HOW THIS OIL & GAS COMPANY PROTECTS ITS CELLULAR ASSETS FROM HACKERS

An oil and gas company used routers embedded with SIM cards on pipelines throughout Texas and Oklahoma. These routers provided cellular data access to sensors on pipelines. Suddenly, data usage on the endpoints increased from the usual 50MB per month to 50GB per month, per router.

Cause

The IT staff had been using carrier-provided, public static IP addresses, which are accessible on the Internet. Hackers found those addresses and launched DDOS attacks on the routers.

Solution

MobilSentry was able, via white-listing capability, to limit access to a IoT device to a small set or even a single IP address for communication. Choosing private addresses, rather than public, is a common-sense action but it wasn't enough. The solution lies in the ability to limit access to a finite list of IP addresses, thereby preventing malicious access.

MobilSense assigned private IP addresses to the routers, and the oil and gas company now tracks the routers via MobilSentry™. Real-time analytics offer insight into data usage and MobilSentry™ sends alerts if any router surpasses usage thresholds. The platform allows the organization to blacklist and whitelist routers as needed, which has led to reduced data costs and improved security measures.

To learn more about how real-time analytics can offer insight into your company's data usage.

blog | Kit Livingston | May 18, 2020 4:11 pm | Leave a Comment | Enhanced Mobile Data Management, Enhanced Mobility Management, Mobility Management Solutions