Patch Management Policy

1.0 Overview

Marketware, Inc. is responsible for ensuring the confidentiality, integrity, & availability its data & that of customer data stored on its systems. Marketware, Inc. has an obligation to provide appropriate protection against malware threats, such as viruses, Trojans, & worms which could adversely affect the security of the system or its data entrusted on the system. Effective implementation of this policy will limit the exposure & effect of common malware threats to the systems within this scope.

2.0 Purpose

This document describes the Global Security Office's (GSO) requirements for maintaining up-to-date operating system security patches on all Marketware, Inc. owned & managed workstations & servers.

3.0 Scope

This policy applies to workstations or servers owned or managed by Marketware, Inc. This includes systems that contain company or customer data owned or managed by Marketware, Inc. regardless of location. The following systems have been categorized according to management:

- Microsoft Windows servers managed by Engineering Team
- Workstations (desktops & laptops) managed by the Security Team

4.0 Policy

Workstations & servers owned &/or by Marketware, Inc. must have up-to-date (as defined by GSO's minimum baseline standards) operating system security patches installed to protect the asset from known vulnerabilities. This includes laptops, desktops, & servers owned & managed by Marketware, Inc.

4.1 Workstations

Desktops & laptops must have automatic updates enabled for operating system patches. This is the default configuration for all workstations built by Marketware, Inc. Any exception to the policy must be documented & forwarded to the GSO for review. See Section 8.0 on Exceptions.

4.2 Servers

Servers must comply with minimum baseline requirements, approved by the GSO. Minimum baseline requirements define the default operating system level, service pack, hotfix, & patch level required to ensure security of Marketware, Inc. asset & data that resides on the system. Any exception to policy must be documented & forwarded to GSO for review. See Section 8.0 on Exceptions.

5.0 Roles & Responsibilities

- Engineering will manage patching needs for Microsoft Windows servers on the network & on AWS.

- Workstation Imaging will manage the patching needs of all workstations on the network.
- Information Security is responsible for routinely assessing compliance with the patching policy & will provide guidance to all groups in issues of security & patch management.
- The Change Management Board is responsible for approving the monthly & emergency patch management deployment requests.

6.0 Monitoring & Reporting

Active patching teams noted in the Roles & Responsibility section (5.0) are required to compile & maintain reporting metrics that summarize the outcome of each patching cycle. These reports shall be used to evaluate the current patching levels of all systems & to assess the current level of risk. These reports shall be made available to Information Security & Internal Audit upon request.

7.0 Enforcement

Implementation & enforcement of this policy is ultimately the responsibility of all employees at Marketware, Inc. Information Security & Internal Audit may conduct random assessments to ensure compliance with policy without notice. Any system found in violation of this policy shall require immediate corrective action. Violations shall be noted in the Marketware, Inc. issue tracking system & support teams shall be dispatched to remediate the issue. Repeated failures to follow policy may lead to disciplinary action.

8.0 Exceptions

Exceptions to patch management policy require documented approval from the GSO. Any servers or workstations that don't comply with policy must have an approved exception on file with the GSO. Please refer to the GSO or local Information Security representative for details on filing exceptions.

7.0 Definitions

Term	Definition
Patch	A piece of software designed to fix problems with or update a computer program or its supporting data.
Trojan	A class of computer threats (malware) that appears to perform a desirable function but in fact performs undisclosed malicious functions.
Virus	A computer program that can copy itself & infect a computer without the permission or knowledge of the owner.
Worm	A self-replicating computer program that uses a network to send copies of itself to other nodes. May cause harm by consuming bandwidth.

9.0 Revision History

1.0 initial policy version, 6/13/2016