Pressemitteilung

Neues TÜV SÜD-Whitepaper 20. Juli 2022

Cybersicherheit für Produkte im Internet der Dinge

München. TÜV SÜD hat ein neues Whitepaper veröffentlicht unter dem Titel „Das Internet der Dinge für eine vernetzte Welt. IoT Cybersicherheit – Bedrohungen und Regulierung". Darin erfahren Hersteller, warum die Cybersicherheit bei IoT-Produkten für Konsumenten (CIoT-Produkten) bedeutend ist und welchen Herausforderungen sie gegenüberstehen. Darüber hinaus erläutert TÜV SÜD die geltenden Standards und zeigt, wie der internationale Marktzugang gelingt.

Produkte im Internet der Dinge (Internet of Things – IoT) bieten Komfort und Barrierefreiheit. Gleichzeitig sind vernetzte Geräte und Systeme Cyberrisiken ausgesetzt. Bei Konsumentenprodukten wie Smart Home Gateways, internetfähigen Fernsehern oder Hausüberwachungs- und Beleuchtungssystemen bestehen beispielsweise potenzielle Gefahren für die Datensicherheit oder die Privatsphäre. Sind sie nicht ausreichend gesichert, kann der Hersteller unter Umständen zur Verantwortung gezogen werden.

Mit der wachsenden Nachfrage nach CIoT-Produkten nehmen auch die Risiken zu, da mögliche Sicherheitslücken oder Konstruktionsfehler in einem Gerät stärker ins Gewicht fallen. „Im Jahr 2020 wurden weltweit etwa 11,7 Milliarden IoT-Geräte aktiv genutzt. Bis 2025 werden es voraussichtlich mehr als 30 Milliarden sein", sagt Florian Wolff von Schutter, Leiter IT-Security von CIoT-Produkten bei TÜV SÜD Product Service. „Leider steht dem Marktwachstum aber eine ebenso hohe Zunahme der Schäden durch Cyberkriminalität gegenüber, die bis 2025 auf über 10 Billionen US-Dollar steigen dürften", führt er fort.

Strengere Anforderungen der EU-Funkanlagenrichtlinie

Laut EU-Kommission richten sich gegenwärtig mehr als 80 % aller Cyberangriffe gegen drahtlose Geräte. Mit dem delegierten Rechtsakt zur Funkanlagenrichtlinie (RED) 2014/53/EU wurden daher die Cybersecurity-Anforderungen an diese Produkte erhöht. Dazu gehören beispielsweise Smartphones, Tablets, elektronische Kameras und sogenannte „Wearables" wie Smartwatches und Fitness-Tracker,

aber auch manche Kinderspielzeuge und Babymonitore. Die Verordnung gilt seit dem 12. Januar 2022. Bis zum Ende der Übergangsfrist am 1. August 2024 müssen Hersteller von IoT-Produkten mit geeigneten Maßnahmen die Privatsphäre schützen, das Betrugsrisiko verringern und die Netzstabilität gewährleisten. Da entsprechend harmonisierte Normen bislang fehlen, sollten Hersteller ihre Produkte rechtzeitig von unabhängigen Prüfstellen bewerten lassen.

Herausforderungen meistern

Für den Marktzugang von CIoT-Produkten sind die Anforderungen gestiegen, die unter den „3C" zusammengefasst werden: Connectivity (Konnektivität), Cybersicherheit und Compliance. Beispiele für die Konnektivität sind ein nahtloser Informationsfluss zwischen CIoT-Produkten sowie die Möglichkeit für Upgrades und Aktualisierungen. Zur Gewährleistung der Cybersicherheit zählt der Schutz vor böswilligen Angriffen, zum Beispiel durch eingeschleuste Malware oder solche, die aufgrund schwacher Passwörter oder fehlender Verschlüsselung möglich sind.

Was die Compliance betrifft, müssen Hersteller sich an den Normen und Vorschriften zur Cybersicherheit sowie dem jeweiligen nationalen Recht orientieren. In Europa und teilweise im Vereinigten Königreich gibt es beispielsweise die ETSI EN 303 645, während in den Vereinigten Staaten die NIST IR 8259 zum Tragen kommt und in Indien oder auf anderen Kontinenten wie Australien wiederum andere Leitfäden Anwendung finden. Auch gelten andere Datenschutzgesetze und -verordnungen in den USA als in Europa oder Asien.

Externes Know-how einbinden

Hersteller, die alle geltenden Vorschriften erfüllen, haben langfristig ein größeres Erfolgspotenzial in der IoT-Branche und sichern sich das Vertrauen ihrer Kunden. Auch wenn Hersteller von CIoT-Produkten über eigene Sicherheitsexperten verfügen, sind sie gut beraten, auf externe Dienstleister zurückzugreifen.

TÜV SÜD unterstützt nicht nur bei der Umsetzung von Standards und Richtlinien, sondern bietet auch produktspezifische Risikoanalysen sowie entwicklungsbegleitende Tests. Neben möglichen Bedrohungen für den Datenschutz und die Cybersicherheit kommen dabei auch Aspekte der funktionalen Sicherheit in den Blick. Mit Prüfzeichen wie „TÜV Cybersecurity Certified" (TÜV CSC) weisen Hersteller die hohe Cybersicherheit ihrer Produkte nach und sichern sich einen entscheidenden Marktvorteil.

Link zum Whitepaper (DE): https://www.tuvsud.com/de-de/wissenswert/white-paper/whitepaper-iot-cybersicherheit

Weitere Informationen von TÜV SÜD zur Prüfung und Zertifizierung von IoT-Geräten finden Sie unter:
www.tuvsud.com/de-de/dienstleistungen/cyber-security
www.tuvsud.com/ps-informationssicherheit

Pressekontakt:

Dirk Moser-Delarami TÜV SÜD AG Unternehmenskommunikation Westendstr. 199, 80686 München	Tel. +49 (0) 89 / 57 91 – 15 92 Fax +49 (0) 89 / 57 91 – 22 69 E-Mail dirk.moser-delarami@tuvsud.com Internet https://www.tuvsud.com/de-de

Im Jahr 1866 als Dampfkesselrevisionsverein gegründet, ist TÜV SÜD heute ein weltweit tätiges Unternehmen. Mehr als 25.000 Mitarbeiter sorgen an über 1.000 Standorten in rund 50 Ländern für die Optimierung von Technik, Systemen und Know-how. Sie leisten einen wesentlichen Beitrag dazu, technische Innovationen wie Industrie 4.0, autonomes Fahren oder Erneuerbare Energien sicher und zuverlässig zu machen. https://www.tuvsud.com/de-de