Cybersecurity: utilities at its most vulnerable

By Vladimir Mlovanovic

23 Dec 2021

The evolution of technology has brought incredible advancements, particularly in unprecedented times where both organisations and individuals have had to adapt to stay competitive. But it's a bit of a catch-22; as technology continues to progress, so do cybercriminals become more sophisticated, exploiting the vulnerabilities that come with online, digitised environments.

Vladimir Mlovanovic | image supplied

Municipal utilities are unfortunately a practical example. In the last year, various security reports have warned against an increase in cyber attacks (against utilities) across the globe, citing vulnerabilities and the resultant disastrous effects.

Why utilities?

A utility provides vital services and represents critical infrastructure; it’s an attractive target that can be exploited in many ways by cybercriminals. And unfortunately, recent attacks abroad have demonstrated that utility companies were unprepared and lacked the proper security to protect sensitive data.

Furthermore, recent onslaughts had targeted operational systems and disrupted essential services with a detrimental ripple effect that left many without electricity, water, and other services.

Utilities are also responsible for large amounts of sensitive data which provides cyber attackers with fertile ground to launch attacks on both IT and operational technology (OT) infrastructure. The impact can be devastating, leading to:

- Large-scale power outages;
- Compromised water provision;
- Breach of consumer and employee information;
- Potential damage to infrastructure and networks that could lead to costly repair; and
- Millions of Rands lost due to ransomware demand.

Sound cybersecurity policies

As utilities adopt modern technology to streamline processes, vulnerabilities are exposed. For example, the Industrial Internet of Things (IIOT)) assists companies in the collection of data, providing insights, and improving efficiency and safety; however, it also adds a layer of security weakness if not safeguarded effectively.

Utilities across the globe will benefit from comprehensive cybersecurity policies, tailored to their unique requirements. For one, it's essential to understand where the security gaps lie; a professional assessment will pinpoint the vulnerabilities and provide a customised security plan to plug these holes.

Also, a cybersecurity policy lays out formal security rules which clearly define the obligations of employees, contractors, and other authorised users when it comes to protecting technology and information assets.

It should list and classify hardware and software assets and equipment, identify threats, and assess risk, define information protection rules, describe users' responsibilities, and access such as what's not allowed and the consequences of violating it, and detail incident response plans and teams.

Utilities need to consistently review and update cybersecurity system processes to maintain an effective security baseline.

It's also important when implementing security policy and risk mitigation actions, utilities choose technology based on international standards offer secure-by-design approaches.

Lastly, is establishing a paper trial so to speak. The cybersecurity documentation should include detailed processes, network diagrams, security architectures, and technical documentation supplied by vendors.

It's also essential to possess as-built documentation of deployed systems, approved cybersecurity templates for periodic audits, security risk assessments, as well as engineering, servicing, commissioning, and patch management documentation.

In the end, utilities need to take stock of their security posture particularly in time when cybercriminals have readjusted their aim to exploit a potentially lucrative target.

ABOUT THE AUTHOR

Vladimir Milovanovic, Vice President, Power Systems, Anglophone Africa at Schneider Electric