

## **IoT (Internet of Things) in Gefahr: Neue Sicherheitslücken und deren Auswirkungen**

11.12.2020, 12:05 | Medien & Telekommunikation

Pressemitteilung von: *TDT AG*

Presseagentur: *TDT AG*

---



Michael Pickhardt (Vorstandsvorsitzender der TDT AG)

**Essenbach, 11. Dezember 2020: Mitte dieser Woche sorgten Medienberichte für Unruhe, dass Millionen vernetzter Geräte von gut 150 Herstellern von Software-Schwachstellen betroffen sind. Der Digitalexperte Michael Pickhardt erklärt Ursachen und Schutzmöglichkeiten.**

Das auf Sicherheitsanalysen spezialisierte Unternehmen Forescout Research Labs hat in einer Studie sieben Open Source TCP/IP Stacks untersucht. In vier Stacks wurden teils kritische Sicherheitslücken entdeckt. Insgesamt wurden 33 Sicherheitslücken gefunden, vier davon als kritisch eingestuft.

Ein Fehler in der Implementierung des Netzwerk-Stacks (=TCP/IP stack) ist deshalb gefährlich, weil alle Datenpakete zuallererst vom Netzwerk-Stack verarbeitet werden müssen. Somit kann ein bössartiger Code schon schlimme Folgen haben, bevor weitere Sicherheitsmechanismen überhaupt greifen können. Digitalexperte Michael Pickhardt: „Diese Sicherheitslücken sind teilweise auf qualitativ minderwertige Software-Entwicklung zurückzuführen. Dadurch kann es beispielsweise passieren, dass vertrauliche Informationen in falsche Hände geraten oder Denial-of-Service (DoS)-Attacken stattfinden.“

Die Schwachstellen wurden allesamt in Software gefunden, die hauptsächlich auf embedded Geräten (IoT devices) läuft. Embedded heißt, dass die Geräte klein, in der Regel nicht sehr leistungsstark und nur für eine sehr spezielle Aufgabe gebaut werden. Betrachtet man diesen Markt näher, ist festzustellen, dass eine Vielzahl von Angeboten „fire-and-forget“-Produkte sind, die sich durch einen sehr niedrigen Preis auszeichnen, aber nicht updatefähig sind. Um zukünftig derartige Sicherheitslücken gar nicht erst aufkommen zu lassen, rät deshalb Michael Pickhardt: „Verwenden Sie nur Equipment und Technik, die updatefähig sind – und für die regelmäßig Sicherheitsupdates bereitgestellt werden. Führen Sie diese Sicherheitsupdates unbedingt zeitnah durch!“ Wichtig ist auch zu wissen, dass das Problem nicht in der Open Source-Welt zu suchen ist. Michael Pickhardt: „Das Gegenteil ist der Fall. Gerade weil der Quellcode in dieser Open Source-Welt für alle offensteht, konnten diese Lücken überhaupt gefunden werden!“

## Pressekontakt

Pressekontakt:

Dr. Sascha Priester  
Leiter der Pressestelle / Pressesprecher / Head of Press  
TDT AG  
Siemensstraße 1  
884051 Essenbach  
Tel.: +49 8703 929 102  
Mobil: +49 173 6556882  
Email: [spriester@tdt.de](mailto:spriester@tdt.de)

## Portrait

Michael Pickhardt arbeitet seit dem Jahr 1984 in der Telekommunikationsbranche und ist heute Vorstandsvorsitzender der TDT AG.

---

Link zur Pressemitteilung:

<https://www.openpr.de/news/1201317/IoT-Internet-of-Things-in-Gefahr-Neue-Sicherheitsluecken-und-deren-Auswirkungen.html>