Antivirus and Malware Protection Guidelines

Ncell

Guidelines

Approved Date:- 13/12/2019

Ncell	Ncell	Classification: Internal
	Antivirus and Malware Protection Guidelines	Owner: CIO/Head of IT
		Effective Date:01-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Guideline Name DOCID: GD-IT-IS-07

Document Control

i. Document Identification

Document Title and Version:	**GD-IT-IS-07 Antivirus and Malware Protection Guidelines**
Effective Date:	01-10-2019
Document Author:	Information Security Team
Owner:	CIO/Head of IT
Approved By:	CEO

ii. Distribution List

All Ncell Employees
Relevant External Parties and Auditor's (If Required)

iii. Document Roles and Responsibilities

Responsible	Information Security Team
Accountable	CIO/Head of IT
Consulted	Function Heads
Informed	All Employees and External Parties

iv. Digital Signature

CEO	CIO/Head Of IT

v. Revision History

Rev	Date	Author	Description	Approved By	Initiated Date
0	01-10-2019	Information Security Team	Initial document	Vishal Mani Upadhyay	05-12-2019
1	13-12-2019	Tarani Prasad Chaudhary	Revised- Formatting	Andy Chong	13-12-2019
2	22-10-2019	Information Security Team	Minor addition in purpose section. Added points on 5.1.VII to 5.1.X	Vishal Mani Upadhyay	20-12-2021
3	13-12-2019	Tarani Prasad Chaudhary	Revised- Formatting	Andy Chong	20-12-2019
4	28-09-2023	Information Security Team	2. Review changed from annual to once every two years 7.i Removed requirement for daily scan frequency. Added Head of IT	Rajesh Lal Nyachhyon	27-12-2023
5	27-12-2023	Tarani Prasad Chaudhary	Minor Formatting Approval	Rajesh Lal Nyachhyon Jabbor Kayumov	27-12-2023
6	13-05-2024	Information Security	Re-branding	CIO/Head of IT	06-06-2024

Table of Contents

1. Purpose

The purpose of this document is to develop and implement systems and procedures for Ncell to protect its information assets from computer viruses and malwares. This document aims at ensuring correct and secure operations at information storage and processing facilities of Ncell and to provide instructions on measures that must be taken by Ncell's employees to help achieve effective detection, prevention and protection against virus and malware. Malware incident prevention and handling should be incorporated into awareness programs .Vulnerability mitigation capabilities should be in place to help prevent malware incidents. A robust incident response process capability should be in place to addresses malware incident handling.

2. Review and Updating

This procedure shall be reviewed annually or whenever significant changes occur in the organization.

3. Scope

The logical scope of this document includes all information storage and processing assets under ownership of Ncell. The definition of computers includes desktops, workstations, laptops, mobile devices, handheld computing devices, servers and any device that is in use for teleworking.

4. Definitions

i. **Computing network:** A computing network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users
ii. **Logic bomb:** Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed
iii. **Malicious Code:** Malicious code includes all and any programs (including macros and scripts) which are deliberately coded in order to cause an unexpected (and usually, unwanted) event on an IT device
iv. **Malicious software:** Malicious software is software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software
v. **Malware Program:** Malware, short for malicious software, consists of programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behavior
vi. **Network gateways**: A network gateway is an internetworking system capable of joining together two networks that can be implemented completely in software, completely in hardware, or as a combination of both
vii. **Network worm:** A worm that copies itself to another system by using common network facilities and causes execution of the copy program on that system
viii. **Scheduler:** This is a software program or machine that organizes or maintains schedules for running the scan on computer systems configured with antivirus solution/ software
ix. **Spyware:** Spyware is software that aids in gathering information about a person or organization without their knowledge and sending such information to another entity without the user's consent, or that asserts control over a computer without the user's knowledge
x. **Trojan horse:** A Trojan horse, or Trojan, in computing is a non-self-replicating type of malware program containing malicious code that, when executed, carries out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm.
xi. **Virus:** A virus is a piece of potentially malicious programming code that will cause some unexpected or an undesirable event. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable Internet files, diskettes, and CDs. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user
xii. **Virus Definitions:** This term typically refers to the database of all current virus signature files used by a antivirus software for virus detection
xiii. **Virus wall:** A Virus Wall is a program used to block the transmission of files "infected" by a Virus. It is usually implemented as a WWW Proxy or Mail Relay. A Virus wall maybe considered a part of a Firewall

5. Antivirus and Malware Protection Procedure

5.1 Antivirus and Malware Protection Solution Installation

i. Identify and quarantine all known malicious software including viruses, malwares, trojans, hacking tools, spywares, adware and their variants;
ii. Provide zero-day protection against unknown threats;
iii. Protect against all types of web and network threats;
iv. Scan proactively based on schedule and on demand basis;
v. Notify users and administrators about the infected system proactively;
vi. Integrate with Security Incident and Event Management (SIEM) platform.
vii. This standard address prevention of malware incidents which should be used for malware prevention efforts, such as user and IT staff awareness, vulnerability mitigation, and threat mitigation.
viii. Scan for malware on all external media before they can be used (e.g. .USB drive should be scanned first in the laptop before using it).
ix. Scan all e-mail file attachments, including compressed files before opening.
x. In response to an impending malware threat, IT should forbid sending or receiving of relevant types of files (e.g. .exe files) via e-mail for a defined time period
xi. Specify the use of preventive software (e.g., antivirus software, spyware detection, and removal utilities) that are required for various types of systems (e.g., file server, e-mail server, proxy server, workstation, personal digital assistant [PDA]) and applications (e.g., e-mail client, Web browser),
xii. Permit access to external networks (including the Internet) only through organizationapproved and secured mechanisms.
xiii. Ensure that all the firewall configuration changes are approved through a formal process.
xiv. Specify the type of mobile code may be used from various sources (e.g., internal Web servers, other organizations Web servers).
xv. Restrict unauthorized mobile devices from accessing the trusted network.

6. Awareness

An awareness program should be implemented to make users aware of their role in preventing a malware incident. The awareness should explain the risk a malware poses, spreading method and user's negligence or poor awareness that causes the incident. Ncell should also make users aware of policies and procedures that apply to malware incident handling, such as identifying infected systems, reporting suspected infection and user's role in assisting the incident handling.

At minimum, the following shall be followed by users:

i. Users should never reply to e-mail requests for financial or personal information.
ii. Users should not provide passwords, PINs or other access codes in response to emails or unsolicited.
iii. Users should not open suspicious e-mail file attachments, even if they come from known senders. If an unexpected attachment is received users should contact the sender (preferably by a method other than e-mail, such as phone) to confirm that the attachment is legitimate.
iv. Users should not respond to any suspicious or unwanted e-mails.
v. Users should not click on suspicious Web browser popup windows.
vi. Users should not visit web sites that are likely to contain malicious content.
vii. Users should not open files with file extensions (e.g. .bat, .com, .exe, .pif, .vbs) which are likely to be associated with malware.
viii. Users should not disable the additional security control mechanisms (e.g., antivirus software, spyware detection and removal utility, personal firewall).
ix. Users should not use administrator-level accounts for regular system operation

7. Client Configuration

i. Anti-virus / anti-malware agent should be configured to do a real time scan of all the files when they are downloaded or copied or executed.
ii. Anti-virus agent should be configured to ensure that anti-virus scanning process resumes if system reboots in-between scanning process.

iii. Anti-virus / anti-malware agent should allow the On-Demand scanning. It should be able to recognize the last scanned file and resume scanning from the file if an "On-Demand Scan" is interrupted.
iv. Anti-virus / anti-malware agent should be configured to quarantine virus / malware infected files if they cannot be cleaned.
v. Anti-virus / anti-malware agent should be configured to automatically scan any externally connected storage media and when email attachments are downloaded.
vi. Anti-virus / anti-malware should be installed on the Internet proxy server and DNS, it should be configured for the following:
vii. Whenever a user downloads/uploads a file, it should be scanned for viruses and malware.
viii. If a virus / malware is found, then the download/upload should terminate, and the user should be informed on the status.
ix. Anti-virus / anti-malware solution should be able to scan and delete/quarantine malwares, spywares, virus and related threats without causing system instability.
x. Anti-virus / anti-malware solution should be able to scan threats in data transmission protocols including but not limited to following:
    a. HTTPS
    b. SMTP
xi. Anti-virus / anti-malware solution should have features for endpoint protection.
xii. Anti-virus / anti-malware solution should support multi-threaded scanning for high degree of accuracy without leveraging on system resources.
xiii. Anti-virus / anti-malware solution should provide protection against mobile code by the following:
xiv. Blocking any use of mobile code
xv. Blocking receipt of mobile code
xvi. Controlling the resources available to mobile code access

7.1 Application Whitelisting for Critical Systems

xvii. Anti-virus / anti-malware solution should be configured such that end users should not be able to change the configuration settings
xviii. If any system is infected, SOC monitoring team should receive automated alerts from the SIEM tool. Such alerts shall be analyzed by the team and incident tickets shall be created if required and Incident management procedure should be followed.
xix. Server Administrator should duly update the anti-virus software and their latest virus definitions within 24 hours of release
xx. Anti-virus/Anti malware software at server end should be invoked at start-up and kept enabled all the time while running applications related to email messaging or Internet communications. It should also be invoked whenever any new software or drivers are installed
xxi. Advanced anti-malware solution shall be implemented which is capable of blocking malware traffic through behaviour analysis of proxy and incoming e-mail traffic
xxii. Malware protection/Antivirus software shall be distributed automatically and within defined timescales, to reduce the risk of systems being exposed to the most recent malware

7.2 Support Team

i. The ESPP team supported by the Information Security team shall be responsible for managing malware protection and the antivirus solution across Ncell.

7.3 Antivirus Signature Update

i. The number of anti-virus servers, the location of servers, the server hardware sizing and bandwidth requirements should be designed and implemented to ensure that all systems across the enterprise have updated signatures within 24 hours.
ii. Anti-virus primary server should be configured to download new signatures from the supplier site automatically. Manual review should be performed to ensure that the latest signatures are getting updated on the primary server from supplier's site.

7.4 Status Report

Reports should be extracted on status of anti-virus / anti-malware implementation for systems connected on Ncell's corporate network. The reports should include at least the following:

i. IP Address of client
ii. Host name
iii. Last updated on
iv. Client Version
v. Last communication received
vi. Last scan date
vii. No of alerts received and virus/malware quarantined

7.5 Protection against Malicious Code

i. Protection against transmission of Malicious Code should be in place.

7.6 Backup & Redundancy

i. Following components of anti-virus should be backed up:
    a. Operating system files
    b. Anti-Virus application files
    c. Configuration settings
    d. OS and application log files
ii. Recovery testing of anti-virus/anti-malware server should be performed at least once in a year

7.7 Incident Reporting

i. An incident should be reported if the virus/malware is not getting deleted/quarantined by the Anti-virus/Anti-malware on Ncell's Information assets at infosec@ncell.axiata.com
ii. In case of virus/malware outbreak appropriate incident management should be followed to contain the outbreak
iii. Post reporting of incident related to virus/malware, network should be monitored to detect any traces of virus

7.8 Host Based Firewall Security

i. All the endpoints shall have host-based firewall software enabled
ii. Critical systems shall have their host-based firewalls configured according to the firewall rule policy of Ncell
iii. Personal firewall software shall be required on the mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees) when outside Ncell's network which are also used to access Ncell's network.
iv. Host based firewall software shall be configured such that it is always active on devices such as laptops

8. Governance and Compliance

i. Exception management process shall be followed to raise the exception for this procedure.
ii. Internal and external compliance review shall be conducted as per the organization internal and external audit requirements.
iii. Compliance to the group's Malware Incident Prevention and Handling Standard in addition to these guidelines is mandatory.

9. Associated Documents

i. Information Security Policy
ii. Security Incident Management Procedure