How Can the Energy Sector Fight Cyber Threats?

69 percent of companies are not confident that they can detect cyberattacks

Dubai - Nov 29, 2017: The energy sector specifically is becoming an increasingly popular target for hackers. According to the Department of Homeland security in the United States, the energy sector faces more cyber-attacks than any other industry. Even more worrying is that 69 percent of companies are ‘not confident’ that they are able to detect these attacks. A supervisory control and data acquisition (SCADA) breach not only leads to a loss of data, but can cause damage to physical assets and even a loss of life, which should be more than enough to prompt companies to make sure they have systems in place that enables them to detect and respond to attacks the moment they happen. SCADA systems are crucial for industrial organizations since they help to maintain efficiency, process data for smarter decisions, and communicate system issues to help mitigate downtime.

In the oil and gas industry across the Middle East, SCADA systems are in frequent use and are responsible for communicating data to operators who make critical decisions based on that information. The growing frequency and complexity of cyberattacks therefore is causing both public and private organisations to question their current IT security strategies. Concerns are being raised about the vulnerability SCADA systems, especially those responsible for critical national infrastructure and business continuity.

A big problem is that much of the existing infrastructure within the energy sector was designed with little or no consideration to cyber threats and implemented prior to the proliferation of the internet. SCADA devices subsequently trust their environment inherently and have a wide attack surface. Their protection was initially planned around the physical safeguarding of critical systems, with no provisions for the possibility of devices running SCADA and associated serial protocols, such as Master and Remote Terminal Units, embedded microcontrollers, sensors, actuators and traditional workstations, later converting to Internet Protocol (IP), and thus being made accessible to untrusted networks.

SCADA vulnerabilities

Many SCADA devices employ very basic, easily defeated authentication methods, transmitting data in clear text, with many cyber assets operating on old and vulnerable code bases. Examples of just how vulnerable SCADA systems are to attack include the recent Ukrainian power grid hack, which led to the first large-scale electricity outage, and the attack on a Ukrainian airport, in which suspicious malware was found on a computer at Kiev’s main airport, Boryspil. Closer the home, the now infamous hacks into Saudi oil and gas systems last year echo the same threats.

Gaining control of a SCADA system could, potentially, have a hugely damaging impact on a country and the increasing connectedness of infrastructure finds control systems being even more vulnerable to cyber-attacks, but also

increases the knock-on effect an attack can have on other infrastructure sectors and capabilities. The situation is not likely to improve – as hackers will continue to target systems that require little effort on their part, yet have a large widespread impact.

Changing strategies

What we often find is that those managing critical national infrastructure are relying on security strategies that are out of date and becoming increasingly obsolete. It is a dangerous misconception to think that using point-based perimeter tools, such as anti-viruses and firewalls are sufficient, especially when it comes to these industries that have such a huge impact on a country's economic stability and development.

Today's hackers are becoming increasingly persistent in their approaches and using extremely sophisticated tactics to exploit existing vulnerabilities. Sticking with basic security solutions may have worked in the years before cyber-attacks became one of – if not, the – biggest threat to national security, but this is no longer sufficient. If hackers are finding new, innovative ways to get into IT systems, then logic would dictate that companies need to find new, innovative ways of protecting their IT systems. Unfortunately, avoiding a breach completely is unrealistic, but there are ways to take control and mitigate any subsequent damage.

The intelligent solution

With attacks now a case of when, not if, those running SCADA control systems need to direct their attention to identifying a breach and rectifying the issue as quickly as possible. The time between detection and response is when systems are at their most vulnerable, and without a strategy in place to effectively and efficiently deal with the problem, the consequences could be far reaching.

Critical national infrastructure needs security intelligence, which ensures that all systems are continuously monitored so any type of compromise can be identified and dealt with as soon as it arises. Indeed, SCADA systems tend to be controlled across a variety of geographic locations, therefore, having a centralised system that can provide full visibility across all IT network activity in real-time is vital for the management of security.

Critical national infrastructure will continue to be a top target for hackers, and we cannot afford to have over two thirds of the energy sector not knowing if they can stay safe. Only by taking an approach capable of monitoring and analysing network activity in real-time can sophisticated attacks attempting to control SCADA systems be effectively detected, remediated and correctly attributed before any significant damage is done. This is especially true in situations where political tensions are high and cyberwars are viewed as less costly than conventional wars.

ENDS

About LogRhythm:
LogRhythm, a leader in security intelligence and analytics, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyber threats. The company's patented award-winning threat lifecycle management platform uniquely unifies next-generation SIEM, log management, network and endpoint monitoring, user entity and behavior analytics (UEBA), security automation and orchestration and advanced security analytics. In

Phone +971 (4) 337 2824
Email info@tcf-me.com
P.O. Box 29764
Dubai, United Arab Emirates
Fax +971 (4) 337 2825

addition to protecting customers from the risks associated with cyber threats, LogRhythm provides unparalleled compliance automation and assurance, and enhanced IT intelligence.

LogRhythm is consistently recognized as a market leader. The company has been positioned as a Leader in Gartner's SIEM Magic Quadrant report for five consecutive years, named a 'Champion' in Info-Tech Research Group's 2014-15 SIEM Vendor Landscape report, received SC Labs 'Recommended' 5-Star rating for SIEM and UTM for 2016 and earned Frost & Sullivan's 2015 Global Security Information and Event Management (SIEM) Enabling Technology Leadership Award.

LogRhythm is headquartered in Boulder, Colorado, with operations throughout North and South America, Europe and the Asia Pacific region.

For media enquiries, please contact:
Frances Manabat
Office: +971 (4) 447 2501
E-mail: frances@tcf-me.com

THECONTENT|FACTORY
http://www.tcf-me.com/