CYBER SECURITY

SECURING VITAL INFRASTRUCTURE

In this issue GlobalSign looks at how Public Key Infrastructure (PKI) can secure CNI against cyber-attacks and examine a use case for an early adopter of GlobalSign's NAESB-compliant PKI solutions

CNI is a favourite target of cyber criminals because it offers maximum damage with detrimental economic impact and resulting publicity. The potential for cyber-attacks to cause damage to CNI is an ever increasing threat requiring a coherent and effective strategy.

Cyber criminals commonly strike weakest links, devising strategies to attack single users on a mass scale and compromising a subset of systems within targeted organisations. Attackers utilise their knowledge of common IT security weaknesses such as default passwords, common passwords, shared passwords, and the use of shared public password spreadsheets.

Data breaches as the result of these password vulnerabilities strongly suggest single-factor methods of authentication (i.e. user name/passwords) are no longer sufficient security control. Two-factor authentication is essential to protect organisations' sensitive data.

THE USE OF PKI TO SECURE CNI

Many organisations 'strategy' is to simply react to threats and requirements as they present themselves. The organisation becomes a pinball, bouncing between threats and regulations. Organisations need to spend time developing and then implementing a security policy that relies on top level best practices, such as user authentication, network intrusion detection and prevention, business continuity and disaster preparedness, employee education and training, malware detection and prevention, data loss prevention (DLP) and encryption.

Crafting a broad-reaching, best practices based strategy is the first, most critical step to protecting against threats. Implementation of standards-based PKI has become increasingly popular among US wholesale energy participants because it is scalable, flexible and cost-effective.

PKI technology offers organisations the means to control large numbers of Digital Certificates for authentication. However, implementation of PKI still needs to be executed correctly in order to prevent system vulnerabilities. The North American Standards Board (NAESB) are combatting the potential vulnerabilities by producing a set of standards for the Wholesale Energy sector based on best practices and effective management processes. Many organisations wishing to implement PKI could potentially benefit from adopting similar guidelines.

MANAGED PKI

A Managed PKI solution from a third-party, public CA, like GlobalSign, provides access to Digital Certificates through a highly functional, trustworthy, WebTrust-audited, cloud-based environment capable of managing the full lifecycle of Digital Certificates, administrators and certificate profiles. There is no need to purchase, establish, operate and protect an in-house Certificate Authority (CA), resulting in reduced project costs and a faster deployment. Digital Certificates can be deployed efficiently to achieve convenient and secure certificate-based and token-based two-factor authentication for the protection of enterprise networks, data, and applications.

Organisations should partner with a CA that understands enterprise-specific requirements. Automation capabilities such as Active Directory integrations and APIs simplify and automate certificate management, improving efficiency and saving valuable IT time and resources.

CASE STUDY: EARLY ADOPTION OF NAESB-COMPLIANT PKI

Due to the critical nature of ensuring efficient and reliable delivery of electricity, and based on recommendations from the Executive Order to improve CI cybersecurity, ISO New England opted to increase the level of identity authentication for their power generators, regional utility companies, and other market participants that utilise their eMarket portal. With GlobalSign, they found a NAESB-compliant partner who was committed to helping them meet their need for strong authentication in a way that is transparent for their stakeholders, while ensuring highly-trusted, authenticated energy transactions.

Authentication is listed as a key area for improvement in the NIST Preliminary Cybersecurity Framework, the set of standards, guidelines, and best practices that has been drafted to put the recommendations from the Executive Order into action. The Framework specifically mentions the inadequacy of passwords as a means of authentication.

"PKI is a long-established and proven method for securely authenticating digital identities, but there are a variety of implementation details that can mean the difference between a weak and vulnerable identity management system and a highly secure one," states Lila Kee, GlobalSign's chief product officer. "NAESB helped standardise PKI for the energy market to reduce the risk of weak implementations, so we're pleased to help ISO New England lead the adoption of the guidelines to secure their platform. Now, ISO New England is able to strongly authenticate their eMarket users and help meet the Executive Order recommendations for Improving Critical Infrastructure."

GlobalSign is the only public NAESB-authorised Certificate Authority trusted in all popular browsers and operating systems and is a key member and active participant in establishing PKI standards for NAESB. As a member of NAESB's Wholesale Electric Quadrant (WEQ) Board of Directors, Kee played a lead role in the development of the PKI and other cybersecurity standards. ■

FURTHER INFORMATION

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

GlobalSign®