STANDARD OPERATING PROCEDURE
Do not Photocopy

Document Information Classification: Unrestricted

Title:	Protecting the TRE from Malware
Effective Date:	02 May 2019
Reference Number:	SOP-03-11
Version Number:	1.8
Owner:	Information Security Manager,
Review Date:	02 May 2021

Table of Contents

1. Purpose

Detection, prevention and recovery controls to protect against malware should be implemented.

This document sets out the policy for the protection of the TRE environment and for the continued provision of TRE services that we provide to our Collaborators, and other TRE users, against the threat of malware. It provides guidance and direction on minimising the risk of a malware infection(s) and what to do if one is encountered.

2. Scope

This document applies to TRE resources, and to all users that have access to TRE assets and accounts.

3. Responsibilities

TRE users are responsible for:

- Ensuring that their assets are appropriately updated and protected from malware.

4. Procedure

4.1. What is malware?

Malware is short for 'malicious software'.
Malware infections on your computer or other data storage devices can have a serious impact depending on what the malware was designed to do. For example, it can:

- corrupt or make important data inaccessible;
- introduce hidden software which can detect usernames and passwords to University systems, or personal data such as bank and credit card details, and transmit them to criminals to use in fraudulent activities.

4.2. Anti-Virus Protection (AV)

All ‘end points’ and network ‘entry’ points should be protected from malware and its effects, and should provide protection to the resources they host or provide access to. Where practicable, an AV solution will be deployed on all TRE assets and will mediate all traffic that may be processed on that end point.

In the case of ‘boundaries’, the point of access to the environment outside of the TRE is to provide protection from malware to any traffic it allows into and out of the environment. For example, email and web traffic is to be scanned for malware at the point of entry/exit to/from the environment.

4.3. Isolation of devices that cannot be protected by AV Software

Whenever a networked device cannot have AV software installed such devices are to be configured to operate in a separate ‘unprotected’ VLAN with appropriate mitigation separating such devices from the rest of the environment. This will minimise the risks to both the ‘protected’ and ‘unprotected’ devices minimising the risk of propagation between devices.

4.4. Patch Management

Fully patched devices are significantly less likely to be affected by malicious software. Malware targets known weaknesses, or vulnerabilities, in target operating systems or applications, and uses these to attack the target system. For known weaknesses vendors quickly distribute software updates/patches to prevent exploitation via that particular mechanism. it is therefore important to follow-up on these newly release patches to ensure any newly identified vulnerability is mitigated as quickly as possible; ISMS-03-13: Special Interest Contact list document provides a list of groups that may provide information about possible patch releases. Regular review, assessment and installation of the latest patches should be completed as close to regular release cycles.

Patch Management should aim to ensure that relevant devices are:

- Routinely patched with security patches (patches which have failed testing may be excluded on a host by host basis). The University of Manchester IT Services team update patches on managed desktops on a regular basis;
- Servers: should be no more than 2 months behind available and tested security patches;
- Desktops and Laptops: should be no more than 1 month behind available and tested security patches. This should apply to no less than 70% of systems on or connected to the network;
- Networks/Other: should be no more than 1 month behind available and tested security patches.

4.5. Restricted Download rights

Software programs or executable files are not to be downloaded from the Internet and installed on TRE assets without permission from TRE operations. This is because downloadable programs will need to be assessed for their potential impact on TRE security before installation. Technical controls are in place to restrict the ability of the majority of users to download files from the Internet and onto the TRE. TRE system administrators have greater flexibility to download however; all users should take appropriate precautions to ensure they limit the possibility of downloading malicious software. Should malicious software be suspected of being downloaded onto TRE assets, the user shall report the incident via the Reporting incident procedure (SOP-02-02).

5. Cross-referenced ISMS Documents

Number	Type	Title
ISMS-03-13	ISMS\Policy & Guidance\TRE Operations - policy & guidance	Special Interest Groups Contact List
SOP-02-02	ISMS\SOP\ISMS Management - SOP	Reporting Security Events

6. Appendices

None