre Daten in der Cloud sicher sind. Sensible Firmendaten und Betriebsgeheimnisse sollen vor unbefugtem Zugriff geschützt sein, bei Kundendaten muss der Datenschutz gewährleistet sein. Forderungen, die die Deutsche Telekom ernst nimmt. Deshalb ist bei der Cloud der Dinge die Sicherheit oberstes Prinzip. Sie wird durch einen umfangreichen Maßnahmenkatalog gewährleistet: Sämtliche Daten werden auf Servern in hochsicheren Rechenzentren in Deutschland gespeichert und unterliegen dem strengen deutschen Datenschutz. Übertragungen von Sensordaten laufen generell verschlüsselt. Für Sicherheit sorgen standardisierte Verfahren für Datenschutz und Sicherheit, Schutzkonzepte für Infrastruktur und IT-Systeme sowie die Absicherung von Netzen und Kommunikationsschnittstellen.

Device Management
Das Device Management in der Cloud der Dinge liefert einen Überblick über alle angeschlossenen Geräte, ihren aktuellen Betriebszustand und den Fluss der Nutzdaten. So wird kein Update vergessen und Sicherheitslücken werden vermieden. Das Gerätemanagement hilft auch beim Erkennen von Anomalien oder Angriffen (Intrusion Detection) und benachrichtigt den Administrator automatisch bei Sicherheitsverletzungen.

Fernwartung von Geräten aus der Cloud der Dinge
Über die Cloud der Dinge lassen sich IoT-Geräte aus der Ferne warten und dadurch alle Komponenten einschließlich Firmware und Betriebssystem auf aktuellem Stand halten. Dabei werden auch potenzielle Sicherheitsrisiken behoben, die sich durch neue Angriffstechniken ergeben könnten. Per Fernwartung lassen sich zudem – ohne hohen personellen, zeitlichen und finanziellen Aufwand – schwer erreichbare Maschinen mit Updates versehen und vor möglichen Gefährdungen schützen.

2. SICHERHEIT UND DATENSCHUTZ BEI DER DEUTSCHEN TELEKOM

Zwei dedizierte Unternehmensbereiche sind bei der Telekom ausnahmslos für die Sicherheit der Kunden da: Group IT Security (SEC) und Group Privacy (GPR). Die SEC trägt die Verantwortung für die technische Sicherheit: Sie legt ein angemessenes Sicherheitsniveau fest und setzt es mit geeigneten Maßnahmen um. Die GPR bestimmt die strategische Ausrichtung des Konzerns in Fragen des Datenschutzes und definiert dabei die Anforderungen aus rechtlicher, technischer und organisatorischer Sicht. Außerdem vertritt sie zudem den Konzern in allen Angelegenheiten des Datenschutzes nach innen und nach außen. Das Datenschutz-Managementsystem der Telekom ist nach IDW PS 980 zertifiziert.

2.1 SICHERE PROZESSE DURCH DAS PSA-VERFAHREN

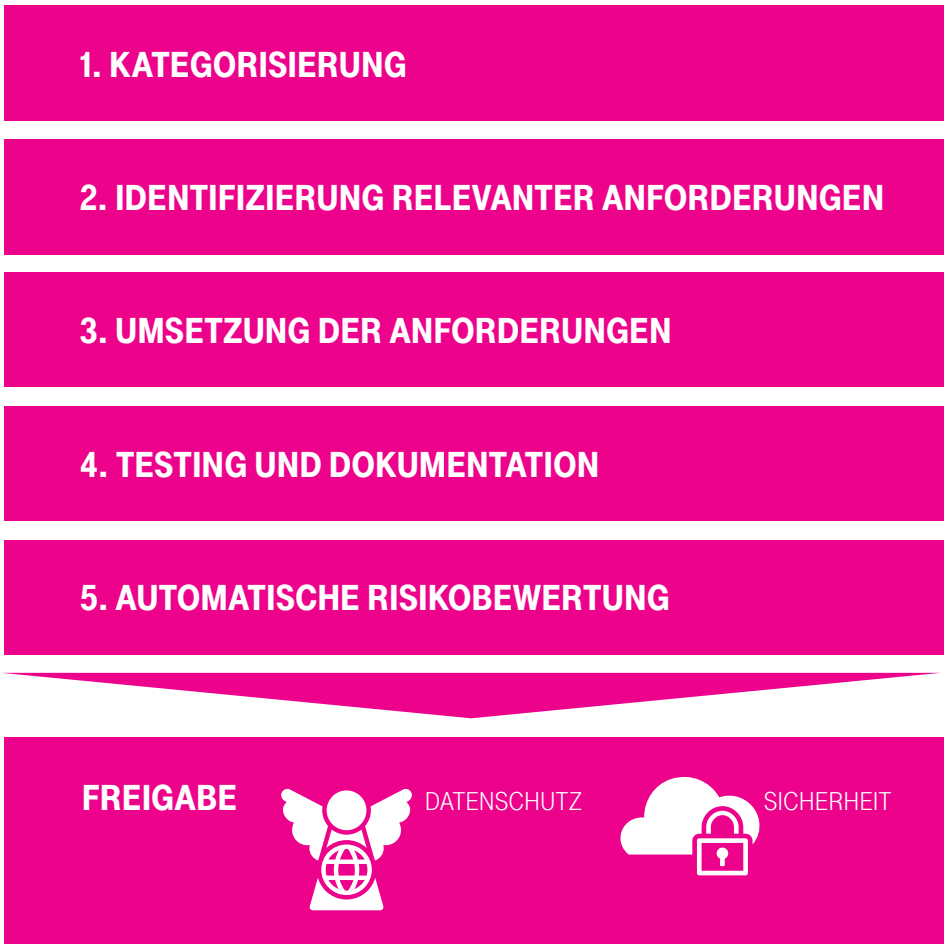
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat einen Katalog von Maßnahmen entwickelt, mit denen Unternehmen die Sicherheit von Anwendungen, Netzen, IT-Systemen und Infrastrukturen umsetzen können. Darauf basierend – und auf den Anforderungen der europäischen Aufsichtsbehörden an das Risikomanagement zum Datenschutz im Unternehmen – hat die Deutsche Telekom einen Standardprozess für alle Telekom-Produkte etabliert: das Privacy and Security Assessment, kurz PSA.

Das PSA-Verfahren gewährleistet die Integration von Sicherheit und Datenschutz in die Produkt- und Systementwicklung und kommt bei jedem Release der Cloud der Dinge zur Anwendung. Dieses standardisierte Verfahren der Telekom beinhaltet sowohl Beratung, Testing und Dokumentation als auch Risikobewertung und Freigaben.

Anhand eines Fragebogens wird zu Prozessbeginn die Datenschutz- und Sicherheitsrelevanz eines Projekts festgelegt. Die Kategorisierung (A, B, C) basiert auf Eigenschaften wie der Verarbeitung besonders sensibler Daten, der Komplexität der Plattformen und Systeme oder der strategischen und finanziellen Bedeutung. Je kritischer und komplexer ein Projekt, desto umfassender ist der Beratungs- und Betreuungsansatz seitens der Bereiche Datenschutz und Datensicherheit. Die Cloud der Dinge wurde in Kategorie A eingestuft und muss somit die höchsten Anforderungen erfüllen.

„Unsere Kunden, unsere Aktionäre, die Aufsichtsbehörden und die Öffentlichkeit erwarten zu Recht, dass wir mit den uns anvertrauten Daten unserer Geschäftspartner, Kunden und Mitarbeiter sorgsam umgehen. Wir setzen alles daran, diese Erwartung nicht nur zu erfüllen, sondern das Vertrauen in uns weiter auszubauen. Datenschutz und Informationssicherheit sind für uns nicht nur Pflicht, sondern ein besonders wichtiges Anliegen. Darauf können Sie sich verlassen!“

Dr. Claus-Dieter Ulmer,
Konzernbeauftragter für den Datenschutz des Telekom-Konzerns



Das PSA-Verfahren im Überblick

THE AUDIT COMPANY

„Im Rahmen der ISO-27001-Zertifizierung des zentralen Sicherheitsmanagements der Deutschen Telekom wurde auch das PSA-Verfahren als ein Leistungsprozess des Bereichs Group IT Security vorgestellt. Das Verfahren wurde im Zertifizierungsverfahren als eine gute und sinnvolle Möglichkeit zur priorisierten Bearbeitung von Entwicklungsprojekten in Hinsicht auf Datenschutz und Sicherheit positiv bewertet.“

Peter Rothfeld und Ingo Vasen, externe Auditoren der DQS GmbH,
Deutsche Gesellschaft zur Zertifizierung von Managementsystemen

2.2 STANDARDISIERTES SICHERHEITS- UND DATENSCHUTZKONZEPT

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

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

2.3 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.

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 und Produktentwicklungsprozesse für die Cloud der Dinge 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
Ebenfalls zertifiziert – vom TÜV Rheinland – wurde das „Zero Outage“-Programm der Telekom. Es wurde bereits 2011 aufgelegt, um Ausfällen von IT-Systemen vorzubeugen. Schon eine Stunde Downtime geschäftskritischer IT-Systeme kann schnell einen sechs- bis siebenstelligen Betrag – und Reputation obendrein – kosten. Mit Twin-Core-Rechenzentren, neuesten Technologien und geschultem Personal sorgt die Telekom für eine höchstmögliche IT-Verfügbarkeit von bis zu 99 Prozent und im Fall einer Störung für eine schnelle, kompetente und effiziente Fehlerbehebung.

Hochsicherheitsserver im Rechenzentrum

Honeypots
Parallel dazu hat die Telekom als zentralen Bestandteil ihres Frühwarnsystems sogenannte Honeypots installiert. Diese „Honigtöpfe“ sind aus dem Internet erreichbare, isolierte Serversysteme, die keine Verbindung zu den realen Systemen der Telekom haben.

Die Honeypot-Systeme sind selbstlernend: Sie zeichnen unbekannte Angriffe auf und analysieren sie. Diese Analysen nutzen die Experten der Telekom, um schädliche Angriffe auf die realen Systeme des Unternehmens abzuwenden und Kunden zu informieren, deren Rechner möglicherweise Teil eines Botnetzes geworden sind. Die Methode hat Erfolg: Bis heute haben die Honeypots keine Verwundbarkeiten an Systemen der Deutschen Telekom aus dem Internet entdeckt.

„Mit dieser konsolidierten Dokumentation von Datenschutz- und Sicherheitsaspekten und ergriffenen technisch-organisatorischen Maßnahmen liegt die Deutsche Telekom deutlich über dem üblichen Standard. Aus unserer langjährigen Erfahrung in der Prüfung und Zertifizierung ist das SDSK als äußerst positiv zu bewerten.“

Monika Wojtowicz, Projektleiterin Datenschutz-Zertifizierung für Cloud-Dienste bei der TÜV Informationstechnik GmbH

3. SICHERHEIT IN DER CLOUD DER DINGE

Zusätzlich zu den konzernweiten Sicherheitsstrategien bei der Deutschen Telekom wird die IoT-Plattform Cloud der Dinge durch spezielle Maßnahmen vor potenziellen Risiken geschützt.

3.1 IT-SYSTEME

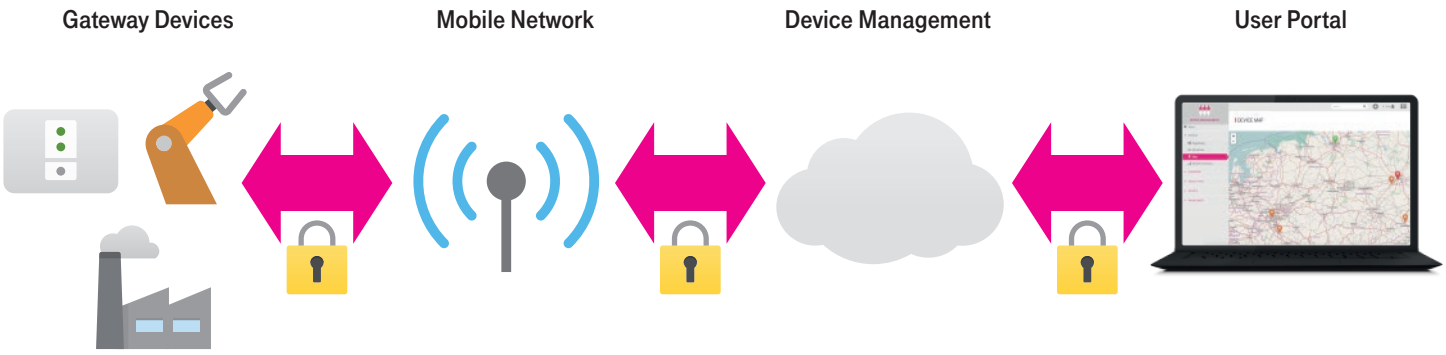
Die in den IT-Systemen der Telekom verwendeten Betriebssystemkerne und Softwarekomponenten unterliegen höchsten Anforderungen an die Pflege von Softwareständen und den Schutz vor Viren und Malware. Die können ausschließlich aus dem internen Netz und über Virtual Private Networking (VPN) administriert werden und sind insbesondere nicht aus dem Internet erreichbar. Alle Daten werden verschlüsselt gespeichert.

Ständige Pflege und Kontrolle
Alle Komponenten wie Betriebssysteme, Datenbanken oder Application Server werden aktiv gemanagt und unterliegen ständiger Kontrolle. Rechte für die Administration der IT-Systeme werden spezifisch vergeben.

Überlastschutz
Die IT-Systeme der Cloud der Dinge 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 überprüfen unabhängige Experten die IT-Systeme auf die Einspielung der neuesten Softwarestände und -patches. Im Rahmen dieser Überprüfung simulieren sie mit Penetrationstests gezielt Angriffe, um in der Vorgehensweise eines potenziellen Angreifers zu versuchen, in die Systeme einzudringen.

SICHERE ÜBERTRAGUNG IN DER CLOUD DER DINGE



3.2 SICHERHEIT IM NETZ

Ein potenzielles Angriffsziel für Cyberattacken sind die Netzwerkverbindungen zwischen dem Browser des Kunden und der Cloud der Dinge 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 Kommunikation
Die Verwendung eines anerkannten und standardisierten Authentifizierungsmechanismus stellt sicher, dass sich kein Dritter in die Kommunikation zwischen einem IoT-Gerät oder dem Browser des Kunden und der Cloud der Dinge einschalten kann. Vor jeder Kommunikation über ein Netzwerk weist die Cloud der Dinge ihre Identität durch ein Zertifikat nach. Zertifikate stellen sicher, 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 der Dinge 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).

Verschlüsselung mit AES
Die gesamte Datenkommunikation der Cloud der Dinge 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 der Dinge 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 der Dinge weitere Verschlüsselungsverfahren wie 3DES oder Camellia.

Die starke Verschlüsselung stellt sicher, 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 Lkw 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 der Dinge 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 der Dinge verwendet ein mehrstufiges 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 der Dinge. Die Sicherheitsexperten der Telekom überprüfen die Firewalls regelmäßig mit Penetrationstests: So werden Schwachstellen aufgedeckt und geschlossen. Hacker haben keine Chance, die Firewalls auf diese Weise zu durchbrechen.

3.3 ZUSÄTZLICHE MASSNAHMEN FÜR ERHÖHTEN SCHUTZ

Eine weitere Angriffsfläche bieten die Schnittstellen zur Cloud der Dinge. 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 der Dinge 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.

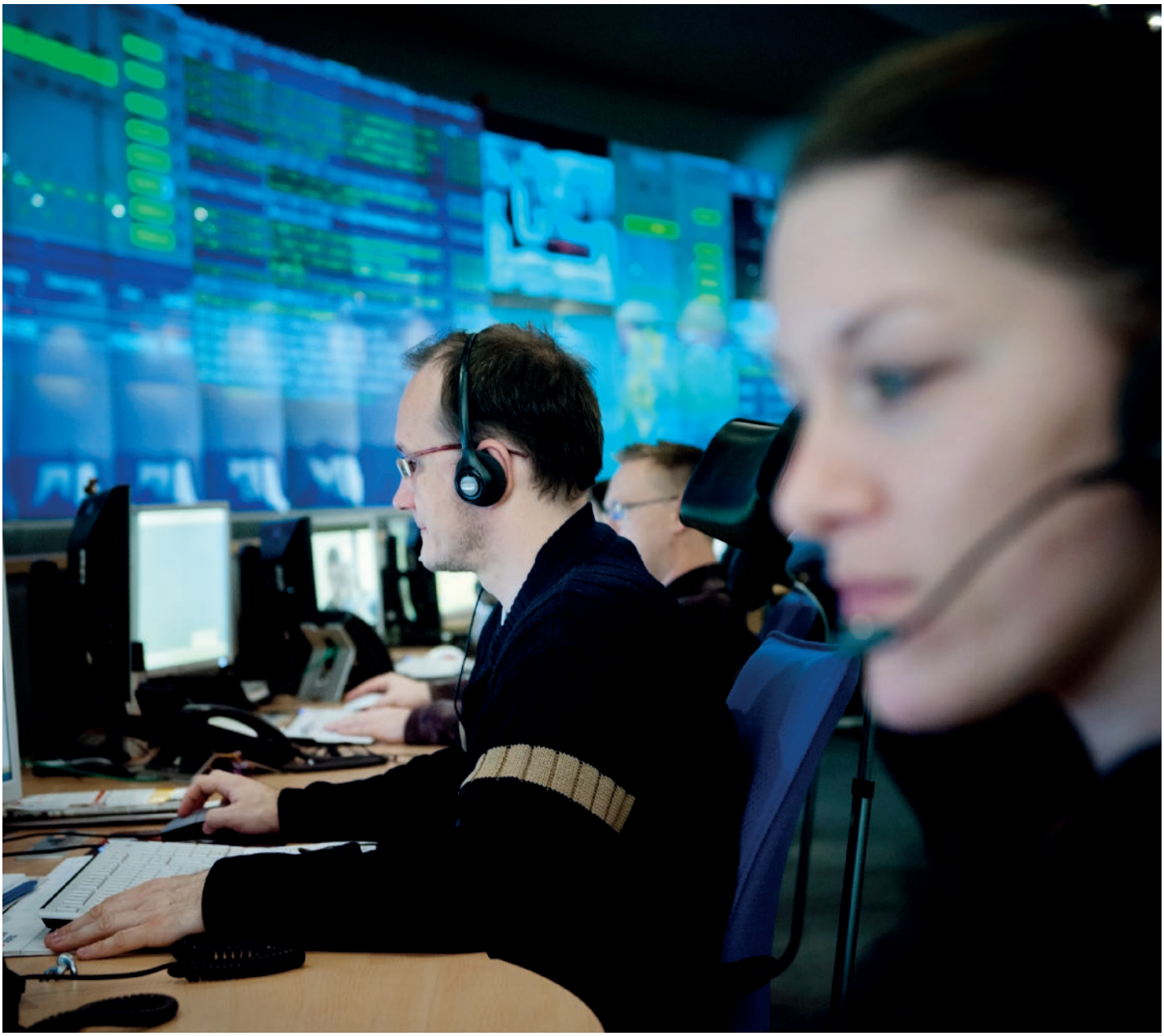
Trennung von Nutzerdaten und Nutzdaten
Eine zweite Trennung schützt vor Datenspionage oder -manipulation: Innerhalb eines jeden Tenants werden Kunden- und Nutzerdaten getrennt von den Nutzdaten verwaltet und abgelegt. In der Cloud der Dinge ist es somit nicht möglich, etwa bei der Übermittlung einer GPS-Position (= Nutzdaten) heimlich einen Datenbankbefehl mitzusenden, um den Namen des Kunden zu erhalten (= Kundendaten) und für andere Zwecke zu nutzen.

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.

Keine eingebauten Hintertüren
Die Cloud der Dinge hat wohldefinierte und abgesicherte Schnittstellen für manuelle Nutzer über das Cockpit und für Geräte über die Softwareschnittstellen. Darüber hinaus gibt es in der Cloud der Dinge keine zusätzlichen Ports oder andere eingebaute Hintertüren – weder für Kunden mit eigenen Schnittstellen noch für die Deutsche Telekom bezüglich Wartung und Administration. Alle Anfragen müssen über die standardmäßig verwendeten Ports und somit über die gleichen Firewalls und Sicherheitsmechanismen abgewickelt werden. Auch Anfragen zur Administration und Wartung haben keine eigenen Schnittstellen, die sich von einem Angreifer ausnutzen lassen könnten.

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

Zertifizierungsprozess für IoT-Geräte
Die Experten der Telekom prüfen und zertifizieren alle IoT-Geräte der Businesspartner, die für die Nutzung in der Cloud der Dinge infrage kommen. Für diese Geräte ist daher sichergestellt, dass sie die Anforderungen an technische Sicherheit und Datenschutz 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.



Mitarbeiter im Rechenzentrum

4. TIPPS FÜR SICHERES ARBEITEN IM INTERNET DER DINGE

Die Deutsche Telekom sorgt mit einem umfangreichen Maßnahmenkatalog für höchstmögliche Sicherheit in der Cloud der Dinge. Doch die sicherste Plattform nützt nichts, wenn die IT-Umgebung des Kunden nicht ausreichend geschützt ist. Diese Checkliste soll 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 der Dinge – 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. Die Deutsche Telekom unterstützt Sie dabei gerne!

- **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

Ohne das Internet der Dinge kann es keine digitalisierte Industrie 4.0 geben – und ohne Sicherheit kann es kein Internet der Dinge geben. Unternehmen wollen einerseits die Vorteile einer Cloud-basierten IoT-Plattform nutzen, um ihr Geschäftsmodell zukunftsfähig zu machen. Andererseits wollen sie aber absolut sichergehen, dass Firmen-, Kunden- und Sensordaten nicht in falsche Hände geraten.

SICHERHEIT UND DATENSCHUTZ BEI DER DEUTSCHEN TELEKOM

Die Deutsche Telekom hat deshalb auch für ihre IoT-Plattform Cloud der Dinge die Sicherheit zum obersten Prinzip erhoben. Konzernweit sorgt das Privacy and Security Assessment für die Integration von Datensicherheit und Datenschutz in die System- und Produktentwicklung. Für die Rechenzentren, aus der die Cloud der Dinge bereitgestellt wird, gelten die höchsten Sicherheitsstandards: 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 DER DINGE

Ein spezieller Maßnahmenkatalog schützt die Cloud der Dinge zusätzlich. Betriebssystem und Software werden geimpft gegen Viren und Malware. 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 gemanagt. Außerdem ist die Plattform durch eine mehrstufige Firewall vor unbefugtem Zugriff geschützt.

Die einzelnen Module der Cloud der Dinge arbeiten völlig unabhängig voneinander. Attacken auf ein Modul können so nicht auf andere Module übergreifen. Auch die Kundenkonten werden getrennt verwaltet: Kein Nutzer kann auf den Bereich eines anderen Nutzers zugreifen. Ebenfalls unabhängig sind Kunden-, Nutzer- und Nutzdaten gespeichert. Von den Nutzdaten lässt sich nicht auf einen Nutzer schließen; der Datenschutz ist stets gewährleistet. Mit diesem umfangreichen Sicherheitspaket ebnet die Deutsche Telekom den Weg von Unternehmensanwendungen ins Internet der Dinge.

GLOSSAR

3DES – Triple Data Encryption Standard: Vorgänger von AES.

AES – Advanced Encryption Standard: Verschlüsselungsverfahren mit einem sehr hohen Maß an Sicherheit.

BSI – Bundesamt für Sicherheit in der Informationstechnik.

Camellia: Ein symmetrisches Blockverschlüsselungsverfahren 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.

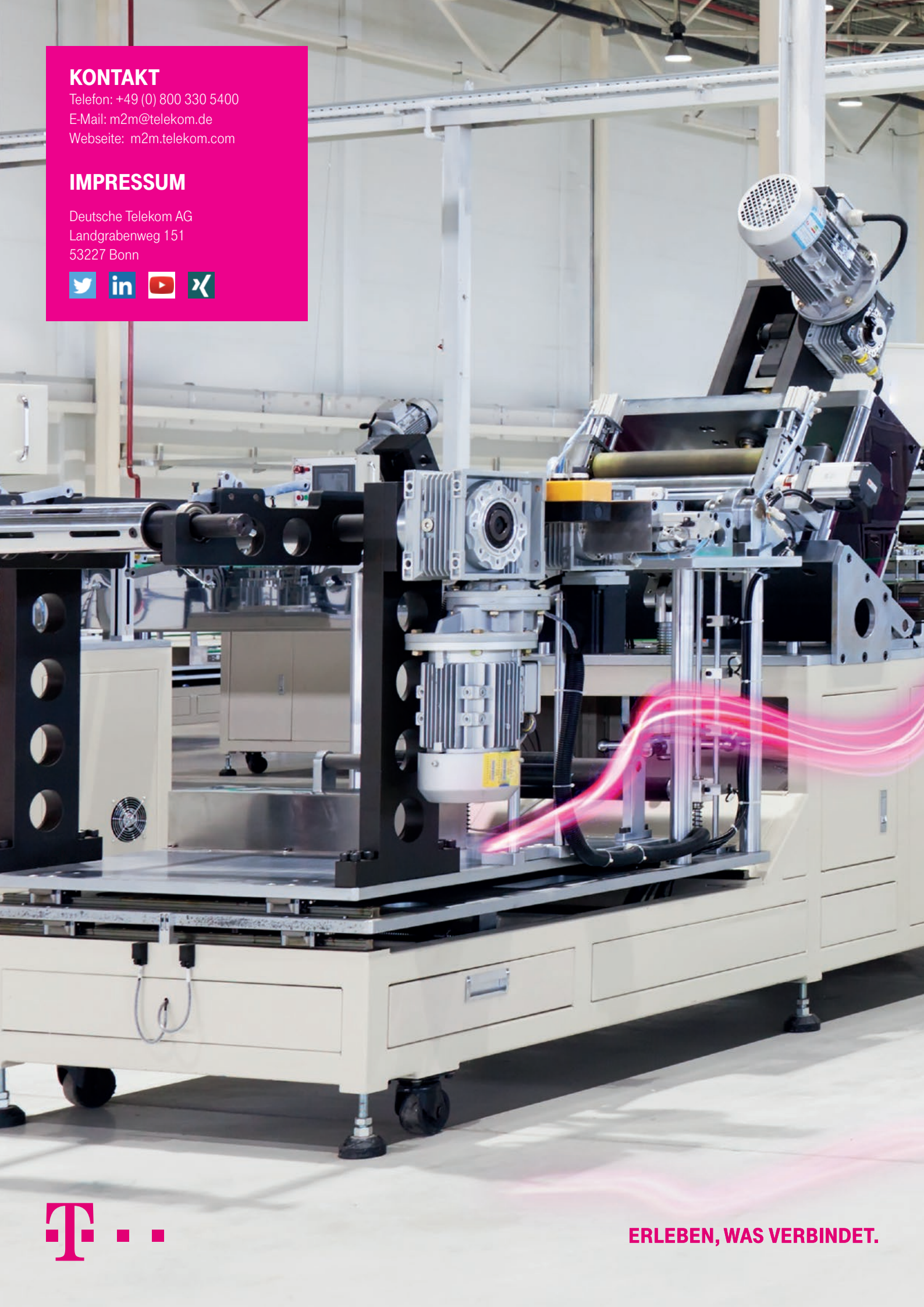
PKI – Public Key Infrastructure: Ein System zum Ausstellen, Verteilen und Überprüfen von digitalen Zertifikaten zur Authentifizierung mithilfe eines Paares von öffentlichen und privaten Kryptografieschlüsseln.

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

Telefon: +49 (0) 800 330 5400
E-Mail: m2m@telekom.de
Webseite: m2m.telekom.com

IMPRESSUM

Deutsche Telekom AG
Landgrabenweg 151
53227 Bonn

ERLEBEN, WAS VERBINDET.