USE CASE:

THE EXPANSION OF THE REGULATED ENERGY & UTILITY MARKET

U.S. Public Utility Company

SITUATION ANALYSIS

Cyber security, as it should be, is a concern for all organizations and the energy sector is no different. Stuxnet, a malicious computer worm that targeted SCADA (Supervisory Control and Data Acquisition) systems in 2010, was a watershed moment for the sector and it showed how a cyber-attack can have a serious impact on the physical and digital world.

At Certes Networks we understand that the energy sector is evolving, and its cyber security has to evolve as a result. Power grids are creating many new and complex challenges. New technologies and devices are being integrated with existing hardware and software to improve efficiency and usability. The challenge is that these innovations can also provide a pathway for cyber-criminals. While this may be enhancing efficiency and the customer experience, cyber-criminals are increasingly targeting these innovations to undermine their benefits. It is well-known that Industrial Control Systems (ICS), such as SCADA are central to the operation of infrastructure in electricity, transportation, oil and gas, water, manufacturing, and other critical infrastructure sectors.

Industrial Control Systems (ICS)
ICS are devices, systems networks and controls used to operate and/or automate industrial processes. These devices are often found in nearly any industry from vehicle manufacturing and transportation to the energy and water treatment segment.

Supervisory Control and Data Acquisition (SCADA)
SCADA networks are systems and/or networks that communicate with ICS to provide data to operators for supervisory purposes as well as control capabilities for process management.

As automation continues to evolve and become more important worldwide, the use of ICS/SCADA systems are going to become even more frequent. Such is the case with a U.S. diversified energy and utility company that operates in 23 states that recently contacted Certes Networks regarding our encryption management solutions.

This U.S. company operates regulated utilities and electricity generation through two primary lines of business. One includes electric and natural gas utilities serving 3.1 million customers on the east coast. The second line is a renewables business operating 6.5 gigawatts of electricity capacity, primarily through wind power, in states across the U.S.

In order to promote better compliance practices and to provide staff and the board of directors an understanding of cybersecurity preparedness, the energy company asked Certes Networks to respond to an RFP that focused on some of the following criteria:

Access Rights and Controls – How to maintain more control over security posture in the event of a data breach from a failure to implement basic controls and policies that would prevent unauthorized access to systems and information.

Data Loss Prevention – How to monitor the volume of content transferred outside of an agency by its employees or through third parties, such as email attachments or uploads. How to monitor potentially unauthorized data transfers and verify the authenticity of a customer request to transfer funds.

Security Policies and IR - Best practices for generating, deploying and enforcing policies, including assigned roles, assessed system vulnerabilities, and how to address possible future events. Include which data, assets, and services warrant the most protection to help prevent attacks from causing significant harm.

CHALLENGES

Below are just some of the many challenges that faced our customer, and the energy sector as a whole, highlighting the need for simple, scalable and uncomplicated encryption management solutions that can be easily managed and implemented.

1 UNDERSTANDING THE IMPACT OF INCREASED CYBER-ATTACKS

While data breaches are prevalent, the subject of cyber security in the energy sector should be perhaps greater concern. When service delivery is impacted, it can have a massive and immediate negative effect on the population of a region. This is not a case of financial and reputation loss; it is a case of severe power outages effecting critical services provided to mass populations in rural and urban cities everywhere. To avoid this, the customer wanted to ensure the implementation of a safe and effective encryption management solution.

2 KEEPING PACE WITH TECHNOLOGY INNOVATION IN THE ENERGY SECTOR

The customer realized that as the energy sector evolves, its cyber security has to evolve as a result. Power grids are fast becoming digital jungles and as with any other industry, new technology innovations – like IoT sensors, smart meters and integrated cloud services – are being integrated with legacy hardware and software. While this may be enhancing efficiency and the customer experience, the customer understood that cyber criminals are increasingly targeting these innovations to undermine their benefits.

3 DETECTING THREATS BEFORE THEY HAPPEN

By creating a cyber-security culture our customer wanted to move toward a more sensible approach, versus the normal reactionary method, and define more proactive measures to be used in the event of a breach or a severe infiltration.

The customer wanted new cyber-security technologies implemented that could detect threats before they escalated into a crisis. They also realized that they needed to take these threats seriously by turning to new tools that employ better visibility and observability into their encrypted data and those who were assigned to receive/send data.

SOLUTION REQUIREMENTS

2019 will be an important year for the energy sector. The big challenges will stem from the proliferation of end-user data in the sector combined with its allure and appeal to attackers. It is essential that IT teams continue to be aware of, and responsive to, cyber-security risks; however, there is plenty that energy companies can do starting with establishing a cyber-security culture and taking full control of their system access.

Encryption is a Critical Safeguard Against Cyber Attacks

Encryption is critical to the security of the industrial control systems and the communication channels through which they send/receive sensitive data to keep critical infrastructure functioning. It protects the integrity of data in transit, enables observability of communications channels through which data is sent and received, and enables secure policy assignments to defend against compromise. For example, encryption is used to protect data in transit across the electricity grid, including communications to and from operations centers, power generation systems, distribution substations, and home “smart grid” networks.

THE SOLUTION

SIMPLE, SCALABLE & UNCOMPLICATED

Certes Networks can help the energy sector make the move toward a more secure network ecosystem while encrypting data without the complexity of other solutions. The vulnerabilities and threats associated with protecting large volumes of data moving across a vast multi-user network, involves a security strategy that is simple, scalable and uncomplicated to avoid any disruption to operational functionality and the provision of critical services.

POLICY SEGMENTATION & AUTHORIZATION

Certes CryptoFlow® Network Creator software is a Zero Trust crypto-segmentation software solution that now makes crypto-segmentation possible. Through an easy, drag-and-drop Graphical User Interface (GUI), policies can be defined and deployed quickly and simply. Also, automated key rotations can be scheduled at intervals you choose without staff oversight. Policy generation and key management has never been easier.

OBSERVABILITY

With Certes Observability, organizations can now do more than just try to monitor and identify threats to keep them out of their network. Using Certes Observability, raw data can be used to analyze and gain a deeper understanding of network policy deployment and enforcement to analyze every application that tries to communicate across the network. All of this happens while monitoring pathways for potential threats because each policy is observable in real-time. As most utility companies are under state or national regulations, please be sure to understand what encryption solution will be best for compliance assurance.

THE RESULT

Certes Networks is able to provide a simple, scalable and uncomplicated encryption solution through their Layer 4 technology, which includes placing Certes Enforcement Point (CEP) appliances between Data Centers and substations to encrypt data. This technology can be employed without having to disrupt, move or replace the vast multi-network infrastructure that defines most energy companies.

Our technology solutions are FIPS 140-2 validated and Common Criteria certified which assists in meeting compliance objectives for the next audit cycle. Moreover, the policies defined and deployed through our CFNC software, along with automated key management, will strengthen and provide energy companies with more control over their system access.

CERTES NETWORKS

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.