Ministry of Communications & Information Technology

Malicious Code Standard

Table of Contents

Introduction

1.1 Background

Malicious code, also known as 'malicious software' or 'malware' is a common threat affecting IT systems. Malicious code refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's information, applications, or operating system.

Securing the Government of Samoa (GoS) systems and network from malicious software is of crucial importance to ensure that the government network remains active and continues to operate as intended. It is also imperative that the information held on the network pertaining government activities and information regarding the citizens of the GoS remains secure from malicious actors.

1.2 Purpose and Scope

This standard details the requirements for establishing and maintaining controls to prevent and detect the presence and spread of malicious code in the GoS IT environment.

This standard applies to all GoS systems – including existing infrastructure and those managed by external suppliers or provided via cloud services.

This Standard is one of a suite of policy documents for the betterment of the GoS's security infrastructure. It contains standard requirements and expectations for the purpose of securing the network from malicious code, such as the installation of anti-malware software that works in conjunction with endpoint protection tools.

Unless an exemption has been sought and approved, this standard applies to all GoS systems. A justification for the exemption request must be provided to the MCIT for a risk-based assessment, and subsequently approved by the CEO. It must then be recorded in the Government risk register.

1.3 Requirements

1.3.1 Anti-Malware Software

The following statements outline the key requirements for Anti-Malware software deployed within the GoS IT environment.

All Government Systems must have Anti-Malware software installed.

- All IT systems connected to the Government of Samoa's network must have anti-malware software installed and enabled.

- Only approved malicious code detection solutions reviewed and implemented by the MCIT and its related divisions are to be installed.

All anti-malware software implemented by GoS is to meet specific configuration requirements. Anti-malware software must be configured to meet the following requirements:

- The software cannot be uninstalled or re-configured without administrative credentials;
- The software must quarantine or remove any detected malware;
- The software must automatically update definitions files daily;
- Scans of inserted removable media and downloaded files must be performed automatically;
- Systems scans must be performed at least once daily, which includes the master boot record, memory, system files and program files; and
- Alerts must be generated for detected infections, which are sent to an administration console and logged.

1.3.2 File Integrity Management

A File Integrity Management (FIM) solution must be used to detect any unauthorised changes and potential corruption of any sensitive data.

Sensitive information should be based off the classification schema determined by the Ministry of Communication, Information and Technology Information Classification and Handling Standard and as defined by the MCIT. Parties to be connected to the FIM will be determined by the MCIT.

The solution must be configured to specifically detect changes on at least the following:

- Files containing credentials, privilege settings and security settings;
- Sensitive content (e.g. any files containing Personally Identifiable Information);
- System Files (e.g. System 32, Program Files, DLLs, Drivers);
- Audit Log Files; and
- File deletion and copies.

1.3.3 Host Based Intrusion Detection and Prevention (HIDS / HIPS)

A host-based Intrusion Detection Solution (HIDS) must be used on critical systems.

A host-based Intrusion Detection solution must be used on critical systems to detect any unauthorised connection attempts and identify and log any suspicious traffic patterns.

- The Critical systems (e.g. those that provide key government functions, hold sensitive data, healthcare systems and where possible key gateways) that require HIDS will determined by the MCIT; and
- System owners looking to change or alter these systems must inform the MCIT of the proposed change, and seek an exemption as per the process required by this Standard.

Where feasible, Host based intrusion Prevention should be applied.

Where possible to apply, a host-based Intrusion prevention solution (HIPS) should be used on critical systems to prevent any unauthorised connection attempts and log any unusual attempts to enter the network.

1.3.4 Content Filtering

GoS's systems must use a content filtering mechanism to detect malicious content from external sources (e.g. websites or email).

The GoS's systems must use a content filtering mechanism to detect and prevent malicious content from emails, websites or downloaded executables. Malicious code found in any content means that content must either be blocked or quarantined.

- The MCIT will identify and maintain a content filtering solution; and
- Signatures for content filters must be updated automatically daily.

A blacklist will be used to assist content filtering efforts / solutions.

The MCIT will define a government wide content filtering blacklist for all ministries and government organisations.

- An exemptions process through the MCIT must be obtained in order for a ministry not to adhere to requirements of the government wide blacklist.

1.3.5 Application Whitelisting

Application whitelisting will be implemented and standardised across GoS systems.

An application whitelist must be created and implemented based on GoS's Standard Operating Environment (SOE) and the approved applications. Implementation requirements include that:

- SOE's must be documented;
- Whitelists, including hashes for integrity checking, must be updated as part of the patching process for whitelisted applications;
- Whitelisted applications must be tested prior to deployment to ensure they function as expected; and
- Integrity checks must be conducted by the ICT teams of each Ministry (with recommendations available from the MCIT) to validate that whitelisted applications have not been modified.

Glossary

Application whitelisting	An application whitelisting is implemented by administrators to prevent unauthorised applications from running on a network.
FIM	File Integrity Management.
SOE	Standard Operating Environment is the build and deployment of a standardised operational environment.
Content Filtering	Content filtering is a process that manages or screens access to specific emails or webpages. The goal is to block content that contains harmful information.
Host Based Intrusion	Software, resident on a system, which monitors system activities for malicious or unwanted behaviour.
Host Based Prevention	Software, resident on a system, which monitors system activities for malicious or unwanted behaviour and can react in real-time to block or prevent those activities.
Anti-Malware Software	Software that protects the computer from malware. It scans the system for all types of malicious software that manage to reach the computer.

Version Management

Version	Date	Comments and Remarks
1.0		