Service de sécurité géré du gouvernement du Canada (SSGGC)

Annexe A-5 : Énoncé des travaux – Antipourriel

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 ANTIPOURRIEL

(1) L'antipourriel 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'antipourriel, 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'antipourriel ne doit pas dépasser le taux d'une détection fausse positive par million de courriels analysés. Une détection fausse positive correspond à la détection incorrecte d'un pourriel dans un courriel légitime.

1.2 Détection et réponse

(3) L'antipourriel doit analyser les courriels entrants et sortants.

(4) L'antipourriel doit détecter les pourriels.

(5) L'antipourriel doit détecter les pourriels dans les pièces jointes des courriels qui adoptent un des formats suivants :

a) Microsoft Office;

b) PDF;

c) Fichiers images;

d) HTML.

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

(7) L'antipourriel doit être doté de systèmes de filtrage que comprennent, sans s'y limiter :

a) Des expressions rationnelles;

b) Des cotes découlant de l'évaluation de la réputation des expéditeurs;

c) Des cotes découlant de l'évaluation de la réputation des expéditeurs IP;

d) Des mécanismes fondés sur les signatures;

e) Des mécanismes fondés sur le contenu;

f) L'étranglement du débit des messages;

g) L'analyse bayésienne;

h) L'analyse de l'empreinte du message;

i) L'analyse de la somme de contrôle;

j) L'évaluation heuristique;

k) L'authenticité des messages;

l) Les listes noires d'expéditeurs;

m) Les listes blanches d'expéditeurs;

n) Les listes blanches de domaines;

o) Les listes noires de domaines.

(8) L'antipourriel doit bloquer les messages fragmentés.

(9) L'antipourriel doit prendre en charge l'antiusurpation d'adresse électronique, y compris :

a) L'identification de l'expéditeur du message;

b) Le cadre politique de l'expéditeur;

c) L'identification de l'expéditeur;

d) Le courrier identifié par clé de domaine;

e) La vérification inverse du SND.

(10) L'antipourriel doit offrir une variété de réponses, notamment, sans s'y limiter, en :

a) Rejetant le courriel;

b) Écartant le courriel;

c) Acceptant le courriel et en y insérant un message d'avertissement dans la zone Objet et dans le corps et l'en-tête du message.

1.3 Traitement des messages

(11) L'antipourriel doit prendre en charge de multiples domaines de courriel.

(12) L'antipourriel doit prendre en charge les passerelles de courriel SMTP pour les serveurs de courriels courants que précise le Canada.

(13) L'antipourriel doit prendre en charge l'acheminement de courriel basé sur LDAP en recourant à un serveur LDAP que précise le Canada.

(14) L'antipourriel doit prendre en charge le relais de courrier sortant SMTP.

1.4 Configuration

(15) Lorsqu'il est hébergé sous le type de profil de fonction XL de la capacité de gestion des menaces du SSGGC, l'antipourriel 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.

(16) L'antipourriel doit prendre en charge les mécanismes de configuration permettant de dresser des listes noires afin de permettre à l'organisation cliente de concevoir des entrées personnalisées.

(17) L'antipourriel doit prendre en charge les mécanismes de configuration permettant de dresser des listes blanches afin de permettre à l'organisation cliente de concevoir des entrées personnalisées.

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

1.5 Mises à jour de sécurité automatiques

(19) L'antipourriel 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.

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

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

1.6 Protocoles réseau

(22) L'antipourriel doit surveiller les protocoles suivants, sans s'y limiter :

a) SMTP;

b) POP3;

c) IMAP.

1.7 Rapports

1.7.1 Rapports quotidiens

(23) L'entrepreneur doit fournir au Canada un rapport quotidien sur l'antipourriel; 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 empilées, 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 total de messages par type (bloqué, pourriel positif, pourriel soupçonné) empilé figurant sur l'axe y.

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

i) La date;

ii) Le nombre total de messages entrants;

iii) Le nombre total de messages bloqués;

iv) Le nombre total de pourriels positifs;

v) Le nombre total de pourriels soupçonnés;

vi) Le nombre de messages bloqués en pourcentage;

vii) Le nombre de pourriels positifs en pourcentage;

viii) Le nombre de pourriels soupçonnés en pourcentage.

e) Une liste, sous forme de tableau, des sept principaux domaines récipiendaires indiquant, depuis le début du mois :

i) Le domaine récipiendaire;

ii) Le nombre total de messages entrants;

iii) Le nombre total de pourriels positifs;

iv) Le nombre de pourriels positifs en pourcentage;

v) Le nombre total de pourriels soupçonnés;

vi) Le nombre de pourriels soupçonnés en pourcentage.

f) Une liste, sous forme de tableau, des 25 principaux domaines expéditeurs indiquant, depuis le début du mois :

i) Le domaine expéditeur;

ii) Le nombre total de messages entrants;

iii) Le nombre total de pourriels positifs;

iv) Le nombre de pourriels positifs en pourcentage;

v) Le nombre total de pourriels soupçonnés;

vi) Le nombre de pourriels soupçonnés en pourcentage.

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

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

ii) Le nombre total de messages par type (pourriel positif, pourriel soupçonné) empilé figure sur l'axe y.

h) 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 total de pourriels positifs;

iv) Le nombre total de pourriels soupçonnés;

v) Le nombre de pourriels positifs en pourcentage;

vi) Le nombre de pourriels soupçonnés en pourcentage.

1.8 Mise en œuvre

(24) 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'antipourriel de l'organisation cliente.

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

1.9 Gestion des changements

(26) L'entrepreneur doit configurer la réponse aux détections positives de pourriels, selon ce que précise le Canada, et ce, dans les deux JOFPF suivant le moment où il en fait la demande.

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

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

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

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

(31) 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.

(32) L'entrepreneur doit configurer l'ATM de l'antipourriel 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.