Rick Abraham

My Company  Dallas, TX

Risk Assessment – Malware Risks

Contents

[Introduction 2](#_Toc182579146)

[Risk Identification 2](#_Toc182579147)

[Risk Analysis 3](#_Toc182579148)

[Mitigation Recommendations 3](#_Toc182579149)

[Employee Endpoints 3](#_Toc182579150)

[File Servers 4](#_Toc182579151)

[Email Systems 4](#_Toc182579152)

[Backup Systems 4](#_Toc182579153)

[Network Infrastructure 4](#_Toc182579154)

[Monitoring and Review 5](#_Toc182579155)

[Frequency 5](#_Toc182579156)

[Daily 5](#_Toc182579157)

[Monthly 5](#_Toc182579158)

[Quarterly 5](#_Toc182579159)

[Bi-Annually 5](#_Toc182579160)

[Annually 6](#_Toc182579161)

[Incident Response 6](#_Toc182579162)

[Documentation and Compliance 6](#_Toc182579163)

Risk Assessment – Malware Risks

# Introduction

Purpose: This risk assessment identifies and evaluates potential malware-related threats to the organization’s IT infrastructure and data. It outlines vulnerabilities, assesses their impact, and recommends mitigation strategies to protect systems from malware infections, minimize downtime, and safeguard data integrity.

Scope: Includes endpoints (e.g., laptops, desktops, mobile devices), servers, email systems, network infrastructure, and any software prone to malware attacks.

# Risk Identification

| **Asset** | **Threat** | **Vulnerability** | **Impact** | **Risk Rating** |
| --- | --- | --- | --- | --- |
| Employee Endpoints | Infection via phishing emails or malicious downloads | Lack of user awareness and weak antivirus solutions | Data corruption, system downtime, spread of malware | High |
| File Servers | Malware propagation through infected files | Overly permissive file-sharing policies and lack of scanning tools | Data loss, operational disruption | High |
| Email Systems | Distribution of malware via phishing or malicious attachments | Lack of email filtering and attachment scanning | Credential theft, compromised systems | High |
| Backup Systems | Ransomware encrypting or deleting backup files | Lack of encryption, offsite storage, and immutability | Permanent data loss, inability to recover systems | High |
| Network Infrastructure | Malware spread across devices and servers | Lack of segmentation, outdated IDS/IPS systems | Network-wide disruption, unauthorized access | Medium |

# Risk Analysis

| **Asset** | **Likelihood** | **Impact Severity** | **Overall Risk Level** |
| --- | --- | --- | --- |
| Employee Endpoints | High | High | Critical |
| File Servers | High | High | Critical |
| Email Systems | High | High | Critical |
| Backup Systems | Medium | High | High |
| Network Infrastructure | Medium | Medium | Moderate |

# Mitigation Recommendations

## Employee Endpoints

* Deploy **Endpoint Detection and Response (EDR)** solutions to identify and block malware in real time.
* Regularly update and patch operating systems and installed applications.
* Provide **ongoing employee training** to recognize phishing emails and avoid malicious downloads.
* Enable **application whitelisting** to restrict installations to approved software only.

## File Servers

* Integrate **anti-malware scanning tools** with file servers to detect and remove malicious files.
* Restrict file-sharing permissions to limit access to critical data directories.
* Perform **routine vulnerability scans** to identify potential weaknesses in server configurations.

## Email Systems

* Implement **advanced email filtering** and attachment scanning to block phishing attempts and malicious links.
* Enforce **DMARC, SPF, and DKIM protocols** to prevent email spoofing.
* Use a **sandboxing solution** to analyze suspicious email attachments before delivery.

## Backup Systems

* Maintain **offline, encrypted, and immutable backups** to ensure recovery in the event of a ransomware attack.
* Regularly test backup integrity and ensure backups are stored in a physically secure offsite location.
* Use **air-gapped backups** to prevent malware from spreading to stored copies.

## Network Infrastructure

* Implement **network segmentation** to isolate critical systems and prevent lateral movement of malware.
* Update intrusion detection/prevention systems (**IDS/IPS**) to monitor and block malware traffic.
* Configure firewalls to block connections to known malicious IP addresses and domains.

# Monitoring and Review

## Frequency

### Daily

* Monitor **antivirus and Endpoint Detection and Response (EDR)** logs for detected malware, blocked attempts, and quarantined files.
* Review alerts from email filtering systems for malware-laden attachments or links.
* Ensure all **signature databases** (e.g., antivirus, IDS/IPS) are updated with the latest threat intelligence.

### Monthly

* Audit malware detection systems, ensuring full coverage across endpoints, servers, and email platforms.
* Review logs for recurring malware threats or patterns, such as repeated phishing attempts or targeted attacks.
* Test system recovery processes using backup data to ensure integrity and malware-free restoration.

### Quarterly

* Perform **vulnerability scans** on critical systems to identify unpatched software that may be targeted by malware.
* Assess the performance of malware detection tools (e.g., EDR, email filters) against current threat intelligence.
* Review and refine malware containment protocols, such as isolation measures for infected devices.

### Bi-Annually

* Conduct **penetration tests** simulating malware attacks to evaluate system defenses and incident response effectiveness.
* Run **tabletop exercises** for malware-specific incidents, such as ransomware outbreaks, to identify gaps in response plans.
* Evaluate backup and disaster recovery processes to confirm they meet recovery time objectives (RTOs) and are resistant to malware infections.

### Annually

* Reassess malware risks based on changes in the threat landscape, organizational infrastructure, and new attack vectors.
* Update malware response playbooks and procedures to incorporate lessons learned from incidents and simulations.
* Conduct organization-wide **malware awareness training** for employees, focusing on real-world scenarios such as ransomware or Trojan infections.

## Incident Response

* Maintain a dedicated **Malware Incident Response Team (MIRT)** to investigate and resolve malware incidents efficiently.
* Conduct **bi-annual incident response drills** focusing on malware scenarios, such as ransomware or worm infections, to test readiness.
* Document all malware incidents, including the source, type, impact, and resolution, to improve detection and prevention strategies.

## Documentation and Compliance

* Maintain logs of malware detection events, including origin, type, and remediation steps taken.
* Document updates to antivirus, EDR, email filtering, and other malware detection tools.
* Ensure compliance with applicable regulations and standards, including:
  + **NIST SP 800-53**: SI-3 (Malware Protection), SI-4 (Monitoring), and CP-10 (System Recovery).
  + GDPR, CCPA, and ISO 27001 for data protection and incident reporting.