SAUVEGARDE DES SYSTÈMES D'INFORMATION - Les fondamentaux

Ce document est une matrice de conformité en référence aux critères énoncés dans le document « Sauvegarde des systèmes d'information - Les fondamentaux » par l'ANSSI (ANSSI-BP-100 - Octobre 2023).

Taux de conformité de la solution Oxibox : **97%**

RAPPELS	Commentaires
Besoin d'une PDMA de moins de 24h ; dans ce cas, privilégier d'autres solutions telle que la réplication (synchrone ou asynchrone).	**Oxibox permet une PDMA inférieure à 24h.**
Les composants essentiels d'une infrastructure de sauvegarde sont : • le catalogue/index qui permet de savoir ce qui est sauvegardé • l'agent logiciel de sauvegarde présent sur les serveurs sauvegardés • le serveur de sauvegarde qui traite le flux de sauvegarde avant envoi sur un support • le support de sauvegarde : disques, bandes magnétiques, disque externe USB, etc.	
La stratégie de sauvegarde doit notamment définir les durées de rétention des sauvegardes. Cette stratégie précise la répartition à long terme : 15 jours de sauvegardes journalières, 1 an de sauvegardes mensuelles, 5 ans de sauvegardes annuelles par exemple.	**L'agent Oxibox (cross plateforme) s'installe sur les postes/serveurs à sauvegarder.**
L'opérateur de sauvegarde doit être considéré comme un administrateur à hauts privilèges sur le SI. Il faut donc être vigilant sur le niveau de confiance accordé à ces opérateurs et intégrer des clauses de sécurité spécifiques en cas de recours à de la sous-traitance.	**Oxibox possède son propre Plan d'Assurance Sécurité (PAS). Oxibox se conforme au PAS de son client dans le cadre d'une prestation en sous-traitance directe (B2B). Dans le cadre d'une relation en B2B2B, cette mise en conformité est du ressort de la relation entre le client et son sous-traitant direct.**

FONDAMENTAUX	Commentaires
Architecture	
Les serveurs de sauvegarde doivent être cloisonnés et positionnés au sein du SI d'administration, ou au moins dans une zone réseau distincte de la zone de production hébergeant les serveurs sauvegardés.	**Oxibox se conforme à l'architecture du client.**
Les flux de sauvegarde doivent transiter au sein du réseau d'administration.	**Oxibox se conforme au paramétrage du client.**
Les flux de sauvegarde doivent transiter au sein d'un sous-réseau logique dédié (VLAN).	**Oxibox se conforme au paramétrage du client.**
Il est recommandé de dédier une instance de serveur de sauvegarde et un magasin de données par niveau de sensibilité des données et/ou applications. Par exemple, les éléments suivants doivent disposer d'une instance de sauvegarde dédiée : > le SI d'administration ; > les systèmes stockant des secrets (ex. : annuaire, infrastructure de gestion de clés, coffre-fort) ; > les postes bureautiques, si ceux-ci doivent être sauvegardés.	**Oxibox se conforme au paramétrage du client qui peut dédier des serveurs de sauvegarde selon les différents niveaux de sensibilité de ses données.**
Les serveurs hébergeant l'infrastructure de sauvegarde ne doivent pas faire partie d'un domaine Windows (Active Directory) de production. Ils doivent disposer d'un système d'authentification indépendant (comptes locaux, annuaire dédié à l'administration)	**Oxibox possède son propre système d'authentification.**
Les flux de sauvegarde doivent être filtrés strictement au moyen d'un pare-feu interne.	**Oxibox a son propre système de filtres de flux de sauvegarde n'autorisant que les opérations licites auxquelles le client peut ajouter ses propres règles.**

✓	En particulier, les magasins de données ne doivent être accessibles que depuis les serveurs de sauvegarde.	**Les magasins de données des appliances ne sont accessibles que par les appliances.**
✓	Les flux de sauvegarde doivent être à l'initiative du serveur vers les clients sauvegardés.	**Les configurations des agents sont gérées par le serveur de sauvegarde, qui contrôle ainsi les flux de sauvegarde.**
✓	Si une infrastructure de sauvegarde est obsolète mais doit néanmoins être conservée, elle doit être maintenue hors ligne en condition de sécurité. L'éventuelle reconnexion de celle-ci en cas de besoin doit se faire depuis un réseau déconnecté ou cloisonné logiquement du reste du SI.	**Oxibox se conforme aux directives du client.**
✓	Les actions réalisées sur l'infrastructure de sauvegarde doivent être journalisées et centralisées sur un collecteur de journaux d'événements.	**Oxibox conforme grâce à ses journaux d'événements.**

Opérations

✓	Il est recommandé d'appliquer la règle « 3 – 2 – 1 » : 3 copies de la sauvegarde sur 2 supports différents dont 1 hors ligne.	**Déploiement possible avec ou sans appliance pour faciliter la mise en oeuvre du 3-2-1.**
✓	Il est indispensable de mettre en place une sauvegarde hors ligne (ou au moins hors site en ligne sous certaines conditions) même si celle-ci est moins fréquente que les sauvegardes locales régulières en ligne (cf. tableau 2 en section 3.5).	
✓	Les opérations de sauvegarde sont des opérations d'administration, elles doivent donc respecter les bonnes pratiques du guide d'administration sécurisée de l'ANSSI.	
✓	Chaque instance de sauvegarde doit disposer de comptes d'administrateurs dédiés.	
✓	Les comptes d'administrateurs pour la sauvegarde doivent être nominatifs et dédiés.	**Les comptes des agents Oxibox sont dédiés et nominatifs**
NC*	En fonction des capacités du logiciel, il est recommandé de segmenter les rôles des opérateurs de sauvegarde en définissant au minimum un rôle d'exploitation (actions quotidiennes) et un rôle d'administration avancée (stratégie, configuration).	**La solution Oxibox permet une segmentation partielle des droits, avec une segmentation complète prévue pour Q2 2024.**
✓	Les comptes techniques de sauvegarde (qui exécutent les agents logiciels notamment) doivent faire l'objet d'une sécurisation : réduction des privilèges système au strict minimum, renouvellement des secrets régulier et si possible automatisé.	**La solution permet à l'utilisateur de réduire les privilèges systèmes des comptes techniques de sauvegarde et de journaliser les actions.**
✓	Il n'est pas recommandé d'autoriser les utilisateurs à exécuter directement une action de sauvegarde ou de restauration sur le SI (fonction parfois proposée par certains éditeurs de logiciels). Cela fait encourir un risque d'accès illégitime à des données et un risque d'élévation de privilèges sur le SI. Si ce besoin existe, il est recommandé de cadrer strictement cet emploi (limiter les utilisateurs autorisés) et de journaliser ces actions.	**Oxibox cadre ses actions et journalise ses actions.**
✓	Il est recommandé de s'assurer que la « restauration croisée » est désactivée par défaut sur le logiciel de sauvegarde.	**Oxibox n'autorise pas les restaurations croisées.**
✓	L'ensemble des composants de l'infrastructure de sauvegarde doit être mis à jour de manière proactive (logiciel de sauvegarde, micrologiciels, etc.). Il est recommandé de suivre les CVE et les bulletins d'alertes fournis par l'éditeur de la solution.	**Oxibox est son propre éditeur de la solution et assure la maintenance de sa solution.**
✓	La sauvegarde doit systématiquement faire l'objet d'un contrôle par les opérateurs de sauvegarde. : Ce contrôle doit inclure une liste de vérifications permettant de détecter un comportement inhabituel : volume de données ou de fichiers incohérent, lenteurs réseaux, modifications de la configuration des politiques de sauvegarde, etc.	**Notifications (emails de rapport récurrents) et journal de sauvegarde généré à chaque sauvegarde et disponible aux administrateurs**
✓	Les sauvegardes doivent être testées régulièrement. Une procédure de restauration du SI doit être rédigée et régulièrement mise en œuvre.	**À travers les fonctionnalités de l'outil Oxirescue ainsi qu'une vérification régulière de l'intégrité des sauvegardes.**
✓	Une stratégie et un ordre de restauration doivent être définis en tenant notamment compte des critères suivants : dépendance du SI vis-à-vis de services d'infrastructure (DNS, NTP, annuaire, etc.), criticité des applications métier, durée de restauration et de resynchronisation des données, mode de restauration (machines virtuelles, BMR, etc.).	**Oxibox a son propre système de filtres de flux de sauvegarde n'autorisant que les opérations licites auxquelles le client peut ajouter ses propres règles.**

* Non-conforme

✓	En cas d'incident de sécurité, la mesure prioritaire doit être d'isoler l'infrastructure de sauvegarde du reste du SI. Cela suppose de prévoir un mode « bouton rouge » d'urgence (ex. : script automatisé, déconnexion d'un commutateur).	**Les magasins de données des appliances ne sont accessibles que par les appliances.**
✓	Il est important de sauvegarder les médias d'installation et les configurations des applications métier.	**Les configurations des agents sont gérées par le serveur de sauvegarde, qui contrôle ainsi les flux de sauvegarde.**
✓	La sauvegarde de l'infrastructure de sauvegarde doit être prise en compte. Elle doit contenir au moins : les binaires pour installer une infrastructure minimaliste (systèmes d'exploitation, logiciels et leurs correctifs), les procédures d'import des sauvegardes, le catalogue de sauvegarde, la liste du matériel pour un déploiement sur un site de secours et, si les données sont chiffrées par le logiciel de sauvegarde, les procédures d'import des clés de chiffrement.	**Oxibox se conforme aux directives du client.**
✓	En cas de restauration après un incident de sécurité, les sauvegardes peuvent contenir des implants de l'attaquant (ex. : code malveillant, porte dérobée). Il faut tenir compte de ce risque lors de la reconstruction du SI, et s'assurer de l'innocuité des éléments restaurés en opérant de manière granulaire dans la mesure du possible : > réinstaller les systèmes d'exploitation à partir d'images officielles de confiance ; > réinstaller les applications métier à partir de binaires signés par les éditeurs ; > réaliser un contrôle de conformité des configurations des applications avant leur redémarrage > réaliser un scan antivirus des données métier avant leur importation dans l'application ; > disposer d'un historique de sauvegardes cohérent par rapport aux valeurs métier.	**La solution Oxibox est conforme grâce à ses journaux d'événements.**

Protection des données

✓	Les flux de sauvegarde doivent être protégés au moyen de chiffrement et d'authentification mutuelle entre client et serveur à l'état de l'art (avec TLS par exemple).	
✓	Le niveau de robustesse de la protection des sauvegardes (chiffrement, etc.) doit être aligné avec le niveau de protection de ces mêmes données dans le SI de production. Si les sauvegardes sont chiffrées, la gestion des clés de chiffrement doit être étudiée : les opérateurs qui les détiennent, leur stockage (coffre-fort), leur sauvegarde (hors ligne).	**Les sauvegardes sont systématiquement chiffrées à la source en AES-256 quelle que soit la source.**
✓	Dans le cas où la sécurité physique d'un site de sauvegarde n'est pas jugée satisfaisante, il est important de chiffrer systématiquement les sauvegardes (disques, bandes magnétiques, etc.).	**Mécanisme asymétrique de dérivation de la clef de chiffrement.** **Oxibox chiffre à la source toutes les données sauvegardées.**
✓	Lors de la mise au rebut des supports de sauvegarde, il est important de réaliser au préalable un effacement sécurisé (suppression des clés de chiffrement des sauvegardes, mise à zéro ou zeroisation en anglais) ou de détruire physiquement les supports (déchiquetage ou incinération).	**Oxibox propose cette option à tous nos clients lors de la mise au rebut des supports de sauvegarde.**

Virtualisation

✓	Dans le cas de la virtualisation, il est recommandé d'étudier la pertinence de sauvegarder directement l'image disque d'une machine virtuelle ou d'installer l'agent de sauvegarde sur la machine virtuelle. Cette étude doit tenir compte des critères suivants : > le volume de données modifiées sur la machine virtuelle à chaque sauvegarde ; > les besoins en granularité dans le processus de restauration ; > le chiffrement ou non de la machine virtuelle (selon les outils, cela peut nécessiter un déchiffrement et re-chiffrement, exposant ainsi des données en clair) ; > la capacité à reconstruire la machine virtuelle à partir de zéro (automatisation)	**La solution Oxibox propose les deux approches.**

Externalisation

✓	Une solution de sauvegarde hors ligne reste considérée comme plus robuste qu'une solution WORM en ligne. Néanmoins, un compromis acceptable peut être d'effectuer des sauvegardes régulières avec une solution WORM et d'effectuer des sauvegardes hors ligne à une fréquence moindre.	**La solution Oxibox est à mi-chemin entre le stockage WORM en ligne et une sauvegarde déconnectée grâce à notre technologie Data Protection.**