Government of Canada Managed Security Service (GCMSS)

Annex A-4: Statement of Work - Antivirus

Date: June 8, 2012

TABLE OF CONTENTS

REFERENCE

Please refer to Annex A - Appendix C: Definitions and Acronyms for a definition of terms and acronyms utilized throughout this annex.

1 ANTIVIRUS

(1) The Antivirus is one of the GCMSS Threat Management Services. When ordered by Canada, by issuing a Task Authorization, the Antivirus, as managed and implemented by the Contractor, must meet or exceed all of the requirements listed in this annex, in the balance of the SOW and elsewhere in the Contract prior to acceptance by Canada and during the entire period of the Contract.

1.1 Quality of Service

(2) The Antivirus detection function must not exceed the rate of one false positive detection per million files scanned. A false positive is the incorrect detection of a virus by the Antivirus in an uninfected file.

1.2 Detection and Response

1.2.1 All Protocols

(3) The Antivirus must scan incoming and outgoing packets.

(4) The Antivirus must scan inside IPv6 native and encapsulated packets.

(5) The Antivirus must detect in real time viruses and malicious code.

(6) The Antivirus must have a virtual execution detection system.

(7) The Antivirus must support multiple languages including double-byte character sets.

(8) The Antivirus must have a Signature-based detection system.

(9) The Antivirus must have a non-signature-based outbreak detection system.

(10) The Antivirus must have a Reputation-based detection system.

(11) The Antivirus must have an Heuristic-based detection system.

(12) The Antivirus must perform file cracking including:

a) scanning of over 100 file types;

b) scanning the following file types:

i) Microsoft Office 2003 (Access, Excel, OneNote, PowerPoint, Publisher, Word, Visio, Project) and above;

ii) Lotus Smart Suite version 9.7;

iii) Adobe PDF version 7 and above;

iv) WinZip version 7 and above;

c) processing embedded files up to the bottom level.

1.2.2 Mail Protocols

(13) The Antivirus must respond to positive virus detections including:

a) Reject the email;

b) Discard the email;

c) Strip the malicious attachments and forward the remaining email content with:

i) a warning message in the subject;

ii) a warning message in the message body;

iii) a list of the stripped attachments; and

iv) a setting in the message header;

d) All other response options supported by the Antivirus solution.

(14) The Antivirus must scan compressed attachments.

(15) The Antivirus must scan embedded attachments.

1.2.3 Web Protocols

(16) The Antivirus must display a virus found web page upon positive virus or malicious content detection.

1.2.4 Other Protocols

(17) The Antivirus must respond to positive virus detections by stripping the malicious content from the data stream.

1.3 Detection Policy

(18) The Antivirus Detection Policy must include, at minimum, the following policies:

a) protocol-based;

b) content-based;

c) message authenticity;

d) sender blacklists; and

e) domain blacklists.

(19) The Contractor must provide the sender and domain blacklists.

1.4 Configuration

(20) When hosted under the GCMSS Threat Management Capacity, Feature Profile Type “XL”, the Antivirus must:

a) provide inbound and outbound proxy mail transfer agent (MTA) services, for email gateways specified by Canada, in support of DNS MX record redirect for content scanning and then relay email to its destination email server; and

b) support domain masquerading.

(21) When hosted under the GCMSS Threat Management Capacity, Feature Profile Type “XL”, the Antivirus must support deployment as a:

a) SMTP relay (performs Antivirus on emails as it is relayed through the device);

b) Web proxy (inspects web content by acting as part of a proxy chain);

c) Routing mode (inspects both Web and SMTP traffic that is routed through the device);

d) ICAP Antivirus based scanner; and

e) stream-based scanner (inspects all content going through the wire).

(22) The Antivirus must support configuration of the sensitivity of the heuristic analysis by Client Organization.

(23) The Antivirus must support configuration to set the max file/email size which can be attached to the email by Client Organization.

(24) The Antivirus must support configuration, by Client Organization, to set the warnings for positive detections in Mail Protocols including:

a) settings in the email header;

b) text in the email subject;

c) text in the email body; and

d) text in the email body for stripped attachments.

(25) The Antivirus must support configuration of blacklists to allow customized entries by Client Organization.

1.4.1 Virus Found Web Page

(26) The Antivirus must allow for the configuration of the virus found web page that the service displays when malware is found in content.

(27) The virus found web page must be Client Organization specific.

(28) Canada must approve the virus found web page.

1.5 Automatic Security Updates

(29) The Antivirus must support automatic security updates of signatures and blacklists directly over the public Internet (i.e. no dependency of any intermediate device) at maximum every hour.

(30) The Contractor must provide automatic security updates within 15 minutes of availability from their supplier.

(31) The Antivirus must apply security updates without rebooting within 15 minutes of receiving the updates.

1.6 Network Protocols

1.6.1 Mail Protocols

(32) The Antivirus must monitor protocols including, but not limited to:

a) SMTP/SMTPS;

b) POP3/POP3S; and

c) IMAP/IMAPS.

1.6.2 Web Protocols

(33) The Antivirus must monitor protocols including, but not limited to:

a) HTTP/HTTPS;

b) FTP/FTPS; and

c) Web 2.0 protocols.

1.6.3 Other Protocols

(34) The Antivirus must monitor protocols including, but not limited to:

a) Telnet;

b) IRC;

c) Peer-to-peer; and

d) Remote desktop protocols.

1.7 Reporting

1.7.1 Daily Reports

(35) The Contractor must provide a daily Antivirus report to Canada in tabular and graphical format that includes:

a) a month to date incoming message activity summary in tabular format;

i) total incoming messages;

ii) number and percentage of messages stopped by reputation filtering;

iii) number and percentage of spam messages detected;

iv) number and percentage of virus messages detected;

v) number and percentage of threat messages detected; and

vi) number and percentage of clean messages accepted;

b) a month to date incoming message activity summary in pie-chart format;

i) number of stopped messages;

ii) number of spam messages detected;

iii) number of virus messages detected; and

iv) number of clean messages accepted;

c) a month to date incoming threat message activity summary in column-chart format;

i) day of the month in the x axis; and

ii) number of threat messages detected in the y axis;

d) a month to date tabular list of incoming messages per day with totals;

i) total incoming messages; and

ii) number and percentage of threat messages detected;

e) a month to date tabular list of outgoing messages per day with totals;

i) date;

ii) total outgoing messages; and

iii) number and percentage of threat messages detected;

f) a month to date tabular list of unique viruses name with number of occurrences detected.

1.8 Implementation

(36) The Contractor must inventory, review, optimize and implement in GCMSS existing rules, policies, and any other configuration of the existing antivirus solution of the Client Organization.

(37) The Contractor must document, review, optimize and implement, in GCMSS, configuration requirements of the Client Organization for the Antivirus.

(38) The Contractor must deploy the Antivirus as specified by Canada.

1.9 Change Management

(39) The Contractor must update the virus found web page for positive detections when requested by Canada within 2 FGWDs.

(40) The Contractor must configure sender blacklists, as requested by Canada, in accordance with priority levels as specified by Canada.

(41) The Contractor must configure domain blacklists, as requested by Canada, in accordance with priority levels as specified by Canada.

(42) The Contractor must configure the Antivirus MTA to correctly function with the DNS MX Record redirect, as requested by Canada, in accordance with priority levels as specified by Canada.

(43) The Contractor must configure the sensitivity of the heuristic analysis, as requested by Canada, in accordance with priority levels as specified by Canada.

(44) The Contractor must configure the max file/email size which can be attached to the email, as requested by Canada, in accordance with priority levels as specified by Canada.

(45) The Contractor must configure the response to virus detection in Mail Protocols, as requested by Canada, in accordance with priority levels as specified by Canada.