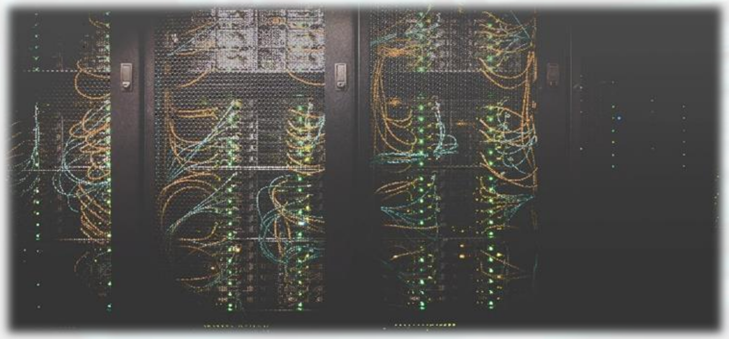
VERMONT ELECTRIC CO OP Vermont Electric Cooperative, Inc.

Cyber Security Practices



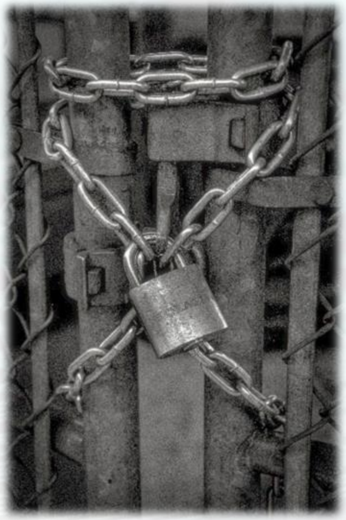
VEC at a glance

Vermont Electric Coop is structured to allow for an Information Technology(IT) network and an Operational Technology(OT) network to work in unison in order to provide the following

- Immediate control of VEC's electrical distribution grid
- Real Time informational status of Distribution/Transmission devices
- Integrated member informational systems
- Outage management systems

Prevention

VEC utilizes many industry recognized cyber security practices



- Defense in depth
- Network Segmentation
- Zero trust networking
- Regular cyber security training
- Cyber Security Steering Committee
- Application of utility specific security control framework
- Secured/managed remote workforce

Recognition

VEC operates with an understanding that prevention of cyber attacks is the best possible scenario, however, more important to that is the recognition of an attack when it happens

- Regular vulnerability scanning
- Multilayer malware detection
- In depth traffic scanning
- Real time logging and alerting to potential threats

Recovery

"It's not a matter of if a business is breached, but when"

- Offsite, offline backups
- Cloud virtual network recovery
- Backup recovery location
- Regular recovery practice

Knowledge

VEC works with industry, state and federal partners in order to share and receive relevant cyber security information. Shared information greatly increases VEC's likelihood to prevent or detect cyber attacks.

Partners

- CISA
- DOE
- National Guard
- Vermont Fusion Center
- E-ISAC
- FBI

Summary

- Prevention
  - Training
  - Secured remote workforce
  - Planning for attacks
  - Segmented networks
- Recognition
  - Regular Scanning
  - In Depth Scanning
  - Logging
- Recovery
  - Practice recovery plans
  - Secure backups

Plan for the worst, Hope for the best.