# Report:

# TechCorp Ransomware Incident Response

Francisco José Morante Lozada
4Geeks Student

## About This Report:

- This document demonstrates security testing performed in a controlled lab environment using intentionally vulnerable machines.
- All testing conducted on dedicated lab systems
- No real systems or data were compromised
- Primary goal: Show all found vulnerabilities.
- These exercises help understand attacker methodologies to build better defenses.
- The test was performed on 28th January, 2026.

## Index

# 1st Identification

### Critical Assets Affected:

1. **File Server:** Contains essential operational documents and project data.
2. **Customer Database:** Holds sensitive personal, financial, and contractual information.
3. **Backup Systems:** Located on the same network, resulting in encrypted backups.

### Vulnerabilities Identified:

1. Lack of network segmentation between production and backup systems.
2. Insufficient email filtering and phishing awareness training.
3. Poor access controls and excessive user permissions (End users shouldn't have admin rights).

# 2nd Protection

### Preventive Measures TechCo Should Have Implemented:

1. **Network Segmentation:** Isolate critical systems (file servers, databases, backups) into separate VLANs.
2. **Email Security:** Deploy advanced phishing filters and attachment sandboxing (e.g., DMARC, SPF, DKIM).
3. **Regular Backups:** Follow the 3-2-1 rule (3 copies, 2 media types, 1 off-site/offline).
4. **Access Controls:** Implement least-privilege access and require MFA or passkey for administrative accounts.
5. **Endpoint Protection:** Use an antivirus and application whitelisting.
6. **User Training:** Conduct mandatory phishing simulation exercises and security awareness training quarterly.

# 3rd Detection

## Monitoring Solutions:

**SIEM** (Security Information and Event Management): Correlate logs from endpoints, servers, and network devices (Wazuh, Security Onion, etc).

**EDR** (Endpoint Detection and Response): Monitor for unusual file encryption activity and process behavior (Microsoft Defender for Endpoint, CrowdStrike).

**Network Traffic Analysis:** Use tools like Zeek or Wireshark, to detect lateral movement and C2 communications. There are also tools specialized on Cloud services (Microsoft Defender for Identity or Amazon VPC Traffic Mirroring)

## Alert Protocol:

Establish a 24/7 Security Operations Center (SOC) or a monitored alerting system.

Define thresholds for suspicious activity (e.g., rapid file changes, unusual RDP connections). (Remote Desktop Protocol)

Implement automated alerts to the incident response team via SMS, email, and dashboard notifications.

# 4th Response

## Incident Response Plan Steps:

### Phase 1: Immediate Actions

**Isolation:** Disconnect affected systems from the network to prevent further spread.

**Activate IR Team:** Notify the Incident Response Team (IRT) and declare a security incident.

**Preserve Evidence:** Capture memory dumps, log files, and a sample encrypted file without altering data.

**Legal & Compliance:** Notify legal counsel and determine regulatory reporting obligations (e.g., GDPR)

**Do not pay the ransom, it will only lead to a major incident.**

### Phase 2: Containment & Eradication

**Identify Attack Vector:** Determine the initial entry point (phishing email) and IOCs (Indicators of Compromise).

**Remove Malware:** Use EDR tools to quarantine and remove ransomware artifacts (Endpoint Detection and Response).

**Patch Vulnerabilities:** Close the exploited entry points and reset compromised credentials.

### Phase 3: Communication

**Internal:**

- Regular updates to the staff to stop spreading misinformation.

**External:**

- Customers: Transparent notification about the incident, impact, and steps taken (via email/status page).
- Authorities: Report to law enforcement and relevant cybersecurity agencies.
- Media: Designate a single spokesperson; prepare a holding statement if needed.

### IRT Roles & Responsibilities:

**Incident Commander:** Overall coordination and decision-making.

**IT/Security Lead:** Technical containment and forensics.

**Legal/Compliance Officer:** Regulatory and legal guidance.

**Communications Lead:** Internal and external messaging.

**HR Lead:** Support affected employees and manage insider threat checks.

# 5th Recovery

## System & Data Restoration Steps:

**Restore from Clean Backups:** Use offline/immutable backups to rebuild affected systems.

**Validate Integrity:** Ensure restored data is uninfected and complete before bringing systems online.

**Gradual Re-integration:** Bring systems back online in stages, starting with non-critical services.

**Monitor for Re-infection:** Continuously monitor for signs of ransomware resurgence.

### Business Continuity During Recovery:

Activate DR (Disaster Recovery) site for critical operations.

Implement manual workarounds for essential processes if needed.

Provide regular recovery status updates to all stakeholders.

# 6th Continuous Improvement

### Post-Incident Evaluation Method:

Conduct a formal lessons-learned session within 2 weeks of resolution.

Use the NIST CSF to assess performance in each function (Identify–Protect–Detect–Respond–Recover).

Perform a tabletop exercise every 6 months to validate the updated plan.

Key Improvements to Integrate:

Implement immutable/air-gapped backups.

Introduce network segmentation and micro-segmentation policies.

Enhance user training with more frequent phishing simulations.

Develop a ransomware-specific playbook within the IR plan.

Establish a cybersecurity insurance policy that covers ransomware incidents.

# 7th Consulted Sources

## 1. NIST Cybersecurity Framework (CSF)

**NIST CSF v1.1**
The core framework used to structure the report—Identify, Protect, Detect, Respond, Recover. Provides a risk-based approach to managing cybersecurity.

## 2. NIST Incident Handling Guide

**NIST SP 800-61 Rev. 2**
Defines the incident response lifecycle (Preparation, Detection, Analysis, Containment, Eradication, Recovery, Post-Incident). Used for response phase steps and IRT roles.

## 3. NIST Security Controls

**NIST SP 800-53 Rev. 5**
Catalog of security and privacy controls for information systems. Informed protection measures (encryption, access control, backups, etc.).

## 4. NIST Risk Assessment Guide

**NIST SP 800-30 Rev. 1**
Methodology for conducting risk assessments. Used for asset identification, threat evaluation, and risk prioritization.

## 5. CISA Ransomware Guide

**CISA Ransomware Guide**
Summary: Practical ransomware prevention, detection, and response steps from the U.S. Cybersecurity and Infrastructure Security Agency. Referenced for recovery and reporting steps.

## 6. NIST Ransomware Profile

**Source: NIST IR 8374**
A ransomware-specific profile of the NIST CSF. Used to align ransomware controls with the five core functions.

## 7. Email Authentication Protocols and Other Tools

**SPF:** Authorizes sending servers.
**DKIM:** Digitally signs emails.
**DMARC:** Policies for email validation and reporting.
Standards to prevent email spoofing and phishing, critical in the TechCo phishing attack vector.

**Network Traffic Analysis (NTA) Tools**
Wireshark, Zeek, Suricata, Darktrace, Cisco Stealthwatch.

**SIEM Platforms**
Splunk, IBM QRadar, Microsoft Sentinel, LogRhythm, Elastic Security.
Security Information and Event Management systems that aggregate, correlate, and analyze logs from multiple sources for threat detection and compliance.

**EDR Platforms**
CrowdStrike Falcon, Microsoft Defender for Endpoint, SentinelOne, Cortex XDR.
Endpoint Detection and Response solutions that monitor endpoints for malicious activity, provide forensic data, and enable automated response.

**FBI IC3 Ransomware Guidance**
FBI IC3 Ransomware
Guidance on reporting ransomware incidents to law enforcement and avoiding ransom payments.

**Cloud & Hybrid Security**
AWS VPC Mirroring, Google Packet Mirroring, Microsoft Azure Sentinel documentation.
Cloud-native tools for extending visibility and protection into hybrid environments.

## 8.Industry Best Practices

3-2-1 Backup Rule: 3 copies, 2 media types, 1 off-site/offline.

Least Privilege & Network Segmentation: Foundational security principles from CIS Controls and ISO 27001.

SANS Institute Incident Response Model: Influenced IRT structure and response workflows.