



POUVOIR ADJUDICATEUR

FranceAgriMer

Adresse du siège : 12 rue Henri Rol-Tanguy - Montreuil sous Bois (93)

Adresse postale : FranceAgriMer -TSA 20002 -93555 Montreuil sous Bois cedex

ANNEXE 3 – Configuration poste de travail

FOURNITURE DE SERVICES D'ASSISTANCE INFORMATIQUE

REFERENCE INTERNE DU MARCHE : SI-U_PROD2026-CDS

1 LA PROTECTION DU BIOS

L'accès au BIOS est protégé par un mot de passe. Le démarrage sur le disque dur est l'unique option autorisée (pas de démarrage sur réseau ou périphériques amovibles).

2 LA PROTECTION ANTIVIRALE DU POSTE DE TRAVAIL

L'ANTIVIRUS BITDEFENDER ENDPOINT SECURITY TOOLS (BEST) EST INSTALLE SUR LE POSTE :

- L'agent Bitdefender permet la visibilité en temps réel du poste à partir de la console d'administration GravityZone.
- Permet de consulter les rapports détaillés d'analyses, de pousser des mises à jour, de déployer des agents à distance et de créer des tâches planifiées applicables en temps réel.
- Les mises à jour du contenu de sécurité sont automatiques : le serveur vérifie la disponibilité de nouvelles versions toutes les 2 heures auprès des serveurs Bitdefender.
- Une analyse antivirus rapide est planifiée tous les jours à 13h00.
- L'Advanced Threat Control (ATC) surveille l'activité des applications en continu pour bloquer les menaces avancées et les attaques zero-day.
- Le module Antimalware analyse les fichiers locaux et réseau, les secteurs de démarrage et les applications potentiellement indésirables (PUA) en temps réel.
- Le module Contrôle des appareils analyse et gère les supports connectés à l'ordinateur (clés USB, périphériques externes).
- La Protection du réseau sécurise les informations entrantes et sortantes via les protocoles web pour bloquer le phishing et les menaces en ligne.
- Le module Pare-feu (si activé) et la protection réseau recherchent dans le trafic toute trace d'activité caractéristique des attaques.
- Le Capteur d'incidents (EDR) et la Gestion des risques récoltent des données sur l'activité des applications et les vulnérabilités du poste pour offrir une protection proactive.
- Le Sandbox Analyzer permet d'analyser les fichiers suspects dans un environnement sécurisé avant exécution.
- La politique et la configuration de l'antivirus sont centralisées sur la console GravityZone via une stratégie de sécurité unique.
- Le poste bénéficie du service Managed Detection and Response. Une équipe d'experts Bitdefender (SOC) surveille à distance les alertes de sécurité 24h/24 pour identifier et bloquer les attaques.

LE LOGICIEL SQUIDGUARD

Le filtrage du trafic internet sur les postes clients est effectué par le logiciel Squid Guard.
Il assure la politique de filtrage et la partie proxy web classique.
L'authentification est obligatoire pour accéder à internet.

3 PARE-FEU WINDOWS ACTIVE SUR LES PC PORTABLES

Le pare-feu Windows est activé par GPO sur les pc portables de FranceAgriMer. Ces portables sont identifiés grâce au préfixe « PO » sur leur nom d'ordinateurs Windows. Ils sont ajoutés à un groupe de sécurité de l'Active Directory (GRP_GS_PORTABLES_FW) qui active le pare-feu et installe quelques règles.

4 LA MISE A JOUR DU POSTE

Au niveau système, le système est sous Windows 10 Entreprise. Les mises à jour sécurité sont assurées, initiées et suivies par le logiciel SCCM 2016.

Au niveau logiciel, les mises à jour sécurité des outils Microsoft (Office 2013, Outlook 2013,...) sont assurés, initiées et suivies par le logiciel SCCM 2016 via une tâche de déploiement automatisée.

Concernant les logiciels du socle bureautique (FireFox ESR, LibreOffice, Adobe Reader,...), un processus de déploiement est en place à partir de SCCM 2016 :

- Disponibilité du patch de sécurité et/ou du msi sur le site de l'éditeur.
- Préparation de la publication et de la distribution sur les DP (Points de Distribution)
- Validation du patch et/ou du msi avec le groupe de test (U_PROD, U_Etudes, Arborial) soit 30 postes
- Déploiement sur la totalité du parc

5 LA POLITIQUE DE GROUPES ACTIVE DIRECTORY

Un certain nombre de paramètres sont fixés par une politique centralisée au niveau de l'Active Directory.

Ils positionnent entre autres les niveaux de droit pour l'agent à savoir un niveau « d'utilisateur avancé » interdisant l'installation de logiciels et de connexion réseau comme la connexion Wi-Fi. L'utilisateur avancé ne peut pas modifier certains paramètres systèmes et entrées de registres nécessaires au bon fonctionnement du système.

Au niveau de l'accès à l'ordinateur, seul un compte FranceAgriMer est autorisé (pas de compte d'utilisateur local hormis le compte administrateur local) avec une politique de mots de passe.

L'activation des profils Windows garantit une confidentialité des données de l'agent en cas d'utilisation par plusieurs agents (un agent X ne peut par exemple pas accéder au répertoire « Mes Documents » d'un agent Y).

Au niveau du verrouillage du poste, celui-ci est activé de façon automatique au bout de 15 minutes d'inactivité.

6 : SOCLE LOGICIEL

Se référer à l'annexe 2 : Socle bureautique