CERTES NETWORKS

TECHNOLOGY SOUNDBITE

How can the utilities sector prevent a cyber-attack?

HOW CAN THE UTILITIES SECTOR PREVENT A CYBER-ATTACK?

Author: Adrian Niculae, VP Business Development EMEA and Paul Vidic, Director, Certes Networks

As published in *SC Magazine*, September issue.

The Critical National Infrastructure (CNI) is under increasing threat of a cyber-attack. It is completely possible that a global ransomware or a cyber-attack could shut down an entire electrical grid. It's frightening, but it's real, and it's a threat the whole industry is currently facing.

Many recent reports across the U.S. and Europe have exposed the extent of cyber threats and noted how not only are these threats growing and spreading, but a major cyber-attack in this industry is a matter of "when, not if". In the U.K. everyone has heard of the repercussions of the 2017 state-sponsored WannaCry attack which greatly affected the NHS - as well as other organisations, emergency service and manufacturing plants across the globe. This attack and others demonstrate the potential consequences on the power sector, which on this occasion, made many critical services grind to a halt.

This, coupled with the increasing use of automated technology, means that ICS/SCADA networks used by the power industry is under mounting pressure to keep data in transit secure. It's a problem that is becoming the topic of many debates, with almost half of power and utility CEOs surveyed believing a cyber-attack on their company is inevitable.

Additionally, the move towards smart grid technology means that a cyber-attack could result in costly financial loss and long-lasting damage to the organisation's reputation. What's worse, it could impact thousands, if not millions of citizens, reaching far beyond the power sector and potentially putting lives at risk and bringing a nation to a standstill.

In an attempt to combat this, and as new threats are continuously identified, cyber security solutions are being layered to patch network vulnerabilities and keep encrypted data secure. Unfortunately, this method can have the opposite effect, with many organisations being left with weaknesses in their networks which are easy for hackers to exploit. Organisations in the CNI sector recognise that they need to make changes to their network security strategies, but how can this be achieved?

Encryption Management

The power industry is beginning to realize that the need to implement a robust encryption management solution that focuses on protecting the data, rather than the network itself. An encryption solution is required that not only safely encrypts data enterprise-wide but is scalable and easy to implement. And, if this can be done without ripping and replacing your entire network system, imagine the resources and costs you can save.

In reality, it only takes a small virus to infect a critical part of a network and cause havoc while hackers expose and access valuable data. However, if data across a network is encrypted, even if the hacker infiltrates part of a network, there is a high likelihood that the data will be useless to the hacker. Therefore, with correctly defined and enforced policies, IT operators will be able to identify a data breach very quickly and shut down that policy, ensuring further damage cannot be achieved.

Conclusion

The CNI sector does not have to wait for a cyber-attack to happen before making essential changes to its cyber security strategy. It is critical for the CNI to focus on encrypting their data and safeguarding it from any potential infiltrations.
This means a robust security management solution that can encrypt data without disrupting your network and allow operators to define, deploy and enforce policies that assign stringent authorization between applications and users.

Contact Certes Networks

300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108

Tel: 1(888) 833-1142
Fax: 1(412) 262-2574

info@certesnetworks.com
sales@certesnetworks.com

We offer an encryption solution that is simple, scalable and uncomplicated.