BIZCOMMUNITY

Cyber security is key to smart metering deployment

By Darren Oxlee

15 Feb 2019

As adoption of advanced metering infrastructure (AMI) becomes more widespread, its appeal to cyber attackers will undoubtedly increase, and addressing security vulnerabilities across layers - and by different stakeholders - must be taken into account from the outset.

Darren Oxlee, chief technology officer and director, Utility Systems

This infrastructure essentially offers an integrated system of smart meters, communications networks, and data management systems that enable two-way communication between utilities and customers. Globally, we are seeing more requirements for automation at end points, as utilities look to remotely diagnose and debug issues in the field.

In theory, every area of any system is open to risk: because AMI allows for bi-directional communication and remote management of in-field devices, security breaches could allow unwanted changes to be made to device configuration and settings.

As such, stakeholders in the ecosystem need to take responsibility for ensuring their respective layer is secure, and that the interfaces between vendors, system integrators and utilities are as impenetrable as possible. AMI systems will have to adopt multi-layer security protocols to provide multi-level protection against potential threats.

AMI often applies to utilities that are of national significance, and failure to adequately secure systems against vulnerabilities can result in dire consequences for stakeholders and end users alike.

Among the challenges that operators face in securing their AMI systems is that there are currently no standards directly relating to AMI. There are, however, standards relating to the various components of an AMI system, and common to ICT installations, that operators still need to adhere to.

Security by design

For example, radio communications is generally covered by IEEE 802.15.4 (the technical standard which defines the operation of low-rate wireless personal area networks), data protection and privacy is covered by (amongst others), the EU’s General Data Protection Regulation (GDPR) or South Africa’s Protection of Personal Information Act (PoPI).

Other related standards that can help improve security of AMI systems include the ISO 27000 family, ISO 15408, RFC 2196, ANSI 62443, IEC 62443 and guidelines from a number of committees including TC CYBER, CISQ, NERC and NIST. The European Union has proposed a standardised cyber security certification framework. It is likely that any locally developed government regulation will be based on standards such as the ones listed above.

Methods currently being used to combat breaches include secure data communications using encryption, secure database design, proper access control using proven authentication methods amongst others. In addition, cyber security is increasingly benefitting from intelligence-driven capability supported by machine learning.

The most important aspect is that each component of the AMI system be designed from the start with security in mind and the ability to adaptively react to threats based on continuous, intelligent risk profiling.

The correct implementation of security best practices prevents, as far as possible, breaches of complex systems, and allows AMI component manufacturers to develop skills in the area of cybersecurity which help protect customers from potential and unwanted cyber-attacks.

However, while utilities may often rely on service providers and vendors to comply with cyber security regulatory requirements, it is incumbent on all parties to adhere to the highest level of security as mandated, by a global standard if possible.

ABOUT THE AUTHOR

Darren Oxlee, chief technology officer and director, Utility Systems