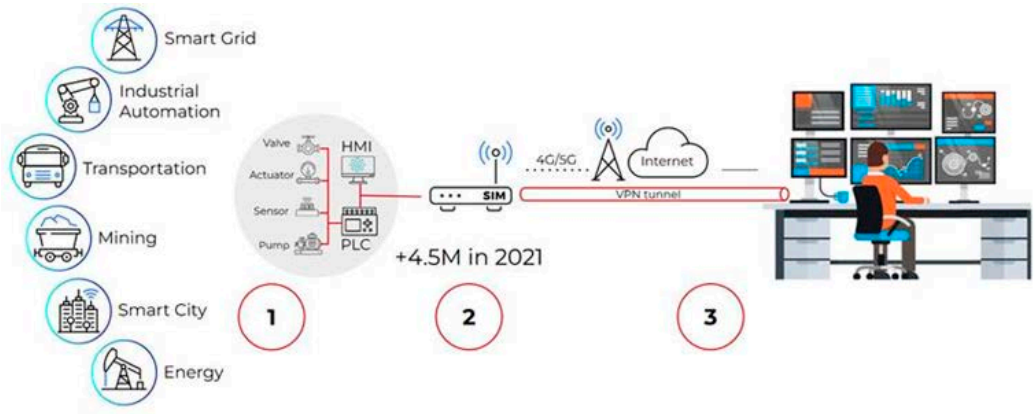
# Schwachstellen aufgedeckt - Schutz für Anwender von Cloud-Management-Plattformen für industrielle Mobilfunk-Router

***Forscher decken Cyber-Risiken in M2M-Protokollen (Machine-to-Machine) und Asset-Registrierung auf, die Hunderttausende von Geräten und OT-Netzwerken externen Angriffen aussetzen***




Otorio, führender Anbieter von Management-Lösungen für Cyber- und Digitalrisiken im Bereich für Operational Technology (OT), hat heute bekannt gegeben, dass drei bedeutende Hersteller von Mobilfunk-Routern für die Industrie Schwachstellen in ihren Plattformen für Cloud-Management aufweisen: Durch diese sind die Betriebsnetze der Kunden externen Angriffen ausgesetzt. Diese Problematik wirft Fragen über die Sicherheit der Verbindung von OT mit der Cloud auf und legt die Notwendigkeit von standardisierten Branchenvorschriften zur Beseitigung solcher Sicherheitsrisiken nahe.

Roni Gavrilov, Security Researcher bei Otorio, hat auf der Konferenz Black Hat Asia 2023, die vom 9. bis 12. Mai im Marina Bay Sands in Singapur stattfand, über wichtige Erkenntnisse und Tipps zur Behebung der Probleme auf diesem Sektor gesprochen (www.blackhat.com/asia-23/).

## Schwachstellen in Cloud-Plattformen

Gavrilov erläutert: ein industrieller Mobilfunk-Router versetzt mehrere Geräte in die Lage, sich über ein Mobilfunknetz mit dem Internet zu verbinden. Solche Router werden häufig in industriellen Umgebungen eingesetzt, zum Beispiel in Fertigungsbetrieben oder auf Bohrinseln, auf denen herkömmliche kabelgebundene Internet-Verbindungen eventuell nicht zur Verfügung stehen oder nicht zuverlässig sind. Die Hersteller dieser Geräte verwenden Cloud-Plattformen, um ihren Kunden Funktionen wie zum Beispiel Fernverwaltung, Skalierbarkeit, Analysen und Security zu liefern. Die Untersuchung von Otorio ermittelte jedoch 11 Schwachstellen in den untersuchten Cloud-Plattformen, die die Ausführung von Remote-Code und die vollständige Kontrolle von außen über Hunderttausende von Geräten und OT-Netzwerken ermöglichen – in einigen Fällen sogar über solche, die nicht aktiv für die Nutzung in der Cloud konfiguriert sind.

## Hohe Infektionsgefahr

„Da der Einsatz von IIoT-Geräten immer beliebter wird, ist es besonders wichtig, sich darüber klar zu sein, dass die Plattformen von Cloud-Management von Bedrohungsakteuren ins Visier genommen werden können“, erläuterte Gavrilov auf der Konferenz. „Eine einzelne IIoT-Plattform eines Herstellers, die für die Zwecke der Angreifer ausgenutzt wird, könnte als Dreh- und Angelpunkt für sie funktionieren und auf Tausende von Umgebungen gleichzeitig zugreifen.“

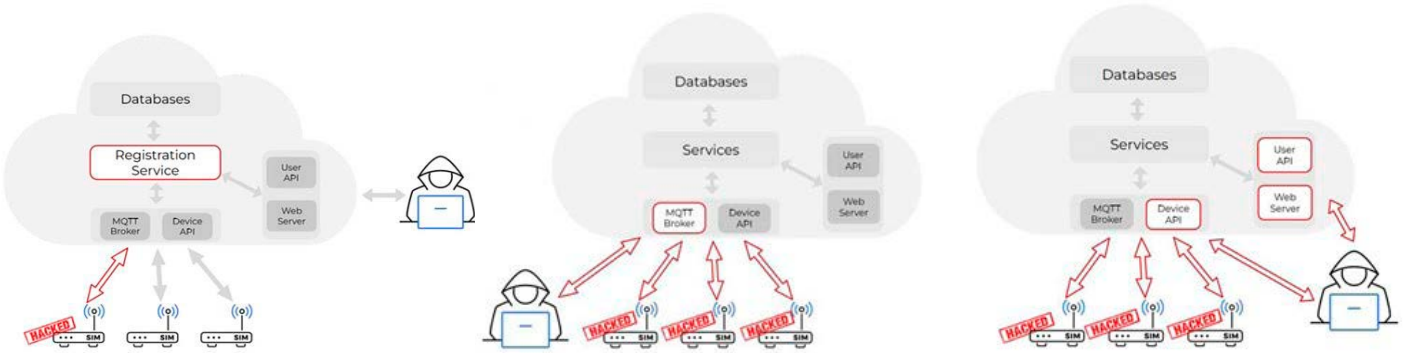
## Angriffsvektoren

Otorio entdeckte bei seinen Untersuchungen eine breite Palette von Angriffsvektoren, die auf dem Sicherheitsniveau der Cloud-Plattform des jeweiligen Anbieters beruhen. Darunter sind auch mehrere Schwachstellen in M2M-Protokollen (Machine-to-Machine) und schwache Mechanismen zur Asset-Registrierung. In einigen Fällen ermöglichen diese Sicherheitslücken den externen Angreifern folgende Zugriffe:

- Root-Zugriff über eine Reverse-Shell zu erlangen
- Geräte im Produktionsnetzwerk zu kompromittieren, um unbefugten Zugriff und Kontrolle mit Root-Rechten zu ermöglichen sowie
- die Funktionsfähigkeit von Geräten zu beeinträchtigen, um sensible Informationen herauszuschleusen und Operationen wie zum Beispiel einen Shutdown durchzuführen.

Einige Angriffe erfordern Identifikatoren wie zum Beispiel den Zugang zur MAC-Adresse (Media Access Control), die Seriennummer oder die IMEI (International Mobile Equipment Identity), um in mit der Cloud verbundene Geräte einzudringen, andere hingegen nicht. Ein ernsthaftes Problem, das bei allen drei Herstellern auftritt, besteht darin, dass ihre Plattformen Geräte

*OTORIO*
*www.otorio.com*




offenlegen, die nicht für die Verwendung in der Cloud konfiguriert wurden. Darüber hinaus können Attacken auf diese Geräte alle Sicherheitsebenen des Purdue Enterprise Reference Architecture Model für mehrere verschiedene Anbieter umgehen (https://en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture).

## Direkter Weg zu internen OT-Netzwerken

Die heutige Ankündigung folgt auf die von Otorio im Februar diesen Jahres entdeckten drahtlosen IIoT-Schwachstellen, die einen direkten Weg zu internen OT-Netzwerken bieten und es Hackern ermöglichen, die gemeinsamen Schutzschichten in den jeweiligen Bereichen zu umgehen (www.prnewswire.com/news-releases/otorio-to-present-zero-day-research-affecting-operational-technology-environments-at-s4-2023-301741989.html).

## Wer schreibt:

OTORIO entwickelt und vermarktet die nächste Generation von OT-Sicherheits- und digitalen Risikomanagementlösungen.

Das Unternehmen kombiniert die Erfahrung führender staatlicher Cybersicherheitsexperten mit modernsten Technologien für das digitale Risikomanagement, um ein Höchstmaß an Schutz für kritische Infrastrukturen und die Fertigungsindustrie zu bieten. ◀