

Marché public de services

Sécurisation des accès extérieurs

Appel d'offres ouvert

Cahier des Clauses Techniques Particulières (C.C.T.P.) - Annexe 1

SECURITE INFORMATIQUE

CONFORMITÉ

Droit d'audit

L'ETABLISSEMENT DE SANTE se réserve le droit de contrôler la qualité et la sécurité du Système fourni par le titulaire, via des audits et/ou des tests d'intrusion.

Un accord formel du titulaire doit préciser :

- Les types de tests d'intrusion et d'audit technique autorisés,
- Les audits techniques qui nécessitent de prévenir le titulaire.

Les types d'audits techniques à considérer sont les tests d'intrusion (de niveau réseau et/ou applicatif), les audits de configuration de composants logiciels et les audits de code source. À l'issue de l'audit, si un plan de remédiation est proposé, le titulaire s'engage sur un planning de mise en œuvre.

Sous-traitance

En cas de recours à de la sous-traitance pour les actions d'administration et de maintenance du DM, le titulaire s'engage à faire respecter à ses propres sous-traitants les mêmes objectifs de sécurité que ceux auxquels il est soumis

GESTION DES ACCÈS

Gestion des profils et des droits

Le titulaire doit décrire les fonctions accédées par les différents profils d'utilisateur du dispositif médical. Il doit également décrire les fonctions avancées accédées spécifiquement par le ou les profils d'administrateur (accès aux configurations, aux paramètres, au mode sans échec, au mode debug...)

CONNECTIVITÉ ET SÉCURITÉ DES RÉSEAUX

Protocoles d'authentification

Le titulaire doit pouvoir fournir la procédure de connexion du dispositif médical sur le réseau de l'établissement, notamment une description des mécanismes standards d'identification et d'authentification supportés par le dispositif. Les protocoles de chiffrement utilisés pour sécuriser l'authentification et la connexion doivent être surs et connus (ex: SHA256, AES, AES-CBC, RSA-OAEP).

Matrice de flux réseaux

Le titulaire assure la mise à disposition d'une matrice des flux réseaux qui décrit les flux entrants et sortants du dispositif médical. Elle décrit notamment :

- l'identification et la description de chaque flux,
- l'exposition à Internet (télésupervision, télémaintenance, Big Data...),
- l'émetteur (application, poste, serveur, base de données...),
- le récepteur (application, poste, serveur, base de données...),
- le protocole réseau utilisé,
- le chiffrement (algorithme), si applicable.

Si le dispositif médical est composé de plusieurs matériels connectés en réseau, le titulaire doit pouvoir fournir la matrice des flux réseaux entre ces matériels. Les flux réseaux doivent être limités au strict nécessaire.

Schéma d'architecture

Si le dispositif médical est composé de plusieurs composants physiques (poste, serveur, appareil...) qui sont connectés entre eux, le titulaire doit fournir un schéma d'architecture réseau à l'établissement. Il doit notamment faire apparaître :

- les serveurs physiques et/ou virtuels
- les postes clients et de pilotage

- les matériels médicaux
- les sous-réseaux traversés par les flux entre ces composants

EXPLOITATION ET COMMUNICATION

Mise en service

Si le dispositif médical nécessite des actions de la part de l'établissement, le titulaire doit fournir un guide d'installation et de mise en service intégrant les modalités ci-dessous :

- la liste des éventuels services à désactiver,
- la liste des comptes inutiles ou obsolètes à désactiver ou à supprimer,
- la liste des comptes à privilèges dont les mots de passe doivent être modifiés

Détection d'une vulnérabilité critique

En cas de mise en évidence d'une vulnérabilité critique (niveau de CVSS supérieur à 7) affectant le dispositif médical, le titulaire doit mettre à disposition de l'établissement et dans les meilleurs délais une solution de contournement ou une solution palliative (mise à disposition de correctifs) n'affectant ni les performances ni les fonctionnalités du DM. Le titulaire collabore également avec l'établissement pour déterminer l'origine de la vulnérabilité et les actions à engager pour l'éradiquer.

Mise au rebut

En cas de maintenance du matériel ou de mise au rebut, le titulaire doit supprimer de manière sécurisée les données à caractère personnel de santé présentes sur les disques durs ou dans la mémoire intégrée. Un procès-verbal doit être signé entre le titulaire et l'établissement.

DÉVELOPPEMENT ET MAINTENANCE DES LOGICIELS

Maintenance

Le titulaire doit pouvoir fournir une procédure de maintenance précisant les modalités de mise à jour en toute sécurité du dispositif médical.

Ces modalités doivent inclure :

- méthodes et outils (logiciels ou matériels) utilisés par les intervenant,
- sécurité appliquée sur ces outils (configuration, contrôle d'accès, traçabilité),
- fonctionnalités du dispositif médical qui restent actives durant l'opération de maintenance,
- mesures de sécurité qui empêchent l'accès aux données personnelles de santé stockées dans le dispositif médical par le mainteneur, • contrôle de l'origine et de l'intégrité des fichiers de mise à jour,
- modalités de retour arrière en cas d'échec de la mise à jour.

Cette procédure doit être validée par l'ETABLISSEMENT DE SANTE. Chaque opération de maintenance doit faire l'objet d'un compte-rendu de l'opération notifié et consultable par l'établissement.

Il doit être possible de faire scanner le contenu de la mise à jour avant son installation dans le DM, quel que soit le moyen de support utilisé par le mainteneur (portail fabricant, clé USB, disque dur, PC d'opérateur, etc.).

Télémaintenance

Dans le cadre d'un accès de télémaintenance, le titulaire doit utiliser les moyens de connexion à distance mis en œuvre par l'ETABLISSEMENT DE SANTE.

Toute opération de télémaintenance doit être annoncée à l'établissement par le titulaire.

L'opération doit être planifiée et cadrée dans le temps avec une date de début et de fin. La connexion ne sera accordée et ouverte uniquement que durant la période convenue.

Une procédure d'exception peut être prévue pour autoriser temporairement, afin de répondre à des besoins d'intervention en urgence.

Un compte-rendu de l'intervention doit être dressé par le titulaire à la fin de l'opération de télémaintenance et transmis à l'établissement.

Le titulaire doit fournir les IP publiques à partir desquelles les opérateurs de maintenance réalisent leurs opérations.

Gestion des logiciels tiers

Le titulaire doit fournir la liste exhaustive des logiciels tiers (OS, firmwares, librairies, outil de télésurveillance, outil de télémaintenance, etc.), i.e. qui n'ont pas été développés par le titulaire, avec leurs versions au moment de la commande. Le titulaire s'engage à maintenir ces logiciels tiers pendant la durée de vie du dispositif médical, notamment dans le cadre de la matériovigilance.

Le temps de garantie de fourniture des logiciels doit être inclus dans le marché de maintenance.

PROTECTION DES DONNÉES

Protection des données personnelles de santé

Le titulaire doit pouvoir décrire les modalités de transfert et d'export des données personnelles de santé, en précisant les protocoles utilisés. Les protocoles de chiffrement utilisés pour sécuriser l'authentification et la connexion doivent être sûrs et connus (ex: SHA256, AES, AES-CBC, RSA-OAEP). Si des données sont stockées dans le dispositif médical, les modalités d'accès et de stockage doivent être conformes au RGPD, aux exigences identifiées dans le Cadre d'Interopérabilité des SIS publiés par l'ANS et à la PSSI de l'établissement.

SÉCURITÉ PHYSIQUE

Sécurité physique du dispositif médical

Les mesures de sécurité physique sur le dispositif médical doivent être documentées pour limiter les risques liés à de l'intrusion physique. L'ensemble des ports physiques (USB, RJ45, et autres) doivent être listés et placés sur un schéma. Il doit être possible notamment de :

- désactiver les ports de debug,
- limiter la possibilité de détourner le démarrage via un support amovible.

L'ETABLISSEMENT DE SANTE doit pouvoir placer sur les ports USB des bloqueurs physiques. Les ports USB doivent donc être accessibles physiquement pour l'établissement.

RÉSILIENCE

Mise en sécurité

Le dispositif médical doit pouvoir décrire un mode de « mise en sécurité » en cas d'attaque cybersécurité sur le réseau informatique garantissant la non mise en danger du patient. Les éléments suivants doivent être décrits dans la documentation du dispositif médical :

- modalités de mise en sécurité,
- fonctionnalités maintenues,
- modalités de remise en service,
- alertes et messages décrivant l'état de compromission du DM.

Mode dégradé

Le titulaire doit pouvoir décrire les modalités d'activation d'un mode dégradé en cas d'attaque cybersécurité sur le DM. Le mode dégradé est une situation où le DM doit pouvoir fonctionner malgré les impacts d'une cyberattaque. Ces modalités contiennent :

- le mode opératoire pour le faire fonctionner sans connexion réseau,

- le mode opératoire pour le faire fonctionner en cas de compromission d'un poste ou d'un serveur qui constitue le DM.

Les modes opératoires doivent tenir compte de l'écosystème dans lequel se trouve le DM.

Traitement des incidents de sécurité

Le titulaire s'engage à contacter les interlocuteurs sécurité de l'établissement désignés pour signaler tout incident de sécurité SI susceptible d'affecter les données ou le SI de l'établissement. Le titulaire dispose d'une procédure de gestion des incidents de sécurité formalisant les étapes de traitement et de résolution d'un incident. De plus :

- si cet incident a lieu sur le SI de l'établissement, un contact sécurité du titulaire est désigné et participe activement à la gestion de l'incident si l'équipement est impliqué ;
- si cet incident a lieu sur le SI du titulaire, un contact sécurité du titulaire est désigné et doit fournir régulièrement un état de la situation aux établissements concernés, à l'ANSM et au CERT-Santé. Le titulaire doit obligatoirement fournir une description des impacts éventuels sur le SI des établissements.

En outre, des réunions périodiques d'analyse post-incident devront être planifiées avec l'établissement (traitement des causes profondes)

Gestion de crise sécurité

Sur son domaine de responsabilité SI, le titulaire applique une procédure formalisée et opérationnelle de gestion de crise, apte à assurer le traitement d'événements remettant en cause de façon inacceptable pour l'établissement le respect des engagements de sécurité du DM. Ce plan précise au minimum :

- les principes d'escalade (critères de déclenchement, synoptique d'escalade),
- la composition de la cellule de crise : fonctions et responsabilités des membres (établissement et titulaire) — la liste nominative des membres et de leurs suppléants est référencée dans un annuaire,
- les moyens dédiés à la gestion de crise (salle(s) de crise, procédures opérationnelles, moyens de communication)

GESTION DES LICENCES

Gestion de la propriété intellectuelle

Le titulaire s'assure de l'acquisition de l'ensemble des licences ou des abonnements nécessaires et de la concession des droits d'usage à l'établissement dans le cadre du service (droits d'usage de matériels, de logiciels et/ou de couches logiques).

Le titulaire s'assure de la bonne validité des licences des logiciels qu'il met à disposition de l'établissement dans le cadre de la prestation, et ce durant toute la durée du marché. Par exemple, concernant les licences Windows, le titulaire s'engage à fournir des licences à jour ou à apporter la preuve qu'un contrat de support étendu qui court sur la période prévue de la prestation.

PROTECTION DES DONNÉES

Protection des secrets stockés

Les secrets stockés dans l'appareil (mots de passe, certificats électroniques, clés de chiffrement, etc.) doivent être protégés par des algorithmes de chiffrement sûrs et connus