Service de sécurité géré du gouvernement du Canada (SSGGC)

Annexe A-2 : Énoncé des travaux – Prévention et détection des intrusions

Date : 12 juillet 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 PRÉVENTION ET DÉTECTION DES INTRUSIONS

(1) La prévention et la détection des intrusions (PDI) constituent un des services de gestion des menaces du SSGGC. Lorsque le Canada en fait la commande par l'émission d'une autorisation de tâches, la PDI, telle qu'elle est gérée et mise 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 Détection et réponse

(2) La PDI doit balayer les paquets entrants et sortants.

(3) La PDI doit balayer l'intérieur des paquets encapsulés.

(4) La PDI doit détecter les événements d'intrusion en temps réel.

(5) La PDI doit être dotée d'un système de prévention des intrusions axé sur le hachage flou.

(6) La PDI doit être dotée d'un système de prévention des intrusions axé sur les signatures.

(7) La PDI doit être dotée d'un système de prévention des intrusions axé sur les anomalies statistiques.

(8) La PDI doit détecter et atténuer les attaques par déni de service.

(9) La PDI doit être compatible avec les vulnérabilités et expositions courantes (VEC).

(10) La PDI doit prendre en charge des capteurs basés sur des profils externes aux fins de PDI, permettant notamment ce qui suit :

a) L'intégration transparente des capteurs;

b) L'activation des capteurs;

c) La configuration des capteurs;

d) L'acceptation des rapports provenant des capteurs;

e) La surveillance de multiples capteurs;

f) L'identification d'événements à partir des rapports produits par les capteurs;

g) La transmission de commandes aux capteurs afin de répondre aux événements.

(11) Le PDI doit prendre en charge une diversité de techniques de prévention, y compris au minimum :

a) L'abandon de paquets;

b) La réinitialisation TCP.

(12) La PDI doit prendre en charge le fonctionnement à état (compatible avec la session), notamment :

a) Le réassemblage des paquets TCP;

b) La défragmentation des ID;

c) L'inspection bidirectionnelle;

d) La collecte de données judiciaires;

e) Les listes d'accès.

(13) La PDI doit inspecter le trafic Web, dont le langage est HTML 5 ou inférieur.

(14) La PDI doit bloquer les requêtes HTTP/HTTPS dont l'URL est plus longue que la valeur précisée par le Canada.

(15) La PDI doit comporter un mode silencieux configurable où aucun message n'est envoyé lorsque les demandes sont bloquées.

(16) L'état à sécurité intégrée de la PDI doit être configurable à la position ouverte ou fermée par le Canada.

1.2 Configuration

(17) La PDI doit prendre en charge la configuration des réponses en fonction de chaque signature.

(18) La PDI doit prendre en charge le balayage des configurations d'exclusion en fonction de chaque hôte.

(19) La PDI doit prendre en charge le balayage des configurations d'exclusion en fonction de chaque signature.

(20) La PDI doit prendre en charge la définition des signatures au moyen d'expressions rationnelles.

(21) La PDI doit prendre en charge la configuration de la longueur maximale d'une URL.

(22) La PDI doit prendre en charge la configuration de signatures personnalisées.

(23) La PDI doit prendre en charge les configurations suivantes :

a) Hors bande en mode SDI (flux de trafic par connecteur réseau [PAT]);

b) Intrabande en mode SPI en utilisant un mode passerelle (agit comme un dispositif de couche 2 sans exigence d'adresse IP);

c) Intrabande en mode SPI en mode acheminé (le trafic est acheminé au travers de dispositifs au niveau de la couche TCP/IP).

(24) La PDI doit prendre en charge la configuration de la réponse de la DPI en fonction d'une signature.

1.3 Mises à jour de sécurité automatiques

(25) La DPI doit prendre en charge les mises à jour de sécurité automatiques exécutées directement depuis Internet (c'est-à-dire sans dépendre d'un dispositif intermédiaire) toutes les heures, au plus.

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

(27) La DPI doit appliquer les mises à jour de sécurité sans redémarrage dans les 15 minutes suivant leur réception.

1.4 Protocoles réseau

(28) La PDI doit surveiller les protocoles suivants, sans s'y limiter :

a) TCP/IP;
b) ICMP;
c) PTF;
d) UDP;
e) SMTP;
f) HTTP/HTTPS;
g) SNMP;
h) SND;
i) APD;
j) NetBIOS;
k) Telnet.

(29) La PDI doit surveiller le trafic MPLS.

(30) La PDI doit surveiller le trafic 802.1Q (à ressources partagées).

1.5 Capteur de la DPI

(31) Le capteur de la DPI doit prendre en charge les plateformes suivantes :

a) Microsoft Windows Server 2003 et supérieur;
b) Solaris (architecture de processeur à échelle variable [SPARC]);
c) Serveur Linux SUSE;
d) Red Hat Enterprise Linux;
e) HP-UX;
f) AIX;
g) Autres systèmes d'exploitation tel qu'en conviennent le Canada et l'entrepreneur;
h) La solution matérielle spécialisée du fabricant d'équipement d'origine.

(32) Le capteur de la PDI doit permettre la réalisation de ce qui suit :

a) L'analyse de journaux;
b) La vérification de l'intégrité des fichiers;
c) La détection des programmes malveillants furtifs;
d) L'alertage temporel;
e) La détection des infractions aux politiques;
f) Les réponses actives selon les politiques enfreintes;
g) Le renvoi d'information à la PDI.

(33) Le capteur de la PDI situé sur la solution logicielle spécialisée du fabricant

d'équipement d'origine doit :

a) Prendre en charge la vitesse filaire de la capacité de gestion des menaces;

b) Être entièrement géré par l'entrepreneur.

1.6 Journalisation

(34) La PDI doit enregistrer les paquets d'événements et toutes les métadonnées connexes qui y sont liées.

1.7 Rapports

1.7.1 Rapports mensuels

(35) L'entrepreneur doit fournir au Canada un rapport mensuel concernant la gestion de la PDI; les données sont ventilées par organisation cliente et portent sur ce qui suit :

a) Un résumé comparant le nombre d'événements survenus pendant le mois courant par rapport au mois précédent et présentant en termes simples les écarts et les facteurs qui expliquent ces statistiques;

b) Le nombre de billets d'incident du type « demande d'information » en suspens;

c) Le résumé, sous forme de tableau, concernant la gestion d'un problème;

   i) L'état du billet d'incident (ouvert, fermé, en suspens);

   ii) Le numéro du billet d'incident;

d) Le nombre de demandes de changement traitées;

e) Une liste, sous forme de tableau, des billets d'incident du type « demande d'information » indiquant :

   i) La date de fermeture;

   ii) La date de création;

   iii) Le numéro de billet;

   iv) La gravité de l'incident;

   v) La description de l'incident;

   vi) Les commentaires;

   vii) L'état de l'incident;

   viii) Le temps de réponse (en secondes);

   ix) Le temps de confinement (en secondes);

f) Une liste, sous forme de tableau, des billets relatifs aux demandes de changement indiquant :

   i) Le numéro de billet;

   ii) La description du changement;

   iii) Les commentaires;

   iv) L'état.

1.7.2 Rapports quotidiens

(36) L'entrepreneur doit fournir au Canada un rapport quotidien concernant la PDI par capteur; ce rapport est présenté sous forme de tableau ou de graphique, est ventilé par organisation cliente et indique ce qui suit :

a) Un résumé, sous forme de graphique à bandes, des événements pour les cinq principaux capteurs, où :

i) Le nombre total d'événements concernant le capteur figure sur l'axe x;

ii) Le nom du capteur figure sur l'axe y;

b) Un résumé des 50 principaux événements, présentés sous forme de tableau, indiquant :

i) Le nom du capteur;

ii) Les détails de l'événement;

iii) La gravité de l'événement;

iv) Le nombre d'événements.

(37) L'entrepreneur doit fournir au Canada un rapport quotidien concernant la PDI selon la gravité de l'événement; ce rapport est présenté sous forme de tableau ou de graphique, est ventilé par organisation cliente et indique ce qui suit :

a) Un résumé, sous forme de graphique à colonnes empilées, des événements survenus pendant les deux semaines précédentes, où :

i) La date de l'événement figure sur l'axe x;

ii) Le nombre total d'événements selon la gravité, empilés, figure sur l'axe y;

b) Un résumé des événements survenus pendant les deux semaines précédentes, présentés sous forme de tableau, indiquant :

i) La date de l'événement;

ii) La gravité de l'événement;

iii) Le nombre d'événements.

(38) L'entrepreneur doit fournir au Canada un rapport quotidien concernant la PDI par IP source; ce rapport est présenté sous forme de tableau ou de graphique, est ventilé par organisation cliente et indique ce qui suit :

a) Un résumé, sous forme de graphique à bandes, des événements pour les cinq principales IP source, où :

i) Le nombre total d'événements concernant l'IP source figure sur l'axe x;

ii) L'IP source figure sur l'axe y;

b) Un résumé des 50 principaux événements, présentés sous forme de tableau, indiquant :

i) L'IP source;

ii) Les détails de l'événement;

iii) La gravité de l'événement;

iv) Le nombre d'événements.

(39) L'entrepreneur doit fournir au Canada un rapport quotidien concernant la PDI par IP cible; ce rapport est présenté sous forme de tableau ou de graphique, est ventilé par organisation cliente et indique ce qui suit :

a) Un résumé, sous forme de graphique à bandes, des événements pour les cinq principales IP cible, où :

i) Le nombre total d'événements concernant l'IP cible figure sur l'axe x;

ii) L'IP cible figure sur l'axe y;

b) Un résumé des 50 principaux événements, présentés sous forme de tableau, indiquant :

i) L'IP cible;

ii) Les détails de l'événement;

iii) La gravité de l'événement;

iv) Le nombre d'événements.

1.8 Mise en œuvre

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

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

(42) L'entrepreneur doit installer le matériel du capteur de la PDI, selon ce que précise le Canada à l'égard du NS-TRAT.

1.9 Gestion des changements

(43) L'entrepreneur doit configurer les réponses de la PDI visant des signatures précises, selon ce que demande le Canada, en fonction des niveaux de priorisation qu'il précise.

(44) L'entrepreneur doit configurer les exclusions de balayage visant les hôtes et les signatures, selon ce que demande le Canada, en fonction des niveaux de priorisation qu'il précise.

(45) L'entrepreneur doit configurer les exceptions visant expressément les signatures, selon ce que demande le Canada, en fonction des niveaux de priorisation qu'il précise.

(46) L'entrepreneur doit configurer les signatures de menace, selon ce que demande le Canada, en fonction des niveaux de priorisation qu'il précise.

(47) L'entrepreneur doit configurer les capteurs de la PDI, selon ce que demande le Canada, en fonction des niveaux de priorisation qu'il précise.