Publication: SC Magazine UK
Date: 05.09.2019
URL: https://www.scmagazineuk.com/cni-protected-cyber-attack/article/1593952
Title: How can CNI be protected from a cyber-attack?
Author: Paul Vidic, Director, Certes Networks

How can CNI be protected from a cyber-attack?

By Paul Vidic, Director, Certes Networks

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.

A report released by the government assessing the UK's CNI at the end of 2018 exposed the extent of the threat and noted how not only is the threat to the CNI growing and spreading, but that a major cyber-attack on the UK is a matter of 'when, not if'. 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 provisions and manufacturing plants across the globe – and demonstrated the potential consequences of an attack on the CNI, which on this occasion, made many critical services grind to a halt.

This, coupled with the increasing use of technology within the CNI, means the 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 grinding a nation to a halt.

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

CNI organisations need to have a robust encryption management solution in place 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 the entire network system, imagine the resources and costs that can be saved. In addition, policies and keys should be defined and deployed based on which users should have access to what data; this ensures that only the people who need to send/receive the data have the authorisation to do so.

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 encryption their data and safeguarding from any potential attacks. This means a robust strategy solution that can help encrypt data without disrupting your network and allow operators to define, deploy and enforce policies that ensure stringent authorisation between applications and users.
