WECC

Electric Reliability and Security for the West

Encryption in CMEP Activities

Eric Woodruff

March 2019

Introduction

The security of compliance and enforcement data is vitally important. New threats against this data are always emerging and WECC staff is constantly adding capabilities to keep WECC's data secure. Since no single method can address all threats, many layers of defense are used. Segmented networks, threat detection using advanced analytics, personnel background checks, multi-factor authentication, and encryption are just a few of the security layers used protect the data critical to our work.

Encryption is a vital security tool deployed in several ways throughout CMEP activities. The following is an overview of the types of encryption used and the various threats they help to mitigate.

Types of Encryption

Encrypted Web Connections

We understand the concern that entities have for their data once it leaves their networks. The need for security begins the moment a file travels to WECC servers. Encrypted web connections are used to secure this data while it is in transit. This helps to ensure that senders are connected to the correct receiving server and that malicious users cannot intercept the data. Users know they are on an encrypted web connection when they see the HTTPS prefix in the URL to which they are connecting. WebCDMS and WECC's file transfer server both use modern certificates to encrypt data in transit.

Disk and Database Encryption

Encrypting the disks and databases that store sensitive information is also important. An encrypted disk or database will protect against physical attacks to the associated resources and against attempts to extract information without proper credentials. An unauthorized person who obtains a laptop, backup media, or hard drive that is encrypted would be unable to view the contents. Critical resources such as laptops used in compliance processes are protected by full-disk encryption.

File Encryption

File encryption is another layer of encryption in which a file is encrypted with a key that is specific to the users working with the file. This ensures that the file can only be opened by the intended recipients who have access to a unique decryption key. Data protected in this way is secure from an attacker or malware that gains access to a protected network. In addition, an encrypted file that is accidentally sent to the wrong recipient is also unreadable. When compliance files are uploaded to the Audit Data folder

on the EFT server, they are automatically encrypted using public key cryptography. This encrypted file is immediately transferred through a series of firewalls to its final storage location inside a protected network.