Service de sécurité géré du gouvernement du Canada (SSGGC)

Annexe A-4 : Énoncé des travaux – Antivirus

Date : 8 juin 2012

TABLE DES MATIÈRES

RÉFÉRENCE

Voir l'appendice C : Définitions et acronymes de l'annexe A pour obtenir une définition des termes et des acronymes utilisés dans la présente annexe.

1 ANTIVIRUS

(1) L'antivirus constitue un des services de gestion des menaces du SSGGC. Lorsque le Canada en fait la commande par l'émission d'une autorisation de tâches, l'antivirus, tel qu'il est géré et mis en œuvre par l'entrepreneur, doit respecter ou dépasser toutes les exigences mentionnées dans la présente annexe et dans le reste de l'Énoncé des travaux, ainsi qu'ailleurs dans le contrat, et ce, avant son acceptation par le Canada et tout au long de la durée du contrat.

1.1 Qualité de service

(2) La fonction de détection de l'antivirus ne doit pas dépasser le taux d'une détection fausse positive par million de fichiers analysés. Une détection fausse positive correspond à la détection incorrecte d'un virus par l'antivirus dans un fichier non infecté.

1.2 Détection et réponse

1.2.1 Tous les protocoles

(3) L'antivirus doit analyser les paquets entrants et sortants.

(4) L'antivirus doit analyser l'intérieur des paquets IPv6 natifs et encapsulés.

(5) L'antivirus doit détecter les virus et les codes malicieux en temps réel.

(6) L'antivirus doit être doté d'un système de détection des comportements suspects qui s'exécutent dans un environnement virtuel.

(7) L'antivirus doit prendre en charge de multiples langues, y compris les jeux de caractères à deux octets.

(8) L'antivirus doit être doté d'un système de détection axé sur les signatures.

(9) L'antivirus doit être doté d'un système de détection des virus non axé sur les signatures.

(10) L'antivirus doit être doté d'un système de détection axé sur la réputation.

(11) L'antivirus doit être doté d'un système de détection axé sur une méthode heuristique.

(12) L'antivirus doit effectuer le craquage de fichiers, y compris :

a) L'analyse de plus de 100 types de fichiers;

b) L'analyse des types de fichiers suivants :

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

ii) Lotus Smart Suite version 9.7;

iii) Adobe PDF version 7 et supérieure;

iv) WinZip version 7 et supérieure;

c) Le traitement des fichiers intégrés jusqu'au niveau inférieur.

1.2.2 Protocoles de courrier

(13) L'antivirus doit répondre aux détections positives des virus, notamment en :

a) Rejetant le courriel;

b) Écartant le courriel;

c) Supprimant les pièces jointes malveillantes et en transmettant le reste du contenu du courriel accompagné de ce qui suit :

i) Un message d'avertissement dans la zone Objet du courriel;

ii) Un message d'avertissement dans le corps du courriel;

iii) Une liste des pièces jointes supprimées;

iv) Une consigne dans l'en-tête du courriel;

d) Prenant en charge toutes les autres possibilités de réponse.

(14) L'antivirus doit analyser les pièces jointes compressées.

(15) L'antivirus doit analyser les pièces jointes intégrées.

1.2.3 Protocoles Web

(16) L'antivirus doit afficher une page Web dressant la liste des virus détectés au moment de la détection positive d'un virus ou d'un contenu malveillant.

1.2.4 Autres protocoles

(17) L'antivirus doit répondre à la détection positive d'un virus en supprimant le contenu malveillant du flux de données.

1.3 Politique de détection

(18) La politique de détection des virus doit comprendre, au minimum, des règles concernant ce qui suit :

a) La détection fondée sur les protocoles;

b) La détection fondée sur le contenu;

c) L'authenticité des messages;

d) Les listes noires d'expéditeurs;

e) Les listes noires de domaines.

(19) L'entrepreneur doit fournir les listes noires d'expéditeurs et de domaines.

1.4 Configuration

(20) Lorsqu'il est hébergé sous le type de profil de fonction XL de la capacité de gestion des menaces du SSGGC, l'antivirus doit :

a) Fournir des services d'agent de transfert de messages (ATM) [serveur mandataire] entrants et sortants, pour les passerelles de courrier électronique précisées par le Canada, à l'appui de la redirection des enregistrements MX du SND aux fins d'analyse du contenu et par la suite transmettre le courriel à son serveur de

courriel de destination;

b) Prévoir des mesures de protection contre l'usurpation des domaines.

(21) Lorsqu'il est hébergé sous le type de profil de fonction XL de la capacité de gestion des menaces du SSGGC, l'antivirus doit prendre en charge le déploiement en tant que :

a) Relais SMTP (analyse les courriels aux fins de détection de virus à mesure qu'ils sont transmis au travers du dispositif);

b) Mandataire Web (inspecte le contenu Web dans le cadre d'une chaîne de mandataire);

c) Mode de routage (inspecte à la fois le trafic Web et SMTP qui est acheminé au travers du dispositif);

d) Scanneur de virus basé sur le protocole ICAP;

e) Scanneur axé sur les flux (inspecte tout le contenu qui passe au travers du réseau).

(22) L'antivirus doit prendre en charge les mécanismes de configuration permettant de définir la sensibilité de l'analyse heuristique effectuée par organisation cliente.

(23) L'antivirus doit prendre en charge les mécanismes de configuration permettant de régler, par organisation cliente, la taille maximale des fichiers ou des courriels pouvant être joints au courrier électronique.

(24) L'antivirus doit prendre en charge les mécanismes de configuration permettant de régler, par organisation cliente, les alertes concernant la détection positive de virus dans les protocoles de courrier notamment en :

a) Déterminant les paramètres dans l'en-tête du courriel;

b) Définissant le texte dans la zone objet du courriel;

c) Définissant le texte dans le corps du courriel;

d) Définissant, dans le corps du courriel, le texte concernant les pièces jointes supprimées.

(25) L'antivirus doit prendre en charge les mécanismes de configuration permettant de dresser des listes noires afin de permettre de concevoir des entrées personnalisées par organisation cliente.

1.4.1 Page Web dressant la liste des virus détectés

(26) L'antivirus doit permettre la configuration de la page Web dressant la liste des virus détectés; le service affiche cette page lorsqu'il détecte des codes malveillants dans le contenu.

(27) Le page Web répertoriant les virus détectés doit être propre à l'organisation cliente.

(28) Le Canada doit approuver ladite page Web.

1.5 Mises à jour de sécurité automatiques

(29) L'antivirus doit prendre en charge les mises à jour de sécurité automatiques des signatures et des listes noires exécutées directement depuis Internet (c'est-à-dire sans dépendre d'un dispositif intermédiaire) toutes les heures, au plus.

(30) L'entrepreneur doit fournir les mises à jour de sécurité automatiques dans les 15 minutes suivant le moment où le fournisseur les rend disponibles.

(31) L'antivirus doit appliquer les mises à jour de sécurité sans redémarrage dans les 15 minutes suivant leur réception.

1.6 Protocoles réseau

1.6.1 Protocoles de courrier

(32) L'antivirus doit surveiller les protocoles suivants, sans s'y limiter :

a) SMTP/SMTPS;

b) POP3/POP3S;

c) IMAP/IMAPS.

1.6.2 Protocoles Web

(33) L'antivirus doit surveiller les protocoles suivants, sans s'y limiter :

a) HTTP/HTTPS;

b) PTF/PTFS;

c) Protocoles Web 2.0.

1.6.3 Autres protocoles

(34) L'antivirus doit surveiller les protocoles suivants, sans s'y limiter :

a) Telnet;

b) IRC;

c) Point à point;

d) Protocoles de bureau à distance.

1.7 Rapports

1.7.1 Rapports quotidiens

(35) L'entrepreneur doit fournir au Canada un rapport quotidien sur l'antivirus; le rapport est présenté sous forme de tableau ou de graphique et porte sur ce qui suit :

a) Un résumé de l'activité concernant les messages entrants depuis le début du mois; ce résumé est présenté sous forme de tableau et indique ce qui suit :

i) Le nombre total de messages entrants;

ii) Le nombre et le pourcentage de messages bloqués par filtrage de réputation;

iii) Le nombre et le pourcentage de pourriels détectés;

iv) Le nombre et le pourcentage de virus détectés;

v) Le nombre et le pourcentage de menaces détectées;

vi) Le nombre et le pourcentage de messages sains acceptés;

b) Un résumé de l'activité concernant les messages entrants depuis le début du mois; ce résumé est présenté sous forme de graphique circulaire et indique ce qui suit :

i) Le nombre de messages bloqués;

ii) Le nombre de pourriels détectés;

iii) Le nombre de virus détectés;

iv) Le nombre de messages sains acceptés;

c) Un résumé, sous forme de graphique à colonnes, de l'activité concernant les messages entrants depuis le début du mois, où :

i) Le jour du mois figure sur l'axe x;

ii) Le nombre de menaces détectées figure sur l'axe y;

d) Une liste, sous forme de tableau, des messages entrants depuis le début du mois, ventilés par jour, indiquant :

i) Le nombre total de messages entrants;

ii) Le nombre et le pourcentage de menaces détectées;

e) Une liste, sous forme de tableau, des messages sortants depuis le début du mois, ventilés par jour, indiquant :

i) La date;

ii) Le nombre total de messages sortants;

iii) Le nombre et le pourcentage de menaces détectées;

f) Une liste, sous forme de tableau, des noms uniques des virus et du nombre d'occurrences détectées depuis le début du mois.

1.8 Mise en œuvre

(36) L'entrepreneur doit inventorier, examiner, optimiser et mettre en œuvre, dans le SSGGC, les règles, politiques et toute autre configuration existantes de la solution existante d'antivirus de l'organisation cliente.

(37) L'entrepreneur doit documenter, examiner, optimiser et mettre en œuvre, dans le SSGGC, les exigences de l'organisation cliente relatives à l'antivirus.

(38) L'entrepreneur doit déployer l'antivirus, selon ce que précise le Canada.

1.9 Gestion des changements

(39) L'entrepreneur doit mettre à jour la page Web dressant la liste des virus détectés, dans les cas de détection positive de virus, dans les deux JOFPF suivant la demande présentée par le Canada à ce sujet.

(40) L'entrepreneur doit configurer les listes noires d'expéditeurs, selon ce que demande le Canada, en fonction des niveaux de priorisation qu'il précise.

(41) L'entrepreneur doit configurer les listes noires de domaines, selon ce que demande le Canada, en fonction des niveaux de priorisation qu'il précise.

(42) L'entrepreneur doit configurer l'ATM de l'antivirus pour qu'il fonctionne correctement avec le mécanisme de redirection des enregistrements MX du SND, selon ce que

demande le Canada, en fonction des niveaux de priorisation qu'il précise.

(43) L'entrepreneur doit configurer les mécanismes permettant de définir la sensibilité de l'analyse heuristique, selon ce que demande le Canada, en fonction des niveaux de priorisation qu'il précise.

(44) L'entrepreneur doit configurer les mécanismes permettant de régler la taille maximale des fichiers ou des courriels pouvant être joints au courrier électronique, selon ce que demande le Canada, en fonction des niveaux de priorisation qu'il précise.

(45) L'entrepreneur doit configurer la réponse aux virus détectés dans les protocoles de courrier, selon ce que demande le Canada, en fonction des niveaux de priorisation qu'il précise.