DonRiver

Industry Insight

CSPs must address IoT network security challenges

Opportunities for CSPs, never come without its challenges and the Internet of Things (IoT) is no different. CSPs have extensive possibilities to drive revenues from the barrage of new technology and connections that comes with IoT. Yet, security is still a huge revenue and operational risk.

Security of the network is paramount for the CSP to gain with IoT, however the risk is heightened by the increase in access points and the number of partners.

Protecting your risk

IoT brings with it a vast amount of data that connects to the telecom network through an array of connection points. Depending on the purpose of this data, it links, sends information, enables services, etc.

As CSPs have grown, they have made key partnerships to deliver services and these partners also have access to connect with the CSP network.

Adding to this, some of the data is highly sensitive and is covered by privacy laws, which varies from country to country. Compliance to legislation is one of the biggest risks faced by the CSP.

How important is security for IoT?

The impact of revenue loss and damage to reputation can be significant. And it impacts the end-customer, as well as the CSP - cyber-attacks often hold data for ransom, which can halt operations or cause concern over loss of data.

The seriousness of the situation depends on the nature of the technology. Take autonomous vehicles, control over, or locking owners out of these vehicles can have damaging knock-on effects. Security must be adjusted for IoT technology as part of an ongoing program.

Analyst house Gartner believes that niche technologies are needed for IoT security and that many attempts to use traditional security has failed. “The inordinate focus on devices as primary determinants for security decisions is delivering incomplete or inadequate security prevention, detection, response or prediction for IoT.”

DonRiver

Industry Insight

How can OSS support CSPs?

Monitoring the network is one of the best protection methods for CSPs. With an OSS solution that alerts to network changes or errors, the CSP can ensure every effort is taken to quickly shut down any security breach.

The world is becoming more digital, which provides a wealth of opportunity for CSP revenue. Yet, with it comes cyber threats, hackers who can, utilise technology to make money by corrupting systems and stealing data.

CSPs must take risk management very seriously, especially when new technology, such as IoT is so reliant on connections and data to operate. Customers will only deal with providers that they view to be trusted and secure, so reputation and a robust security and monitoring systems that is tailored to IoT is fundamental for success.

Professional Insight: Kent McNeil.