2024

Colonial Pipeline Incident

SAMPLE INCIDENT RESPONSE (IR) PLAN

ROBERT C. RHODES

DEREZZED INC. D/B/A THREATGEN | 118 Vintage Park Blvd. Suite 700 W, Houston, Texas 77070

Colonial Pipeline Ransomware Incident

Sample Incident Response Plan

****NOTE ** This sample Incident Response Plan is based on the information provided in the corresponding scenario and case study provided by ThreatGEN. This incident response plan for Colonial Pipeline uses their real-world personnel and incorporates elements of their actual response to the 2021 ransomware attack.**

This was generated by Perplexity using versions of the scenario and case study.

1. Incident Response Team

- **Team Lead**: Zion McClure (Incident Response Team Lead)

- **Cybersecurity Lead**: Tron (Cybersecurity Analyst Lead)

- **Executive Oversight**:

  - Melanie Little (President and CEO)

  - Clay Miller (VP and CFO)

  - Adam Tice (CISO)

  - Darrell Riekena (CIO and SVP)

- **Operations**: Angie Kolar (VP Operations Services & Chief Risk Officer)

- **IT**: Marie Mouchet (VP & CIO)

- **Commercial**: Daniel Gordon (VP/Chief Commercial Officer)

- **Legal**: General Counsel (name not provided)

- **Communications**: Corporate Communications Manager (name not provided)

2. Incident Detection and Initial Response

1. **Monitoring and Detection**:

   - Continuous monitoring of network traffic, SCADA systems, and security logs.

   - Immediate escalation of any suspicious activities to the Cybersecurity Lead.

2. **Initial Assessment**:

   - Cybersecurity Lead (Tron) to perform rapid assessment of the situation.

   - Determine the scope and potential impact of the incident.

3. **Activation of Incident Response Team**:

   - Incident Response Team Lead (Zion McClure) to activate the full team if a significant threat is confirmed.

   - Notify all team members via secure communication channels.

3. Containment and Mitigation

1. **Immediate Actions**:

   - Isolate affected systems to prevent further spread.

   - Disable compromised VPN accounts and other potential entry points.

   - Implement network segmentation to protect critical OT systems.

2. **Operational Decision-Making**:

   - Angie Kolar to assess the need for operational shutdowns or adjustments.

   - If necessary, initiate emergency shutdown procedures for affected pipeline sections.

3. **System Recovery**:

   - IT team led by Marie Mouchet to begin restoration of critical systems from clean backups.

   - Prioritize SCADA and control room systems for restoration.

4. Investigation and Analysis

1. **Forensic Analysis**:

   - Engage external cybersecurity experts (e.g., Mandiant) to assist with investigation.

  - Collect and preserve system logs and other evidence for analysis.

2. **Threat Intelligence**:

  - Cybersecurity team to analyze indicators of compromise and identify potential threat actors.

  - Collaborate with law enforcement and intelligence agencies for broader threat context.

5. Communication and Reporting

1. **Internal Communication**:

  - Regular briefings to executive leadership by Adam Tice (CISO) and Darrell Riekena (CIO).

  - Updates to employees on the situation and any necessary precautions.

2. **External Communication**:

  - Corporate Communications Manager to prepare statements for media and stakeholders.

  - Daniel Gordon to manage communication with commercial partners and customers.

3. **Regulatory Reporting**:

  - Legal team to ensure compliance with reporting requirements (e.g., SEC 8-K filings).

  - Notify relevant authorities (DHS, FBI, CISA) as required by regulations.

6. Recovery and Restoration

1. **System Restoration**:

  - Gradually restore systems, starting with critical infrastructure.

  - Implement enhanced security measures, including multi-factor authentication for all access points.

2. **Operational Resumption**:

  - Angie Kolar to oversee the safe resumption of pipeline operations.

  - Conduct thorough testing to ensure system integrity before full restoration.

7. Post-Incident Activities

1. **Lessons Learned**:

  - Conduct a comprehensive review of the incident response.

  - Identify areas for improvement in security measures and response procedures.

2. **Update Security Posture**:

  - Implement recommendations from the post-incident analysis.

  - Enhance employee training and awareness programs.

3. **Stakeholder Management**:

  - Provide updates to board members, shareholders, and regulatory bodies.

  - Manage ongoing communication with affected customers and partners.

8. Ongoing Preparedness

1. **Regular Exercises**:

  - Conduct tabletop exercises to test and improve the incident response plan.

  - Involve all relevant departments in scenario-based training.

2. **Continuous Improvement**:

  - Regularly update the incident response plan based on new threats and lessons learned.

  - Maintain relationships with external cybersecurity experts and law enforcement agencies.