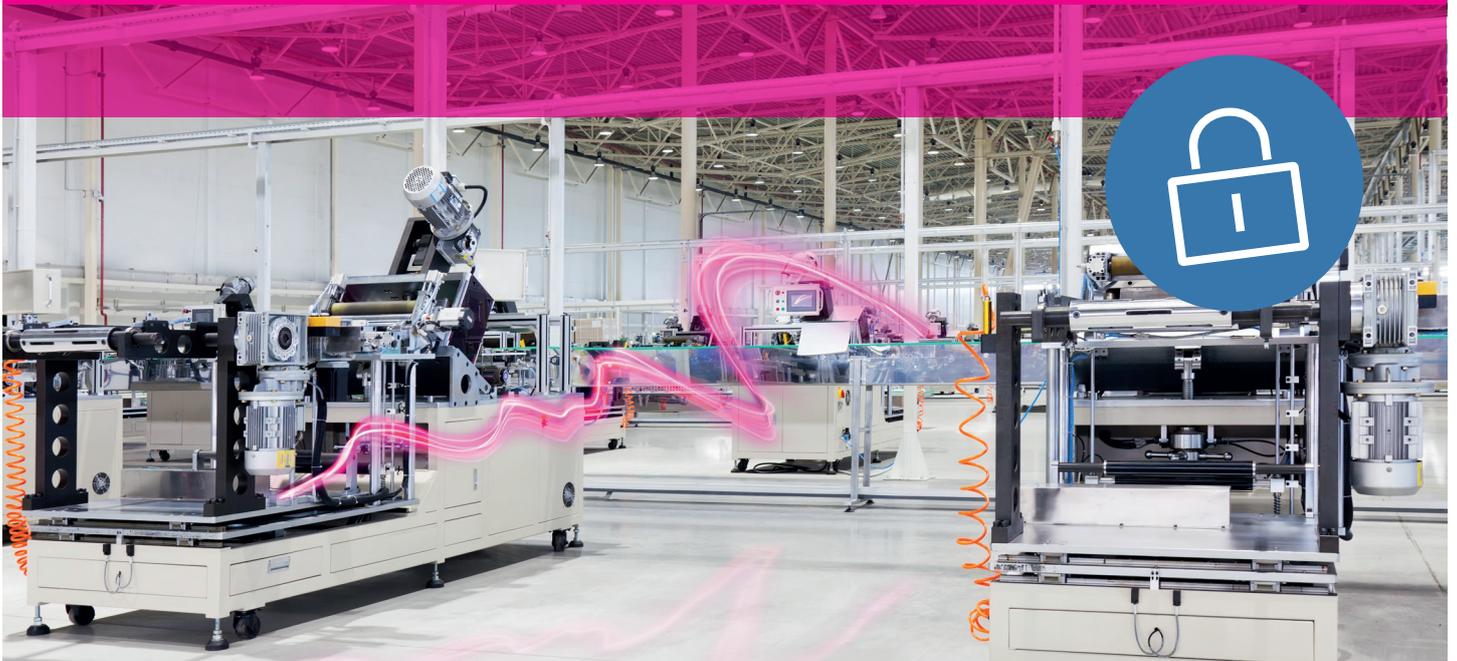


# CLOUD DER DINGE – SICHERHEIT FÜR IHRE DATEN



Wenn sich Menschen und industrielle Prozesse intelligent vernetzen und sich Informations- und Kommunikationstechnik verzahnen, dann sprechen wir von Industrie 4.0. Das Internet der Dinge bildet die Grundvoraussetzung für den reibungslosen Ablauf. Damit die Vorteile einer cloudbasierten IoT-Plattform für Unternehmen im vollen Umfang nutzbar und Geschäftsmodelle zukunftsfähig gemacht werden können, müssen Firmen-, Kunden- und Sensordaten bestmöglichst geschützt werden. Sicherheit spielt eine immer größer werdende Rolle – die wichtigsten Fakten haben wir hier für Sie zusammengefasst.

## MUSS EINE VERSCHLÜSSELUNG WIRKLICH SEIN?

Natürlich ist das Abschließen der Haustür noch lange kein Garant gegen einen Einbruch – aber je schwieriger Sie den Zugang gestalten, umso besser stehen Ihre Chancen, dass der Einbrecher von seinem Vorhaben ablässt. Dies gilt auch für Ihre Daten. Umso besser Sie Ihre Daten schützen, desto geringer ist das Risiko, dass diese in die falschen Hände fallen.

Ähnlich verhält es sich beim Thema Datenverschlüsselung. Leider gibt es auch hier keine Garantie, dass Angreifer nicht doch einen Zugang zu Ihren Daten finden. Wichtig ist, dass der Angreifer selbst in diesem Falle, dank der Verschlüsselung, die Daten nicht lesen kann. Die Datenverschlüsselung schützt ebenso davor, dass weder Veränderungen vorgenommen, noch Fälschungen in den Umlauf gebracht werden. Ihr System und Ihre Daten sind selbst im Fall der Fälle geschützt.

## WARUM DIE CLOUD DER DINGE DER TELEKOM? IHRE VORTEILE AUF EINEN BLICK.

- Standardisierte Sicherheits- und Datenschutzkonzepte durch eigenes PSA Verfahren der Telekom (Privacy and Security Assessment)
- Modernste Rechenzentren in Deutschland – nach höchsten Telekom Sicherheitsstandards
- Multi-Tenancy zur Trennung von Kundendaten in vollständig separierten Datenbereichen
- Freigabe je Release durch Telekom Security Experten
- Prüfung und Qualifizierung von IoT-Geräten in Verbindung mit der Cloud der Dinge

# DIE SICHERHEIT IHRER DATEN HAT OBERSTE PRIORITÄT – UNSERE MASSNAHMEN MACHEN DIE CLOUD DER DINGE NOCH SICHERER.

## HÖCHSTE SICHERHEITSSTANDARDS – EIN MUSS!

Potenzielle Angriffsziele für Cyberattacken sind meistens Netzwerkverbindungen zwischen dem Browser des Kunden und der Cloud der Dinge. Auch die Funkstrecken zwischen den Geräten sind gefährdet. Spionage- oder Sabotageversuche finden hier vielfältige Angriffspunkte – mit gravierenden Folgen für Unternehmen. Neben dem Ausspähen und der Manipulation von Daten kann auch das Image eines Produktes oder sogar des ganzen Unternehmens zerstört werden. Umso wichtiger ist hier die Sicherheit Ihrer Daten.

Aus diesem Grund hat, für die Telekom und ihre IoT-Plattform „Cloud der Dinge“, Sicherheit die höchste Priorität. Das „Privacy and Security Assessment“ Verfahren (PSA) sorgt konzernweit für die Integration von Datensicherheit und Datenschutz in System- und Produktentwicklung. Die Rechenzentren verfügen über ein Frühwarnsystem, welches vor Cyberattacken schützt. Die Infrastruktur wird durch einen umfassenden Gebäudeschutz sowohl vor unberechtigtem Zugriff geschützt als auch vor unvorhergesehenen Ereignissen wie Brand, Wassereintrich oder Stromausfall.

## EIN UMFANGREICHES SICHERHEITSPAKET EBNET DEN WEG VON UNTERNEHMENSANWENDUNGEN INS INTERNET DER DINGE

Ein spezieller Maßnahmenkatalog schützt die Cloud der Dinge zusätzlich:

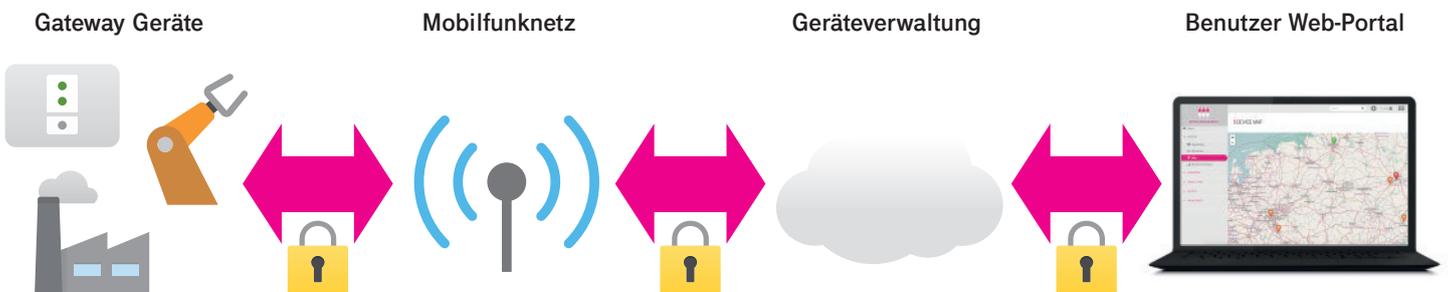
- Betriebssystem und Software werden gegen Viren und Malware geimpft
- Die Daten werden Ende-zu-Ende (AES) verschlüsselt übertragen und vor jeder Netzwerkkommunikation findet eine TLS-Authentifizierung in beide Richtungen statt
- Dank aktiv gemanagter Datenbanken und Server ist die IT gegen DDoS-Angriffe geschützt
- Eine mehrstufige Firewall bietet Schutz vor unbefugtem Zugriff
- Attacken auf Cloud der Dinge-Module können nicht aufeinander übergreifen, da alle völlig unabhängig voneinander arbeiten
- Kundenkonten werden getrennt verwaltet. Kein Nutzer kann auf den Bereich eines anderen zugreifen
- Kunden-, Nutzer- und Nutzdaten werden getrennt gespeichert, was den Datenschutz gewährleistet

## TLS-AUTHENTIFIZIERUNG

Die Verwendung des anerkannten und standardisierten Authentifizierungsmechanismus stellt sicher, dass sich kein Dritter in die Kommunikation mit der Cloud der Dinge einschalten kann. Dabei kommt das „Transport Layer Security“ (TLS) Protokoll zum Einsatz. Die Kommunikationspartner überprüfen ihre Authentizität über Zertifikate und stellen eine verschlüsselte Verbindung her. Einer Quelle, die nicht hinreichend ihre Identität ausweisen kann, wird aus Sicherheitsgründen nicht vertraut.

## VERSCHLÜSSELUNG MIT AES

Der in den USA als Standard für höchste Geheimhaltungssicherheit zugelassene Algorithmus „Advanced Encryption Standard“ (AES) verschlüsselt die gesamte Datenkommunikation zwischen den IoT-Geräten und der Plattform – in beide Richtungen. Für Kunden, deren Geräte kein AES unterstützen, stellt die Cloud der Dinge weitere Verschlüsselungsverfahren wie „3DES“ oder „Camellia“ bereit.



### KONTAKT

- [CloudderDinge@telekom.de](mailto:CloudderDinge@telekom.de)
- +49 800 55 66 900
- [iot.telekom.com](http://iot.telekom.com)

### HERAUSGEBER

Telekom Deutschland GmbH  
Landgrabenweg 151  
53227 Bonn