CYBERSECURITY

HOW PKI CAN SECURE CRITICAL NATIONAL INFRASTRUCTURE

After previously discussing the US approach to Critical National Infrastructure (CNI) cybersecurity for the energy sector and power grid, here, Lila Kee of Globasign, explains how Public Key Infrastructure (PKI) can secure CNI networks against advanced cybersecurity attacks

Written by Lila Kee, Chief Product Officer, GMO GlobalSign Inc

Recent headlines and mounting evidence suggest that cyberattacks on Critical Infrastructure (CI) systems are increasing as cybercriminals have identified electric utility grids as prime targets for disruption activities. As a result, CI cybersecurity has become a prime concern for governments and citizens alike.

THE USE OF PKI IN SECURING CNI

In recent months, US wholesale energy participants have shown that CI providers can strengthen cybersecurity by implementing standard-based PKI. The US energy sector contains more than 6,413 power plants (including 3,273 traditional electric utilities and 1,728 non-utility power producers) with approximately 1,075 gigawatts of installed generation. Electric power providers, the wholesale energy market, regulators and market participants are embracing PKI as a secure, scalable, flexible and cost-effective method to securely authenticate the digital identities involved in the wholesale electricity market.

Independent systems operators (ISOs), which coordinate, control and monitor electrical power system operations from state to state, are using PKI standards developed by the North American Energy Standards Board (NAESB) to strengthen security for their cyber-based business processes and transactions. PKI is a robust technology that provides a method to securely authenticate digital identities on large and complex networks, such as those that manage business processes for the wholesale electric market. However, due to the many implementation details involved, if the technology is not executed correctly it can also produce a vulnerable system.

NAESB members have produced a standard for the wholesale energy sector that is based on best practices, proven management techniques and advanced digital certificate technologies.

IMPROVED SECURITY FOR ALL

In the wake of increasing attacks, US CIs are stepping up efforts to amplify their cybersecurity and strengthen defenses. In fact, in GlobalSign's previous article it noted that in President Obama's recent Executive Order, the National Institute of Standards and Technology (NIST) was directed to lead the effort to develop a cybersecurity framework that would consist of adopting industry best-practices wherever possible. As part of NIST's draft cybersecurity framework of best practices, guidelines and standards, the NAESB standard on PKI stands a good chance of being applied to other CI sectors.

All CIs are managed, controlled and accessible via internet-connected systems, making them vulnerable to cyberattacks. ISOs in the energy sector have recognised the value of cybersecurity frameworks, have adopted standards developed by NAESB and have demonstrated that standards can be developed using shared expertise from both the public and private sectors – setting a framework for all US CI sectors. With regards to protecting the CNI in the UK and Europe, The European Programme for Critical Infrastructure Protection which is leading the EU initiatives for European stakeholders, could potentially benefit from this recent US development.

NAESB: CYBERSECURITY STANDARDS ADOPTION

Through the adoption of these standards, NAESB and its member organisations believe that cyber defences have been significantly strengthened and the possibility of a successful attack that could impact the operations or well-being of the nation's electric power supply has been greatly reduced. "NAESB has made it a priority to establish PKI standards to fortify our cybersecurity framework," said Rae McQuade, president of NAESB. "In establishing these standards we hope to provide a strong cybersecurity strategy so that we may best protect the business practices related to the electricity market that is a critical part of the everyday lives of our citizens."

As part of the standard PKI development, NAESB has also adopted an accreditation specification that describes the minimum requirements an authorised certification authority (ACA) must follow. NAESB recognises the fluidity of cyber threats and expects the PKI subcommittee to continue to review ACA specification for areas that may require changes in the future. When such areas are identified, NAESB will make the appropriate changes.

While most CIs have recognised that they need improved cyber defences, most have not yet made the tremendous strides forward that the energy sector has made.

GlobalSign®

FURTHER INFORMATION

Tel: 01622 766 766
press@globalsign.com
www.globalsign.co.uk