ESCC

Electricity Subsector
Coordinating Council

Electricity Subsector Coordinating Council
Ransomware Preparedness

Introduction

Ransomware can affect anyone, and has targeted individuals, businesses, local police departments and hospitals, as well as energy companies. Ransomware attacks have increased both in frequency and impact in part because of their effectiveness, and because they can be highly profitable for cyber criminals. Ultimately, preparedness is essential to preventing the temporary or permanent loss of data, disruption to operations, financial consequences, and harm to an organization’s reputation. The impacts of ransomware can be mitigated by developing and following principles of business continuity.

Within the context of this document, the term ***data*** is not limited to information related to customers and employees, but may also include information related to operational configuration, such as managing Supervisory Control and Data Acquisition (SCADA) equipment, networks, routers, firewalls, etc.

The following preparedness measures were compiled in support of the Electricity Subsector Coordinating Council (ESCC), and are recommended to utilities to reduce the likelihood of ransomware infection, or to minimize operational impact and facilitate rapid recovery in the event of infection.

These recommended preparedness measures are consistent with the NIST Cybersecurity Framework Core, which is separated into five concurrent and continuous functions: namely **Identify, Protect, Detect, Respond, and Recover.**

These recommended preparedness measures are compiled with the intent of helping utilities to implement more effective ransomware preparedness measures but are not intended to be requirements or mandated to be followed in the context of a specific ransomware event. The recommended preparedness measures are flexible and may be satisfied in any number of ways as may be appropriate in a specific event.

IDENTIFY

1. Perform an impact assessment (IA) to inform a business continuity plan and identify operation-critical components and single points of failure. Establishing specific criteria to determine the organizational value of data and systems before an incident occurs will help an organization better respond to a ransom request, should an attack occur.
2. Consider the operational impact as well as the business implications of losing specific types of data or systems for varying lengths of time. In the event of a ransomware attack, the encrypted data may be inaccessible for several hours, days, or weeks.
3. Ensure that systems and data that are determined business critical have restoration backups to prevent single points of failure, where possible.

Date Published: 6/20/2017

PROTECT

1. Protect and monitor critical administrative credentials, particularly if they could provide access to data or backups that would be a target of ransomware. Apply the principle of least privilege to limit administrative access to systems, including workstations.
2. Consider the implementation of technology such as two-factor authentication and application whitelisting, particularly for critical systems, which may prevent the infection and spread of ransomware.
3. Review existing technology and procedures regarding advanced email protections to screen, filter, and prevent delivery of malicious attachments (including the blocking or quarantine of executables and macros), embedded URLs, and spoofed emails.
4. Segment and monitor backup facilities to protect from unauthorized access. Backup data can be segregated in the cloud or by physically storing backups offline. However, some backup solutions may be vulnerable to ransomware because they continuously back up in real-time (persistent synchronization).
5. Periodically test backup restoration processes to verify the integrity of backups, and exercise recovery actions to determine recovery time.
6. Perform regular security awareness training and educate employees on ransomware risk and impact. Phishing emails are the most common method of ransomware infection.
7. Educate key decision-makers, including senior executives and legal counsel on the threat and mitigation actions available to the organization. Develop thresholds for mitigation and response escalation, up to and including potentially paying ransom.
8. Conduct a review of the organization’s existing cybersecurity insurance policies and consider purchasing coverage.
9. Include ransomware in Incident Response (IR) scenarios and test IR plans periodically.
10. Develop a vulnerability management program (including a patch management process) that, at a minimum, addresses critical vulnerabilities, particularly for internet facing components.
11. Review existing policy regarding the connection of personal devices to the organization’s computer systems. For particularly critical systems, consider physically or virtually blocking USB ports to prevent injection of malware and exfiltration of data.

DETECT

1. Deploy and maintain anti-virus software to help detect ransomware.
2. Consider using an endpoint protection tool that identifies abnormal behavior or zero-day issues.
3. Review existing monitoring processes and procedures as well as technology solutions regarding the ability to detect the presence of ransomware.
4. Review network monitoring solutions in place to determine if they have the capability to detect new or unauthorized portable data devices (USB, drives, etc.) on the system.

RESPOND

1. Implement the organization’s security incident response and business continuity plan.
2. Isolate systems that are verified to be infected by ransomware immediately. Remove infected systems from the network to prevent ransomware from attacking network or shared drives.
3. Contact and engage with stakeholders consistent with the organization’s IR and business continuity plans. Such stakeholders may include local and/or regional law enforcement and the appropriate Information Sharing and Analysis Center (ISAC).
4. Consider requesting support from relevant industry groups, such as the ESCC Cyber Mutual Assistance Program, as part of the overall response.
5. Perform the necessary forensic analysis and process review to determine how and to what extent the ransomware has infected the organization’s systems.

RECOVER

1. Employ a backup and recovery plan for all critical data. Prioritize the recovery plan based on the relative importance of the data to be recovered.
    - Ensure that all ransomware is removed from the organization’s systems before attempting data restoration.
    - Following the analysis of the ransomware infection vector, implement changes to mitigate the risk of that vector being used against the organization in the future.
2. Determine internally, or through an external party, whether sensitive and/or proprietary data affected by the ransomware attack has been made available on the internet.
3. Fully understand applicable state-level data breach laws and regulations to ensure organizational compliance.
4. Perform a post-incident review, document lessons learned, and update related policies and incident response procedures as appropriate.

BEFORE MAKING A RANSOMWARE PAYMENT

1. Determine the technical feasibility, timeliness, and cost of restarting systems from backup versus payment of the ransom.
2. Engage with law enforcement and/or other subject matter experts to determine if there are known decryption keys or procedures that would eliminate the need to pay ransom.
3. Work with legal, public affairs, and other departments to assess the consequences of paying ransom.
4. Consider that paying the ransom does not guarantee that the affected data will be decrypted and restored:
    - Some victims have not been provided with decryption keys after paying the ransom.
    - Some victims who paid the ransom have been targeted again by cyber actors.
    - After paying the originally demanded ransom, some victims were asked to pay an additional amount to receive the decryption key.
    - Irrespective of ransom payment, sensitive and/or proprietary data affected by the ransomware attack may be disclosed in various forms on the internet.
    - Paying the ransom may encourage this criminal business model.

This document was compiled by the ESCC in collaboration with the American Gas Association, the DNG-ISAC, and the E-ISAC.

References:

Alert (TA16-091A) - Ransomware and Recent Variants – US-CERT

- https://www.us-cert.gov/ncas/alerts/TA16-091A

Incidents of Ransomware on the Rise – FBI

- https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise
  See Tips for Dealing with the Ransomware Threat

Ransomware Prevention and Response for CISOs – Multi-Agency Government Report

- https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

ESCC Cyber Mutual Assistance Program

- www.electricitysubsector.org/CMA

Contact Information:

Reporting

Federal Bureau of Investigation

Cyber Task Forces | www.fbi.gov/contact-us/field

Internet Crime Complaint Center | www.ic3.gov

United States Secret Service

Electronic Crimes Task Force | www.secretservice.gov/investigation/#field

Local Field Offices | www.secretservice.gov/contact/

Information Sharing and Analysis Centers (ISACs)

Downstream Natural Gas ISAC | https://www.dngisac.com/

Electricity ISAC | https://www.eisac.com/

Mitigation

United States Computer Emergency Readiness Team (US-CERT) | www.us-cert.gov

NIST Cybersecurity Framework | https://www.nist.gov/cyberframework

Top 10 Information Assurance Mitigation Strategies | https://www.iad.gov/iad/library/ia-guidance/iads-top-10-information-assurance-mitigation-strategies.cfm