NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Security Guideline for Electricity Sector

Primer for Cloud Solutions and Encrypting BCSI | June 10, 2020

Introduction

This document is intended to provide supplemental information for *Compliance Implementation Guidance: Cloud Solutions and Encrypting BCSI*, guidance for using encryption as a means to protect and restrict access to BCSI in a cloud environment. This primer presents the basic concepts and addresses principles of information encryption during storage, transit, and use.

This document is not intended to establish new requirements under NERC's Reliability Standards, to modify the requirements in any existing Reliability Standards, nor provide an interpretation under Section 7 of the Standard Processes Manual. Additionally, there may be other ways to fulfill the obligations of the Requirements that are not expressed within this document.

The technical information that follows is intended to increase understanding of how encryption can provide additional protection for BES Cyber System Information, when used in conjunction with access controls and other CIP requirements.

Concepts

Cloud Service Provider Services and Examples

In Software as a Service (SaaS), a third-party vendor hosts applications and makes them available to customers over the Internet. Common examples include office productivity software, trouble ticket software, and online meeting tools.

Platform as a Service (PaaS) - A cloud computing model in which a third-party provider delivers hardware and software tools, usually those needed for application development. An example of this type of service would be a vendor-managed platform that hosts 3rd party applications during their development.

Infrastructure as a Service (IaaS) refers to the delivery of computer infrastructure on an outsourced basis to support the customer's operations. When a Cloud Service Provider provides remote hardware, storage, network components or data center space, the product is considered to be IaaS. A common example would be cloud-managed storage system used for backing up business records, off-premises.

Encryption

Encryption is the transformation of information into a form unreadable by anyone without the decryption key. Encryption preserves privacy by obfuscating the information from anyone for whom it is not intended. For example, one may encrypt a folder by passing it through an encryption program. Only those with access to the key will be able to reverse the process and read the original contents. Before encrypted information can be used again, the information must be decrypted to its original, readable state. This is accomplished by using a key and the appropriate encryption algorithm to reverse the process.

The strength of a given encryption process is determined by the complexity of the mathematical algorithm behind it. Like many technologies, encryption is constantly changing. To maintain a sufficient degree of information security, utilities should periodically review and keep pace with cyber industry encryption best practices. One such source for cyber industry encryption best-practice information includes (but is not limited to) the Federal Information Processing Standards (FIPS) 140-2.

Encryption Key Management

Two basic encryption key management models are aids for understanding the security of encrypted information. In the first model, when a Registered Entity has control of the encryption keys, access to BCSI by the cloud service provider is entirely controlled by the Registered Entity. In the second model, the encryption process and/or key management may be mutually managed between the Registered Entity and the cloud service provider.

In the first model, which we'll refer to as entity-managed encryption, the Registered Entity manages the encryption keys in a Hardware Security Module (HSM), on their own premises, via a 3rd party separate from the cloud service provider, or in a service within the cloud solution. An HSM is a special network computer/cluster performing cryptographic operations such as key management and encryption. An HSM cluster resides on the Registered Entity's network (on prem, with a 3rd party, or in the cloud) and is designed to scale and offer high speed encryption of your information. Entity-managed encryption is one way that a cloud service provider would not have access to the keys and therefore could not decrypt or read the information.

From a compliance perspective, entity-managed encryption has a major advantage in simplicity and security. The Registered Entity has complete control of the encryption keys and encrypted information. The cloud service provider cannot decrypt or read the information. Consequently, demonstrating access controls around BCSI protected with entity-managed encryption is not as complex as those required for a mutually-managed encryption management approach.

However, entity-managed encryption has some disadvantages. The cloud service provider may not be capable of providing support to a Registered Entity if encryption keys are lost. The cloud service provider does not have access to decrypt information for the purposes of supporting storage or applications. Key material being transferred from the Responsible Entity or 3rd Party to the cloud could be at risk of corruption while in transit. Additionally, there is significant additional overhead burden on the Registered Entity to maintain the keys, or contract with a third party to do so.

In the second model, which we'll refer to as mutually-managed encryption, the Registered Entity may choose an implementation design in which the Cloud Service Provider has some or all control of the encryption process. This may be referred to as mutually-managed encryption, because the Cloud Service Provider and the Registered Entity would share access and management of the encryption keys and processes. The Cloud Service Provider may have access to some or all of the Registered Entity's information because the Cloud Service Provider has access to the keys.

Mutually-managed encryption generally offers more flexibility and support operationally. When a Cloud Service Provider manages part, or all, of the encryption, there is less overhead for the Registered Entity. Cloud Service Providers can manage security, support applications and infrastructure. Other services a Cloud Service Provider can offer under this model are resetting passwords, decrypting files, managing applications and other general support tasks, because the Cloud Service Provider manages all or part of the encryption process.

The disadvantage to the mutually-managed approach is that the key management may not be entirely controlled by the Responsible Entity, and therefore could enable the cloud service provider to decrypt files (including BCSI) and view them in the original, unencrypted form. This inherently can increase the risk of unauthorized disclosure or access. A Registered Entity would need to incorporate controls around mutually-managed key management and cloud service provider access into their CIP access management program.

Three States of Information

CIP-011 discusses handling and protections for BCSI data in storage, transit, and use. Data at rest is data which is not being actively processed or used, and exists in storage. As the name implies, data in transit is being moved from one system to another. Data in use refers to data that is being used or modified by an end-user.

Email serves as a good example of information at rest, and in transit. For example, BCSI data attached to or embodied in an email sent outside of a corporate network (or even within a corporate network that relies upon a cloud-based email service) is simultaneously in transit (from one user to another) and in storage (in email servers, and in backups for those servers).

Another SaaS example would be a document open for editing or review using an online office productivity application. The document is simultaneously in transit from the Cloud Service Provider to the end-users desktop, in storage and backup in the cloud, and in use by the authorized end-user during editing.

Backup data stored off-premises in the cloud can serve as an example for IaaS. When a Registered Entity encrypts backup data and transmits it to the Cloud Service Provider, the BCSI is encrypted in use (during backup operations) and in transit, as it is sent to the Cloud Service Provider. The BCSI will be encrypted at rest, as the Cloud Service Provider saves the information to disk.

Encrypted Information in transit

Encryption of information in transit does not receive a lot of attention in local networks, because the information never leaves the private company network. However, encryption of information is of primary concern in a cloud environment, because the information will traverse network elements that are not controlled by the Regulated Entity as the information travels between the end user and Cloud Service Provider.

Email services and online office productivity applications are good examples. Email and files destined for the cloud move over the public Internet as they move from the Registered Entity to the Cloud Service Provider. Unencrypted information moving over the public internet poses a higher risk of unauthorized exposure or access. On its journey to a Cloud Service Provider, the information must pass through intermediate service provider networks, none of whom will be party to the Registered Entity’s agreement with the Cloud Service Provider. These intermediate service providers have little or no obligation to a Registered Entity or the Cloud Service Provider to protect the transit of the information.

BCSI information travelling across the public Internet must be encrypted in transit to ensure it is not usable by unauthorized individuals. The majority of Cloud Service Providers, email services, and online office applications use encryption to protect information in transit. Transport Layer Security is most commonly used to secure communications between customers and services like e-mail, online shopping, online banking, and other communications over the Internet. Anytime the prefix, “*https://*” is in front of a web address, Transport Layer Security encryption is being used. Even though Transport Layer Security encryption is commonly used to secure information in transit, encryption should be verified and not assumed.

Encrypted Information at Rest (Storage)

Encryption protects information, including BCSI information, at rest whether in the cloud or other environment. Information will be at rest in SaaS, IaaS, on-premises environments, and when on portable devices (e.g. laptops, thumb drives). When information at rest is stored in an encrypted state, it will be extremely difficult or impossible to access without the encryption keys. If encrypted information is stolen, or inadvertently released, decrypting it to its original state will be extremely difficult.

Encrypted Information in Use

BCSI in the cloud environment may not have a “use” state; it is up to each Registered Entity to define “use” and whether that state exists in their specific implementation. Where a “use” state may exist in a cloud environment, encryption of BCSI while being used may not be practical or even an option. Instead, access controls (such as username and password or two-factor authentication) may be used as a security measure to prevent any BCSI in a “use” state from being accessed by unauthorized personnel.

Cloud Geography

For reliability and resiliency reasons, data in the cloud may be distributed and stored over a wide geographical area. It is not uncommon for cloud data to traverse regional locations or international borders, although agreements limiting storage to certain geographical regions or nations are commonplace. Geographical location in the cloud can be complicated because data may be redistributed or moved to a new location as a cost-saving or reliability measure. In effect, the controlling location of cloud data can change, if the agreements between Cloud Service Provider and Registered Entity do not prohibit it.

A disadvantage to this geographically distributed storage model is that if a breach were to occur, while the data is in a foreign country, the Registered Entity may not have the same legal recourse to enforce the terms of the agreement as they would have in the US.

However, utilizing a distributed model for data storage, where the customer's data is split up across multiple locations, can be an effective security control, especially if encryption is also applied. This would prevent a physical attacker from obtaining access to all of the data, and if also encrypted, prevent their ability to read and use the data. A common example of this methodology is Blockchain. Additionally, as a physical security feature, cloud storage does not require physical labeling of Registered Entity data on a specific server location in a data center, which prevents data center personnel from recognizing data owners.

The shared nature of cloud storage means that the Cloud Service Provider may be responsible for managing some or all of the system. Consequently, the Cloud Service Provider may have access to BCSI stored within the system and in transit during communication with the Registered Entity. If the information is not encrypted during transit and while at rest, security management of a cloud service can require more complex access controls, contract language and non-disclosure agreements.

For specific cloud service and key management examples, see *Compliance Implementation Guidance: Cloud Solutions and Encrypting BCSI*