Datensicherheit für das Internet der Dinge

Millionen von Webcams, Fernsehern, Druckern oder Maschinen verfügen heute schon über einen Internetanschluss. Aber nur wenige Hersteller kümmern sich um die Datensicherheit der Geräte. Das Internet of Things (IoT) gilt nach Ansicht vieler Experten als unsicher, die Privatsphäre der Nutzer ist nicht gewährleistet. Ohne großen Aufwand können Hacker mit speziellen Suchmaschinen die ungeschützten Geräte aufspüren und übernehmen. Von Michael Pickhardt, TDT AG

Ein Security-Hersteller hat aktuell IoT-Geräte untersucht und festgestellt, dass in Deutschland von 820.000 Netzwerken mit rund drei Millionen IoT-Geräten über 175.000 Geräte unsicher waren. Darunter 140.000 Router, das sind etwa 17 Prozent. In der Schweiz und in Österreich war die Quote der ungeschützten Router noch höher: Zwischen 33 und 40 Prozent aller Router hatten Schwachstellen. Für die Nutzer ist es schwer, die Sicherheit alleine herzustellen, hier ist die Industrie gefordert. Routerhersteller, die darauf vertrauen, dass die Kunden ihr Passwort nach dem Aufbau schon ändern werden, verhalten sich ebenso fahrlässig wie die Kunden, die aus Bequemlichkeit nichts unternehmen.

Sicherheitslücken in Routern

Die Anforderungen an Router im professionellen Bereich sind unabhängig vom Einsatzgebiet – vom Bankautomaten über die Filialvernetzung bis hin zur rauen Industrieanwendung – immer gleich: Höchste Sicherheit, maximale Verfügbarkeit, unterbrechungsfreie Datenübertragung.

Der Zugang zum Internet ist nach wie vor ein Haupteinfallstor in Unternehmensnetzwerke. Dabei werden keinesfalls nur Großunternehmen Opfer des kriminellen Datendiebstahls. Private Router werden ebenso gekapert wie solche von Verwaltungen oder mittelständischen Unternehmen. Unabhängig von der Anwendung gilt die Devise: Wer sich nicht kümmert, ist anfällig für Angriffe. Und mit der Zahl der vernetzten Geräte wächst auch die Gefahr, denn IoT-Geräte sammeln Daten und Informationen und bieten so ein Einfallstor. Meldungen über Sicherheitslücken in Routern sind alarmierend. Die Schäden reichen von Live-Bildern aus dem Kinderzimmer, über immense Telefonrechnungen durch manipulierte Zugänge bis hin zum Datendiebstahl.

Deutsche Unternehmen im Visier der Angreifer

Deutsche Unternehmen und ihre Produkte sind nach wie vor im Visier der ausländischen Konkurrenz. Schon lange kommen die Einbrecher nicht mehr mit dem Brecheisen, sondern sie

nutzen Sicherheitslücken in den IT-Systemen, um an die wertvollen Daten zu kommen. Jedes zweite deutsche Unternehmen erlebte in den vergangen zwei Jahren einen Spionageangriff oder einen Verdachtsfall, so eine aktuelle Studie zur Industriespionage. Aktuellen Schätzungen zufolge liegen allein in Deutschland die Schäden bei rund 50 Milliarden Euro jährlich.

VPN-Router als Schutz

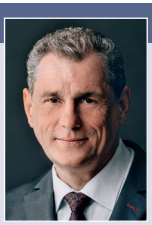
Insbesondere im Small Office/Home Office-Bereich haben Hacker oft leichtes Spiel. Die als Zugaben für einen Internetanschluss mitgelieferten Router sind für den privaten Bereich – so sich die Nutzer um regelmäßige Updates kümmern – ausreichend, nicht aber für professionelle Anwendungen.

Die Gründe dafür sind vielfältig: Das Hauptargument ist die Sicherheit des eigenen Netzwerkes. Experten raten den Nutzern, generell alle vernetzten Geräte in einem VPN (Virtual Private Network) zusammenzufassen. Ein VPN gewährleistet eine sichere Kommunikation der verbundenen Geräte – auch über das Internet hinweg. Professionelle Router bieten hohe Verschlüsselungsstandards ebenso wie die Möglichkeit der Einrichtung von VPN-Netzwerken oder einer sicheren Zugangskontrolle über ein professionelles Netzwerkmanagement.

Im Wettlauf mit den Hackern sind die Anbieter von hochwertigen Routern durch erweiterte Schutz- und Kontrollfunktionen in ihrem System in der Regel immer einen Schritt voraus. Wie bei anderen Bedrohungen auch, hilft es nur bedingt, die Zäune und Hürden immer höher zu bauen, sondern es gilt, die Angreifer intelligent zu erkennen. Gleichzeitig braucht es eine hohe Sensibilität gegenüber dieser Art von virtueller Bedrohung.

Mit der zunehmenden Vernetzung und dem Austausch großer Datenmengen in der Industrie 4.0 steigen auch hier die Sicherheitsanforderungen. Die Anlagen und Produkte müssen ebenso wie die Daten und das Know-how verlässlich vor unbefugtem Zugriff geschützt werden. Als mittelständisches Unternehmen kennt TDT die konkreten Herausforderungen der Wirtschaft aus dem täglichen Geschäft: Sichere Datenübertragung und kompetentes Netzwerkmanagement sorgen dafür, dass die Daten der deutschen Wirtschaft nicht in falsche Hände geraten. □

Der Autor



Michael Pickhardt ist Vorstandsvorsitzender der TDT AG. Das mittelständische Technologie-Unternehmen entwickelt seit 1978 modernste Technik für die Datenkommunikation – beispielsweise High End VPN Gateways für die Hostumgebung, Industrie Class VPN-Zugangsrouter, Mobile Router für die 3/4G-Funknetze und Loadbalancer.