RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

RECOMMANDATIONS RELATIVES AU RECONDITIONNEMENT DES ORDINATEURS DE BUREAU OU PORTABLES

GUIDE ANSSI

ANSSI-PA-097
30/06/2023

PUBLIC VISÉ :

Développeur | **Administrateur** | **RSSI** | **DSI** | Utilisateur

Informations

Attention

Ce document rédigé par l'ANSSI présente les **« Recommandations relatives au reconditionnement des ordinateurs de bureau ou portables »**. Il est téléchargeable sur le site www.ssi.gouv.fr.

Il constitue une production originale de l'ANSSI placée sous le régime de la « Licence Ouverte v2.0 » publiée par la mission Etalab [18].

Conformément à la Licence Ouverte v2.0, le guide peut être réutilisé librement, sous réserve de mentionner sa paternité (source et date de la dernière mise à jour). La réutilisation s'entend du droit de communiquer, diffuser, redistribuer, publier, transmettre, reproduire, copier, adapter, modifier, extraire, transformer et exploiter, y compris à des fins commerciales.

Sauf disposition réglementaire contraire, ces recommandations n'ont pas de caractère normatif ; elles sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	30/06/2023	Version initiale

Table des matières

1
Introduction

1.1 Objectifs du guide

Ce guide s'inscrit dans le cadre de mise en œuvre de la loi anti-gaspillage pour une économie circulaire (dite loi AGEC) du 10 février 2020 [7] qui a notamment pour objectif de limiter la pollution en mettant le réemploi au cœur de la commande publique.

À ce titre, les acheteurs de l'État, des collectivités locales et de leurs groupements sont tenus d'acquérir des biens issus du réemploi, de la réutilisation de matériel ou comportant des matières recyclées [1]. L'article 58 II précise par ailleurs que les proportions d'ordinateurs portables et fixes devant être réemployés sont fixées à 20% et que cette obligation s'apprécie sur le volume annuel total de la dépense hors taxes des matériels et non par unité. Enfin, il prévoit qu'en *cas de contrainte opérationnelle liée à la défense nationale ou de contrainte technique significative liée à la nature de la commande publique, le pouvoir adjudicateur n'est pas soumis à cette obligation*.

Ce guide s'adresse aux différentes entités de l'État concernées par la loi AGEC ainsi qu'aux entités à la recherche de recommandations de sécurité concernant :

- l'acquisition et l'usage d'ordinateurs de bureau ou portables reconditionnés ;
- la cession d'ordinateurs de bureau ou portables.

L'objectif de ce guide est d'apporter les bonnes pratiques pour réduire les risques de compromission ou de propagation de codes malveillants liés à l'usage d'ordinateurs reconditionnés nouvellement acquis ainsi que les risques de fuite d'information lors de la cession d'ordinateurs à une autre entité. Les recommandations proposées traitent des menaces connues au moment de la rédaction du document.

Attention

L'utilisation d'ordinateurs reconditionnés pour traiter des données classifiées de défense « SECRET, TRES SECRET » est interdite.

1. Les produits intégrant des matières recyclées sont à considérer comme tels, quelle que soit la part de matières recyclées qu'ils contiennent [10].

1.2 Conventions de lecture

Pour chacune des recommandations de ce guide, l'utilisation du verbe *devoir* signifie que la recommandation est directement liée à une mesure de sécurité issue de la réglementation (loi AGEC et IGI 1300). La formulation *il est recommandé* est utilisée pour tout ce qui relève des bonnes pratiques et complète la réglementation.

Pour certaines recommandations, il est proposé, au vu des menaces constatées lors de la rédaction de ce guide, plusieurs solutions qui se distinguent par le niveau de sécurité qu'elles permettent d'atteindre. Le lecteur a ainsi la possibilité de choisir une solution offrant la meilleure protection en fonction du contexte et de ses objectifs de sécurité.

Ainsi, les recommandations sont présentées de la manière suivante :

R

Recommandation à l'état de l'art

Cette recommandation permet de mettre en œuvre un niveau de sécurité à l'état de l'art.

R -

Recommandation alternative de premier niveau

Cette recommandation permet de mettre en œuvre une première alternative, d'un niveau de sécurité moindre que la recommandation R.

R --

Recommandation alternative de second niveau

Cette recommandation permet de mettre en œuvre une seconde alternative, d'un niveau de sécurité moindre que les recommandations R et R -.

R +

Recommandation renforcée

Cette recommandation permet de mettre en œuvre un niveau de sécurité renforcé. Elle est destinée aux entités qui sont matures en sécurité des systèmes d'information.

Dans une démarche permanente de gestion du risque numérique et d'amélioration continue de la sécurité des systèmes d'information [2], la pertinence de mise en œuvre des recommandations décrites dans ce document doit être périodiquement réévaluée.

La liste récapitulative des recommandations est disponible en page 25.

2. Se reporter au guide ANSSI relatif à la maîtrise du risque numérique [15].

1.3 Liste des sigles et acronymes

- **Firmware** : nom générique désignant tout logiciel embarqué dans un composant matériel de l'ordinateur (BIOS, UEFI, carte réseau, carte graphique, etc.).
- **IOMMU** : *Input/Output Memory Management Unit*. Composant matériel permettant de filtrer les accès à la mémoire centrale depuis les périphériques.
- **Ordinateur reconditionné** : ordinateur de bureau ou ordinateur portable tels que mentionnés dans la loi AGEC.
- **OEM** : *Original Equipment Manufacturer*. Fabricant d'équipements d'origine. Désigne toute entreprise fabriquant des matériels ou tout éditeur développant des logiciels.
- **PSSI** : Politique de Sécurité des Systèmes d'Information. Ensemble formalisé des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du (des) système(s) d'information de l'entité.
- **Reconditionneur** : désigne un service en charge d'appliquer des procédures de remise en état d'un ordinateur de bureau ou portable. Il peut s'agir soit d'un prestataire de reconditonnement, soit d'un OEM, soit de l'entité elle-même.
- **TPM** : *Trusted Platform Module*. Composant passif spécifié par le *Trusted Computing Group* (TCG) fournissant des services de mesures d'intégrité et de scellement cryptographique.
- **USB** : *Universal Serial Bus*. Norme de bus informatique en transmission série permettant de connecter et d'alimenter des périphériques à chaud et en bénéficiant du Plug and Play.
- **Utilisateur** : la personne utilisant le poste informatique au quotidien, sans privilège particulier.
- **Vulnérabilité critique** : vulnérabilité dont le score CVSS (*Common Vulnerability Scoring System*) est compris entre 7 et 10 (aussi marquée *high*). Si une vulnérabilité n'a pas de score CVSS, elle est par défaut considérée comme ayant une criticité élevée, et l'éventuel abaissement de cette criticité ne peut être envisagé qu'à l'issue d'un échange entre l'éditeur et l'entité.

2
Recommandations concernant le déploiement d'ordinateurs reconditionnés

L'entité peut acquérir des ordinateurs de bureau ou portables reconditionnés de différentes manières :

1. en s'appuyant sur un prestataire de reconditionnement
2. en s'adressant directement aux équipementiers d'origine (OEM) ;
3. en reconditionnant elle-même des ordinateurs d'occasion.

Information

La capacité de réinitialisation des matériels dans un état dit « sortie d'usine » d'un OEM est supérieure à n'importe quel autre acteur de reconditionnement, qu'il soit externe ou interne. (p. ex. HP, Dell).

Dans ce guide, le terme *reconditionneur* désigne indifféremment un prestaire de reconditionnement, un OEM ou un service interne de l'entité en charge du reconditionnement des matériels. Dans ce dernier cas, il appartient à l'entité d'adapter les recommandations du présent guide à son processus interne de reconditionnement.

Les sections ci-dessous détaillent tout d'abord les risques induits par le recours à des matériels reconditonnés. Elles proposent ensuite des recommandations pour organiser le déploiements des ordinateurs reconditionnés et enfin des recommandations pour la réalisation technique de reconditionnement. Si l'entité ne dispose pas en interne des compétences nécessaires à la réalisation du reconditionnement, il est recommandé qu'elle s'appuie sur les services d'un ou plusieurs prestataires externes en charge de ces actions (OEM ou prestataire de reconditionnement). Dans cette hypothèse, l'entité doit s'assurer que le ou les reconditionneurs externes mettent en œuvre les recommandations de ce guide. Le recours à un reconditionneur externe ajoute nécessairement des risques supplémentaires à ceux pesant sur la chaîne d'approvisionnement (*supply chain*). Ces risques sont inhérents aux pratiques et au système d'information utilisé par le prestataire. D'autre part, la compromission de ce prestataire aura nécessairement un impact sur l'ensemble de ses clients, dont l'entité qui sous-traite le reconditionnement de ces ordinateurs.

2.1 Comprendre les risques

Si l'usage d'ordinateurs reconditionnés contribue pleinement aux objectifs écologiques et environnementaux, tels que rappelés dans la loi AGEC, il introduit un certain nombre de risques pour le patrimoine applicatif et informationnel de l'entité, qu'il convient d'appréhender et traiter. En effet, l'historique des possesseurs ou des éventuelles compromissions passées de ces différents matériels ne sont pas connus. Par ailleurs, il est important de garder à l'esprit que certaines techniques d'attaque avancées permettent à des implants de persister sur les machines après la réinstallation du système d'exploitation. Ces types d'implants seront toujours actifs et permettront à l'attaquant de poursuivre son activité malveillante ; le processus de reconditionnement, tel que décrit dans ce guide, ne permettra pas de détecter l'ensemble de ces attaques. Les méthodes de persistance suivantes sont à prendre en compte dans l'analyse de risques. Celles-ci sont classées de la moins sophistiquée, et donc la plus facile à traiter, à la plus sophistiquée et la plus difficile à traiter :

- **Persistance via un code malveillant écrit sur le disque**. Cette méthode de persistance est la plus classique, et l'effacement du disque puis la réinstallation du système à partir d'un support sain protègera de ce risque.
- **Persistance via le piégeage du matériel**. Des pièces peuvent être changées ou ajoutées pour ajouter un implant physique dans la machine. L'objectif est typiquement de permettre une exfiltration de données soit directe (captation de son par microphone caché ou actif en continu, captation de vidéos et d'images par une webcam supposée éteinte), soit indirecte par canal auxiliaire (exploitant le son émis par un disque dur ou des ventilateurs, des émissions électromagnétiques, ou fuite d'information au moyen d'un câble USB intégrant une antenne radiofréquence [3]). Ces techniques sont notamment utilisées pour le piégage d'ordinateurs ayant vocation à être déployés dans des systèmes d'informations isolés. Cette attaque nécessite un accès physique à la machine, ce qui est grandement facilité pour un attaquant dans le contexte d'un ordinateur reconditionné, ou de pouvoir compromettre en amont les pièces de rechange du prestataire de reconditionnement. Cette technique d'attaque échappera aux contrôles du prestataire si elle est faite correctement.
- **Persistance via un piégeage des bus et ports de communication avec des périphériques internes ou externes extérieurs**. En particulier, les connecteurs USB sont le vecteur de nombreuses attaques inhérentes au protocole de communication sous-jacent où chaque périphérique se présente à la connexion et peut donc usurper la description proposée. Parmi les vecteurs d'attaques identifiés affectant l'ordinateur reconditionné, il existe la reprogrammation du microcontrôleur interne ou du *firmware* du périphérique. L'objectif consiste ici à émuler un clavier et ainsi injecter à la volée des commandes permettant l'exfiltration de données ou l'exécution silencieuse de maliciels [4]. Le problème s'étend également aux chargeurs des ordinateurs portables et par extension aux *docking station* pour lesquels le format USB Type-C [5] a vocation à devenir un standard de fait. Là encore, des cas concrets [6] exploitant une reprogrammation du microcontrôleur interne des chargeurs et des câbles USB modifiés ont été observés. Ils démontrent la faisabilité et la dangerosité de ce type de compromission.

3. Attaque USBee de type « air-gap »
4. Attaques de type *Rubber Ducky, PHUKD/URFUKED* ou encore *Avilduino*, etc.
5. comme c'est déjà le cas pour les ordiphones de par la directive de la Commission Européenne d'avril 2022 qui impose un port de recharge USB Type-C à partir de 2024.[4]
6. Attaques de type *USBHarpoon, O.MG cable ou USBNinja*

- **Persistance via réécriture du *firmware* en particulier pour l'UEFI (*Unified Extensible Firmware Interface*).** Cette attaque est beaucoup plus avancée. Toutefois, certaines attaques de cette nature ont déjà été observées tel que le rootkit UEFI LoJax [6]. Ces méthodes de persistance sont difficilement détectables et échapperont probablement au reconditionneur. Cette méthode survit à la réinstallation du système d'exploitation et au remplacement du disque [7].

Les attaques citées précédemment peuvent être réalisées par tous les acteurs ayant soit un accès physique à l'équipement au cours de son cycle de vie, soit de manière distante après avoir pris le contrôle de l'ordinateur. Dans le cadre d'une commande publique d'ordinateurs reconditionnés, ceux-ci peuvent être facilement repérables par un acteur malveillant et à ce titre constituer une cible privilégiée pour mener une attaque ciblée.

Les recommandations et exigences proposées dans la suite de ce guide visent à réduire autant que possible les risques liés notamment aux menaces présentées. Certaines d'entre elles ne pouvant pas être totalement traitées, des risques résiduels persisteront.

2.2 Organiser le déploiement des ordinateurs reconditionnés

En premier lieu, il convient que l'entité mène une réflexion sur la manière d'intégrer des ordinateurs reconditionnés au sein de son système d'information. Cette étude doit porter non seulement sur les aspects techniques et de cybersécurité, mais également sur l'organisation et les processus qui permettent cette pratique.

Cette étude doit s'appuyer sur l'analyse de risques du système d'information de l'entité, dans laquelle doit être traitée plus spécifiquement la problématique d'intégration d'ordinateurs reconditionnés. Celle-ci doit permettre aux décideurs de prendre conscience des principaux risques, d'accepter les risques résiduels et d'orienter les services en charge de la mise en œuvre.

R1

Gérer les risques résiduels

L'analyse de risques doit intégrer les ordinateurs reconditionnés et mentionner les risques résiduels. Ces derniers doivent apparaitre dans l'homologation [8] du système utilisant les ordinateurs reconditionnés.

Cette analyse de risques doit conduire à l'élaboration de la stratégie de l'entité sur l'acquisition et le déploiement d'ordinateurs reconditionnés. Celle-ci doit décrire les principes de cette pratique pour l'entité, les usages et les modalités de mises en œuvre.

7. Il faut noter qu'une partie de la chaîne de démarrage UEFI, liée au chargeur de démarrage, est stockée sur le disque. Les attaques qui visent ces éléments, par exemple le malware BlackLotus, sont à classer dans la catégorie « malware écrit sur disque » bien qu'ils soient également rapportés dans la presse sous le terme ambigu d'attaque UEFI.

8. Se reporter au guide ANSSI relatif à l'homologation en 9 étapes [14]

R2

Élaborer une stratégie d'utilisation des ordinateurs reconditionnés

Au même titre qu'il existe une stratégie d'utilisation des ordinateurs au sein d'une entité, il est nécessaire d'en définir une pour les ordinateurs reconditionnés. L'entité peut prendre en compte plusieurs critères dans sa stratégie : introduction de machines de seconde main dans son parc, réutilisation des ordinateurs en interne en les reventilants d'une unité à l'autre, prolongation de la durée de vie des machines, etc. et réaliser une analyse de risques.

Un facteur dimensionnant en matière de gestion d'un système d'information est l'hétérogénéité du parc d'ordinateurs qui le constitue. Plus le parc est hétérogène, plus il est difficile de le maintenir en conditions opérationnelles (MCO), mais aussi de sécurité (MCS). Il est rare que les reconditionneurs disposent de lots de plusieurs milliers de machines identiques. Pour obtenir la quantité d'ordinateurs reconditionnés répondant à ses besoins, une entité aux besoins conséquents pourrait donc être amenée à introduire des machines provenant de multiples constructeurs dans son parc informatique. Cette pratique entraine une hétérogénéité du parc qui augmente d'autant les sources de risques. Cette complexification engendre également des coûts supplémentaires.

R3

Réduire au mieux le nombre de modèles différents déployés dans le parc informatique

Il est recommandé de réduire autant que possible le nombre de modèles d'ordinateurs constituant le parc informatique (qu'ils soient reconditionnés ou neufs) afin de simplifier les opérations de MCO et de MCS. Notamment, des machines ayant le même rôle et les mêmes exigences de configuration devraient être du même modèle.

D'une manière générale, il convient de veiller à ce que le déploiement d'ordinateurs reconditionnés n'abaisse pas le niveau de sécurité général du système d'information.

R4

Ne pas affaiblir le niveau de sécurité global du SI par l'utilisation d'ordinateurs reconditionnés

L'usage d'ordinateurs reconditionnés ne doit pas nuire aux intérêts essentiels de l'entité en particulier et plus globalement à la défense nationale. Il est notamment bon de garder à l'esprit que l'article 58 II de la loi AGEC prévoit qu'en *cas de contrainte opérationnelle liée à la défense nationale ou de contrainte technique significative liée à la nature de la commande publique, le pouvoir adjudicateur n'est pas soumis à cette obligation* [10].

Il se peut, enfin, que l'ordinateur reconditionné ne dispose pas de toutes les fonctions permettant d'être conforme à la politique de sécurité de l'entité qui souhaite les acquérir (p. ex. absence de lecteur de carte à puce intégré) ou que son ancienneté ne lui permette pas de disposer des dernières fonctionnalités matérielles et de sécurité attendues. Le choix d'utiliser un ordinateur reconditionné ne doit pas se faire au détriment de l'homogénéité et de la cohérence de la sécurité du système d'information. Une bonne pratique consiste à regrouper ces ordinateurs par service ou fonctions métiers afin de réduire le risque à des périmètres bien identifiés.

R5

Restreindre les cas d'usages d'ordinateurs reconditionnés

La priorisation d'attribution des ordinateurs reconditionnés dépend de la sensibilité des données qui y seront traitées et celle-ci est laissée à l'appréciation de l'entitée. Cependant, l'utilisation d'ordinateurs reconditionnés est déconseillée pour traiter des informations sensibles ayant notamment un impact opérationnel, juridique, ou budgétaire inacceptables pour l'entité. Il est également déconseillé d'utiliser un ordinateur reconditionné en tant que poste d'administration.

Dans cet esprit, l'entité doit préciser les modalités d'utilisation des ordinateurs reconditionnés avant qu'ils ne soient concrètement mis en production. Préciser ces modalités est d'autant plus important que les actions de préparation des ordinateurs reconditionnés n'auront peut-être pas été réalisées par l'entité, mais éventuellement confiées à un reconditionneur externe (prestataire en reconditionnement ou OEM).

L'entité doit privilégier une utilisation des ordinateurs reconditionnés pour les cas d'usage les moins risqués. Par exemple :

- données et zones les moins sensibles ;
- projets de moindre sensibilité ;
- usage dédié à des formations ;
- ordinateurs de prêts.

La procédure de reconditionnement est contrôlable sur pièce et sur site directement par l'entité acheteuse ou une autorité à qui elle délègue les opérations d'audit et ce durant la totalité du marché conclu. En pratique, une vérification initiale de la procédure appliquée, couplée à un échantillonnage aléatoire, est conseillée afin de réduire les risques résiduels tout en s'assurant que le reconditionneur se conforme bien aux recommandations de sécurité présentées dans ce guide. Dans le cas du recours au service d'un reconditionneur tiers, il est recommandé d'ajouter une clause d'audit aux exigences du marché.

R6

Élaborer et auditer la procédure de reconditionnement

Les processus et procédures de reconditionnement doivent être formalisés et régulièrement audités. Cette pratique vise à s'assurer du maintien des objectifs de sécurité tels que définis par l'entité au travers de son analyse de risques.

Les attaques sur la chaine d'approvisonnement (*supply chain attack*) sont un risque avéré et le reconditionneur doit également mettre en place des mesures organisationnelles afin de prendre en compte ces risques.

R7

Signaler tout manquement ou irrégularité lors de la procédure de reconditionnement

Le reconditionneur doit signaler tout comportement suspect ou ordinateur compromis découvert lors de la procédure de reconditionnement aux autorités compétentes (voir la page web « en cas d'incident » sur le site de l'ANSSI [1]) et retirer ce lot de

son catalogue.

L'ordinateur reconditionné ayant par définition déjà servi, il convient d'exiger notamment, de la part du reconditionneur, que le matériel soit sous garantie, qu'il soit compatible aux versions à jour des *firmwares* et des systèmes d'exploitation.

R8

S'assurer que l'ordinateur reconditionné acquis est sous garantie

L'entité s'assure que l'ordinateur reconditionné est garanti au moins un an, pièces et main d'œuvre.

Le reconditionneur doit obtenir la liste des versions des systèmes d'exploitation compatibles par lot d'ordinateurs reconditionnés et doit en garantir le bon fonctionnement sur ces matériels. Au minimum, les dernières versions du système d'exploitation (i.e. celles supportées par l'éditeur du système d'exploitation) doivent être compatibles avec l'ordinateur reconditionné.

Pour les systèmes d'exploitation, il est recommandé que l'entité consulte le site de l'éditeur et regarde les spécifications requises pour la dernière version supportée disponible. Par exemple Windows 11 requiert actuellement les spécifications détaillées sur le site web de Microsoft [8]. Ces spécifications ne sont qu'un minimum pour Windows 11 et il est pertinent d'en définir de plus élevées afin d'anticiper les besoins d'une version future et de garder son matériel quelques années.

R9

Établir la liste des systèmes d'exploitation compatibles avec l'ordinateur et garantir leur bon fonctionnement

L'entité doit disposer de la liste des systèmes d'exploitation compatibles avec les matériels reconditionnés afin de s'assurer de pouvoir les déployer conformément à sa politique de sécurité interne.

L'ordinateur reconditionné ne doit pas affaiblir le niveau de sécurité global du parc informatique en introduisant de plus vieux matériels ou systèmes d'exploitation que ceux présents ou en privant l'entité de mécanismes de sécurité proposés par les équimentiers ou les éditeurs de ces systèmes d'exploitation (p. ex. *kernel DMA protection, Virtualization Based Security*).

R10

S'assurer des garanties offertes par l'OEM pour les mises à jour de firmwares

L'entité doit s'assurer auprès du prestataire de reconditionnement ou de l'OEM que les *firmwares* présents sur la machine continueront à faire l'objet de mises à jour de sécurité pendant au moins 2 ans. Les mises à jour doivent être fournies via un processus standard et permettant leur déploiement automatisé (p. ex. *Windows Server Update Services* ou *Linux Vendor Firmware Service*). Elles doivent également provenir directement de l'OEM et être signées par ce dernier. L'entité doit s'assurer de la validité des signatures des mises à jour avant leur application.

R11

Choisir des ordinateurs avec des fonctionnalités de sécurité équivalentes au matériel neuf

Les machines issues du reconditionnement ne doivent pas affaiblir le niveau de sécurité du SI. À ce titre, les fonctionnalités de sécurité attendues pour les ordinateurs reconditionnés doivent être identiques à celles qui seraient exigées pour l'acquisition de matériels neufs. Ces fonctionnalités doivent être précisées dans le marché de reconditionnement. Voici une liste non exhaustive de points pouvant être pris en considération :

- une unité de gestion des entrées/sorties de la mémoire (IOMMU) doit être présente ;
- un TPM v2.0 certifié EAL4+ (au sens des critères communs) suivant le profil « TCG Protection Profile PC Client Specific TPM family 2.0 » doit être présent ;
- la séquence de démarrage et le choix du périphérique de démarrage doivent pouvoir être protégés par mot de passe ;
- l'accès en modification aux paramètres du *firmware* doit pouvoir être protégé par un mot de passe ;
- les modules de *firmware* susceptibles de modifier le comportement du système d'exploitation ou l'intégrité des données (par exemple, les services résidents de protection contre le vol proposés par les OEM ou des vendeurs indépendants tels que Absolute) sont soit absents du *firmware*, soit désactivés par défaut ;
- toutes les clés *UEFI Secure Boot* doivent pouvoir être changeables par l'autorité qualifiée (PK, KEK, db, dbx) ;
- l'intégrité du *firmware* doit être protégée contre les modifications malveillantes ;
- les interfaces et ports de communication doivent pouvoir être désactivés dans l'interface de configuration du *firmware* ;
- l'ordinateur reconditionné doit supporter la virtualisation (VT-d, AMD-v) et la traduction d'adresses de second niveau (« *Second Level Address Translation* »).

Les fonctions de sécurité listées dans la recommandation R11 doivent pouvoir être configurées par les équipes dédiées de l'entité (et non par l'utilisateur). Les fonctions de sécurité ou sur lesquelles se basent des fonctions de sécurité doivent être activées par défaut.

Dans la logique de restreindre les ordinateurs reconditionnés à des usages précis, il est nécessaire de disposer d'une traçabilité de tous les ordinateurs reconditionnés déployés au sein du système d'information. L'objectif de cette mesure vise à les distinguer du reste du parc et à s'assurer qu'ils sont déployés dans le respect de la stratégie définie par l'entité. Leur suivi doit permettre notamment de s'assurer qu'aucun usage sensible ne viendra en être fait tout au long de leur cycle de vie au sein de l'entité, de cartographier les usages et métiers concernés, et d'intervenir lorsqu'une vulnérabilité est identifiée sur ces matériels.

R12

Inventorier et assurer le suivi des ordinateurs reconditionnés

Afin d'assurer la cohérence des usages des ordinateurs reconditionnés, il est recommandé de procéder à leur recensement et leur traçabilité. Comme pour le marquage des matériels sensibles ou classifiés (même si la finalité est différente), une bonne pratique est de marquer les ordinateurs reconditionnés et de sensibiliser les équipes d'exploitation et les utilisateurs finaux à son usage.

À l'instar de ce qui devrait être fait pour le parc informatique neuf, le reconditionneur doit mettre en place une veille informationnelle concernant les alertes de sécurité et bulletin de vulnérabilité des constructeurs sur lesquels il s'appuie pour les matériels reconditionnés (p. ex. mise à jour critique de *firmware*, perte de confiance dans le système de mise à jour, divulgation de clé de signature de mise à jour BIOS, etc.) ainsi que sur les modes opératoires des attaques logicielles et matérielles. Cette mesure vise à pouvoir réagir de manière adaptée, en particulier si une vulnérabilité critique était identifiée.

R13

Réaliser une veille informationnelle de sécurité

Le reconditionneur doit mettre en place une procédure de veille informationnelle des alertes de sécurité et bulletins de vulnérabilité pour les matériels des ordinateurs reconditionnés. Si ce type de veille cybersécurité est déjà mise en œuvre, il convient alors d'y ajouter les références constructeur des ordinateurs reconditonnés utilisés par l'entité.

En complément de cette mesure, il convient également de prévoir des procédures de gestion des incidents de sécurité adaptées aux matériels reconditionnés. Si les autorités notifient le reconditionneur à propos d'une compromission, faille, divulgation de clefs de mise à jour de *firmware*, etc., celui-ci doit s'engager à traiter l'incident, voire à retirer les modèles concernés du marché dans les plus brefs délais. Réciproquement, en cas de découverte d'une compromission affectant ses ordinateurs reconditionnés, il est recommandé que l'entité informe les autorités et son reconditionneur, afin qu'ils puissent gérer l'incident avec les potentiels autres clients de ces matériels.

R14

Établir une procédure de gestion des incidents de sécurité

Des procédures de gestion des incidents de sécurité doivent être prévues, soit pour traiter des incidents notifiés par les autorités, soit pour alerter d'un incident de sécurité découvert par l'entité.

2.3 Préparer techniquement le reconditionnement

Bien qu'il soit difficile d'éliminer les risques liés à l'usage d'ordinateurs reconditionnés, il est conseillé de suivre certains processus afin de les réduire et de les encadrer.

Par principe, le matériel destiné à être reconditionné doit être contrôlé et tout composant physique qui aura été ajouté à l'ordinateur avant son reconditionnement doit être retiré. Si le reconditionneur est en mesure d'effectuer des tests supplémentaires sur l'ordinateur, il est recommandé de les lui faire effectuer.

R15

Retirer tout matériel additionnel indésirable

L'ordinateur doit être inspecté par le reconditionneur et les supports de type carte SIM ou mémoire externe (cartes SD, etc.) doivent être retirés. Tout matériel qui n'est pas d'origine ayant été ajouté au poste avant son reconditonnement doit également être enlevé (p. ex. adaptateur wifi, etc.).

Ensuite, les ordinateurs doivent être réinitialisés puis effacés afin d'éviter que des charges malveillantes ne puissent s'exécuter sur le SI de l'entité.

R16

Réinitialiser les composants disposants de mémoire

Le reconditionneur doit effectuer des opérations sur les ordinateurs pour les remettre à l'état d'origine. Les composants soumis à cette règle sont dépendants de la machine concernée. Il s'agit par exemple de la mémoire NVRAM de l'UEFI, du TPM ou des lecteurs biométriques. De manière générale, tout composant disposant de mémoire doit être réinitialisé.

Enfin, l'ajout ou le remplacement de pièces à l'ordinateur doit être encadré. Toute modification apportée doit être tracée et l'origine des pièces utilisées doit être précisée. Le reconditionneur doit être en capacité de fournir l'ensemble de ces changements à l'entité.

Les mises à jour des *firmwares* représentent une étape importante pour se prémunir des menaces persistantes à une simple réinstallation du système d'exploitation. Le reconditionneur doit s'assurer et garantir que ces mises à jour soient disponibles auprès des équipementiers. Dans le cadre d'un marché public, une clause peut être ajoutée en ce sens.

R17

Mettre à jour les firmwares

Le reconditionneur doit mettre à jour les *firmwares* et utiliser les sources officielles provenant du site de l'OEM.

Il est possible lors du reconditionnement des ordinateurs d'effectuer des tests plus poussés. Un exemple consiste à vérifier le bon fonctionnement des ports USB vis-à-vis des attaques matérielles. Ce type de tests nécessite des compétences techniques en matière de matériels et composants informatiques qui ne sont pas à la portée de tous les reconditionneurs. Ils doivent donc être spécifiés.

R18 +

Vérifier l'intégrité des ports USB, des firmwares et micro-contrôleurs associés

Le reconditionneur s'assure au minimum de la bonne fonctionnalité des ports USB. Ce test peut consister par exemple à s'appuyer sur des cartes externes de validation implémentant les procédures de tests d'interopérabilité xHCI [9]. Idéalement, l'intégrité des *firmwares* et des micro-contrôleurs USB sera également testée, par exemple via des outils matériels open-source éprouvés, comme les cartes GreatFET ou LUNA [3] exploitant les bibliothèques logicielles *FaceDancer* [2].

Une fois ces premières étapes réalisées, il est important de gérer les différents supports de stockage présents dans l'ordinateur et d'en effacer les données. En complément de l'étape précédente, cette

mesure vise à s'assurer qu'aucune donnée ou codes résiduels présents sur le matériel antérieurement à son reconditionnement ne persisteront à l'issue du reconditionnement.

R19

Effacer les supports de stockage

Le reconditionneur doit réaliser un « effacement sécurisé » des données. Les composants soumis à cette règle dépendent de la machine concernée. Il s'agit notamment des disques et leurs partitions système et de récupération.

Attention

Dans ce guide, le terme « effacement sécurisé » est utilisé pour désigner les techniques qui ont pour objectif de rendre très difficile la récupération ultérieure des données. Un « effacement sécurisé » va au-delà d'un effacement « simple » qui consiste à marquer « supprimées » des données au niveau du système de fichiers, alors que celles-ci sont toujours présentes sur le disque (et donc récupérables). Mais le terme « effacement sécurisé » ne doit pas donner la fausse impression d'une sécurisation qui serait absolue : en fonction de la technique d'effacement utilisée (voir section 3.2), il peut demeurer un risque que les données puissent être récupérées par un attaquant motivé et disposant de moyens conséquents. À ce titre un effacement cryptographique (voir R26) devra être préféré à un effacement dit « sécurisé ».

Attention

L'effacement de l'intégralité des partitions d'un disque doit être faite de telle sorte qu'il soit impossible de procéder à une réinitialisation d'usine du système d'exploitation. En effet, les partitions de réinitialisation prévues à l'origine par les constructeurs peuvent être exploitées par des attaquants à des fins de persistance.

Par ailleurs, en complément des prérequis du système d'exploitation choisi (voir R9), les besoins de sécurité de l'entité, notamment décrits dans sa PSSI, sont à prendre en compte. Pour ce faire, il est nécessaire que l'entité dispose d'un catalogue détaillant la configuration des machines de chaque lot.

R20

Lister les spécifications techniques des lots

Le reconditionneur doit lister les composants et spécifications techniques des machines de chaque lot.

Si le remplacement de certaines pièces est nécessaire sur les machines lors du reconditionnement, que ce soit pour réparer un dysfonctionnement ou améliorer les performances, alors ce composant ne doit pas diminuer la confiance dans le matériel. À ce titre, la provenance des composants est importante et celle-ci doit être tracée.

R21

Contrôler l'origine et l'innocuité des pièces de rechange

Si des pièces doivent être remplacées lors du reconditionnement seuls des composants neufs et traçables émanant du constructeur d'origine doivent être utilisés.

Les pièces ne doivent pas provenir de tiers de confiance moindre tels que des sites d'achat en ligne grand public (p. ex. eBay, Amazon, etc.). Cette règle concerne tous les composants (p. ex. carte mère, processeur, écran, etc.) à l'exception des disques durs (HDD, SSD), de la mémoire vive et des supports amovibles. De nombreux constructeurs reconnus proposent en effet des modèles différents mais compatibles. Par ailleurs, ceux-ci peuvent généralement être changés sur du matériel neuf sans compromettre la garantie du constructeur. Pour ces exceptions, on pourra donc se contenter d'acheter des composants neufs de constructeurs reconnus.

R22

Assurer la traçabilité des ordinateurs et des composants

Au-delà du contrôle, le reconditionneur doit garantir une traçabilité de l'origine des machines et des pièces changées. Ces éléments doivent pouvoir être fournis aux autorités compétentes.

Assurer l'intégrité et l'absence de porte dérobée d'un système d'exploitation est une tâche extrêmement complexe. Afin de limiter les risques, il est très fortement recommandé d'acheter des machines vierges de tout système d'exploitation, afin que l'entité procède elle-même à son installation. À défaut, il convient d'effacer l'entièreté du disque dur à la livraison et de réinstaller sa propre image du système. L'image installée devrait de toute façon être personnalisée pour correspondre au standard de chaque entité.

R23

Installer soi-même le système d'exploitation

L'entité doit garder la maîtrise de l'installation des systèmes d'exploitation (gestion des licences, choix de l'OS notamment) sur les ordinateurs reconditionnés. Cette action ne doit donc pas être réalisée par un tiers. La responsabilité reste à la charge de l'entité qui doit, au même titre que pour le reste de son parc informatique, installer sa propre image du système d'exploitation.

Attention

Préalablement à l'installation du système d'exploitation, il est recommandé de procéder à un formatage des disques durs ou SSD des ordinateurs reconditionnés reçus par le reconditionneur.

Lors de cette réinstallation, le chiffrement de la totalité du disque est nécessaire pour permettre son reconditionnement ultérieur. Au-delà de contribuer à la sécurité intrinsèque de l'équipement, cette mesure de chiffrement conditionne la bonne réussite des opérations de nettoyage et d'effacement, en vue d'une cession ultérieure du matériel reconditionné, ou d'une mise au rebut.

R24

Chiffrer les disques dès l'installation du système d'exploitation

Il est recommandé de chiffrer l'intégralité des disques, dès l'installation du système d'exploitation, pour assurer la confidentialité des données, mais également pour anticiper un besoin d'« effacement sécurisé » ultérieur notamment dans le cadre d'un reconditionnement, d'une réaffectation de poste ou de sa cession.

L'algorithme de chiffrement doit être robuste et donc respecter le référentiel général de sécurité (RGS) [16] et [17]. Une bonne pratique est d'utiliser une solution qualifiée pour réaliser ce chiffrement.

R25

Stockage et effacement des clés de chiffrement

Les clés de chiffrement doivent être stockées dans un composant de sécurité tel que le TPM, une carte à puce ou un *token*. Ces composants de sécurité intègrent des mécanismes d'« effacement sécurisés » qui doivent être utilisés pour effacer les dites clés de chiffrement. C'est ce que l'on appelle un effacement cryptographique par perte de clé.

Attention

La clé primaire permettant de déchiffrer le disque ne doit jamais être stockée en clair sur le disque lui-même. Les secrets de chiffrement quant à eux doivent être correctement protégés en confidentialité tout au long de leur cycle de vie et donc sur un support de stockage distinct.

L'ANSSI met à disposition des guides à prendre en compte lors de l'installation des postes et de la définition de la politique de sécurité afférente :

- exigences de sécurité matérielles [11],
- recommandations de sécurité relatives à un système GNU/Linux [13],
- mise en œuvre des fonctionnalités de sécurité de Windows 10 reposant sur la virtualisation [12].

3
Recommandations concernant la cession d'ordinateurs

IGI 1300

La cession de matériel ayant hébergé des informations classifiées de défense « SECRET, TRES SECRET » est interdite.
Les ordinateurs de bureau ou portables destinés à traiter des informations classifiées de défense « SECRET, TRES SECRET » doivent être achetés spécifiquement, être neufs et être détruits après usage.

Céder son matériel pour lui donner une seconde vie est une bonne pratique et concourt à l'effort écologique auquel tout à chacun peut aujourd'hui participer. Afin de procéder en toute sécurité et gérer les riques afférents, cette pratique doit toutefois s'accompagner de bonnes pratiques visant notamment à éviter toute fuite d'information qui pourrait nuire à l'entité.

3.1 Comprendre les risques

Comme évoqué dans le début du présent guide, si la cession de matériels contribue pleinement aux objectifs écologiques et environnementaux, tels que rappelés dans la loi AGEC, elle introduit un certain nombre de risques auxquels l'entité s'expose si elle ne réalise pas quelques actions préalables. Dans le cas des ordinateurs, qu'ils soient de bureau ou portables, ces principaux risques sont :

- **La fuite d'information** : bien souvent le personnel qui gère le parc informatique et le recyclage des machines ne connait ni l'usage qui a été fait du poste de travail ni le type de données qu'il a traité. Cette méconnaissance peut mener à une mauvaise gestion des actions à réaliser avant la cession. L'effacement des données est de la responsabilité de l'équipe qui gère les ordinateurs. Le choix du type d'effacement à réaliser dépend de plusieurs critères tels que le chiffrement initial ou non du poste. Des actions supplémentaires avant la seconde vie de la machine peuvent être requises. Par exemple, le disque pourrait ne pas être réutilisable et son traitement dépend de l'analyse de risques et de la PSSI de l'entité.
- **La compromission par un tiers** : faire réaliser le reconditionnement des ordinateurs par un tiers signifie donner accès aux données à ce tiers. Le reconditionneur choisi doit donc être de confiance et le contrat passé avec lui doit clairement identifier le processus de cession ou de mise au rebut du matériel.

- **La diffusion de code malveillant** : l'ordinateur cédé peut être affecté par un code malveillant. Son utilisation par son futur propriétaire peut l'exposer à une compromission du système d'information sur lequel il le déploiera.

Les recommandations ci-après permettent de traiter ces risques dans une certaine mesure. À l'instar des méthodes de reconditionnement, les techniques d'effacement ont certaines limites qui ne peuvent éliminer tous les risques. Ce chapitre traite donc des techniques d'effacement permettant de se protéger d'une menace cybercriminelle mais ne couvre pas les menaces étatiques. Il revient aux entités d'évaluer les risques et les menaces pesant sur leurs données.

Attention

Chiffrer un disque (dur ou SSD) a posteriori ne garantit pas que les données traitées antérieurement à cette opération de chiffrement ne seront pas récupérables avec des outils d'analyse inforensique. En fonction des données présentes, le processus de recyclage pourra être adapté, comme expliqué en section 3.2.

3.2 Rendre les données inaccessibles

L'effacement des données sur un disque est une problématique complexe. Par exemple, les disques durs mécaniques (HDD) stockent les données par secteurs, et nombre de ceux-ci peuvent tomber en panne sans affecter le fonctionnement opérationnel du disque. Ces secteurs défectueux ne sont plus réutilisés pour la suite de la vie du disque, mais les données initialement stockées dedans sont toujours présentes. La réécriture complète du disque ignore ces secteurs, mais une méthode inforensique légèrement avancée permet tout de même de récupérer ces données.

Les disques SSD, quant à eux, utilisent une technologie totalement différente et répartissent la donnée dans des cellules mémoire. Ces cellules peuvent être lues et écrites de manière individuelle par le *firmware*, mais sont abstraites des systèmes d'exploitation. La capacité réelle des SSD est supérieure à celle exposée au système d'exploitation pour permettre une rotation des cellules. De ce fait, les opérations de réécriture sur l'entièreté du disque depuis le système d'exploitation ne permet pas de s'assurer que toutes les cellules ont bien été traitées.

Concernant le troisième type de disque, dits disques hybrides (SSDH), ceux-ci sont composés d'un disque dur mécanique et d'un SSD. Les recommandations à prendre en considération seront les mêmes que pour les disques SSD.

Ces exemples ne font qu'illustrer la difficulté d'effacer les données d'un support physique. Mais, de nombreuses autres subtilités existent. Il faut également garder à l'esprit que de la donnée peut être stockée dans d'autres composants ayant de la mémoire (NVRAM UEFI, TPM, etc.).

Pour pallier ces problèmes, il est recommandé de chiffrer en amont les disques, avant que les données ne soient traitées dessus. Ceci permet ensuite d'effectuer un effacement cryptographique, dit « par perte de clé » et d'apporter ainsi plus de garanties sur le fait qu'un acteur malveillant ne récupérera pas les données par des opérations inforensiques. Plus précisément, cet effacement cryptographique consiste à effacer de manière sécurisée la clé de chiffrement (quelques dizaines d'octets seulement), rendant le déchiffrement des données impossible par la suite.

R26

Effectuer un effacement cryptographique

Avant d'être cédé, un ordinateur doit faire l'objet d'un effacement cryptographique. Les clés de chiffrement doivent avoir été stockées dans un composant de sécurité, tel que le TPM, une carte à puce ou un *token*. Ces composants de sécurité intègrent des mécanismes d'« effacement sécurisés » qui doivent être utilisés pour effacer les dites clés de chiffrement. C'est ce que l'on appelle un effacement cryptographique par perte de clé.

Attention

Pour réaliser cet effacement cryptographique il est indispensable que les disques aient été chiffrés lors de l'installation initiale de l'ordinateur.

Attention

La clé primaire permettant de déchiffrer le disque ne doit jamais être stockée en clair sur le disque lui-même. Les secrets de chiffrement quant à eux doivent être correctement protégés en confidentialité tout au long de leur cycle de vie et donc sur un support de stockage distinct.

Dans l'éventualité où le chiffrement n'a pas été réalisé lors de la première initialisation de l'ordinateur et en fonction de la sensibilité des données présentes sur les supports de stockage, le processus minimal d'effacement diffère. La gravité d'une fuite de données est à déterminer au cours d'une analyse de risques puisqu'elle dépend du contexte de l'entité.

R26 -

Adapter le processus d'effacement des disques à la sensibilité des données

Lorsque le chiffrement préalable du disque n'a pas été effectué et que l'effacement cryptographique n'est pas possible, un traitement alternatif doit être envisagé. Le logigramme présenté en figure 1 donne l'arbre de décision permettant de choisir le traitement le plus adapté, en fonction du niveau de sensibilité des données présentes sur le support.

Une entité qui met en application le logigramme de la figure 1 peut se retrouver dans le cas de figure où elle doit mettre en place une procédure alternative à l'effacement du disque (cas intitulé « Procédure en accord avec la PSSI de l'entité » dans le logrigramme). Elle peut alors par exemple décider de réutiliser le disque en interne plutôt que le céder, le stocker pendant quelques années ou le détruire.

Attention

Dans le cas d'un ordinateur qui aurait traité des données sensibles, voire DR, en clair puis qui serait réutilisé avec des données DR chiffrées, le chiffrement a posteriori ne permet pas de s'assurer que les données DR initiales ne sont pas récupérables. Le disque est donc à considérer comme « Non chiffré ← DR » dans le schéma.

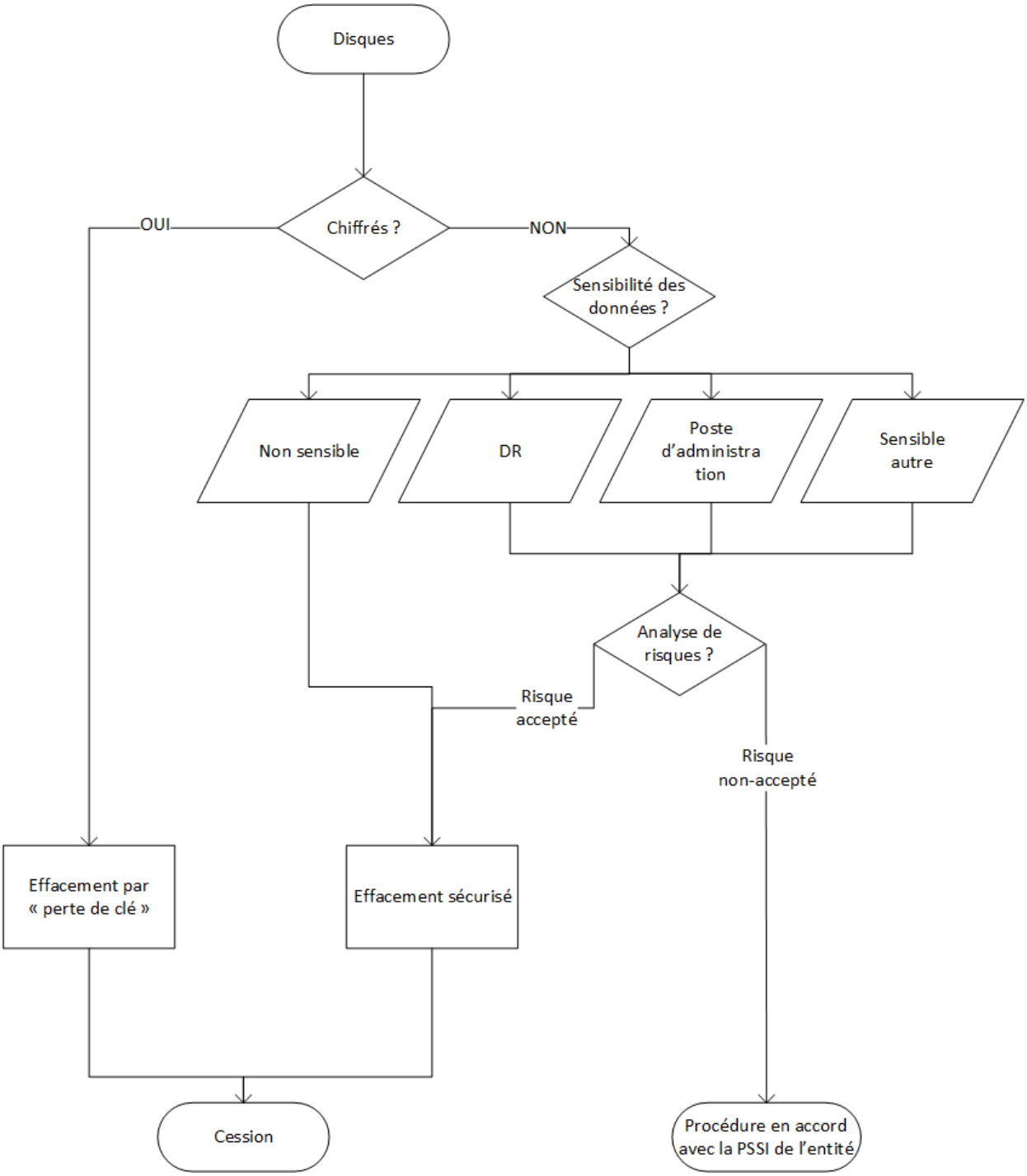

FIGURE 1 – Effacement des données

Pour effectuer un « effacement sécurisé » logiciel, plusieurs solutions sont possibles.

Pour les données non sensibles, il est possible d'utiliser :

- un logiciel ayant reçu au moins une certification CSPN par l'ANSSI, par exemple « Blancco Drive Eraser » dans sa version certifiée ;
- les outils fournis par le fabricant du disque dur effectuant un formatage dit de bas niveau ;

- des outils open source comme *hdparm* dans le but de déclencher les commandes d'« effacement sécurisé » des normes SATA ou NVMe.

Pour un disque implémentant la norme ATA, il est par exemple utiliser la commande hdparm sous Linux ou Windows. Ces commandes nécessitent des privilèges élevés (root) et ne fonctionneront pas sur certains systèmes pour lesquels le BIOS place le disque en mode *security freeze* au démarrage. Dans ces cas, il existe généralement des outils propriétaires fournis par l'OEM pour réaliser l'« effacement sécurisé ».

Sur le principe, la procédure suivante peut être mise en œuvre.

Création d'un mot de passe dans le disque à effacer pour permettre l'activation de la commande secure erase de hdparm pour le disque sdc :

```
hdparm --user-master user --security-set-pass pass /dev/sdc
```

Lancement de la commande *secure erase* avancée de hdparm :

```
hdparm --user-master user --security-erase-enhanced pass /dev/sdc
```

Si le disque ne supporte pas le *secure erase* avancé, il est possible d'utiliser le *secure erase* standard :

```
hdparm --user-master user --security-erase pass /dev/sdc
```

Attention

Les secteurs défectueux (*bad block*) ne seront pas effacés par les logiciels d'« effacement sécurisé ». Dans ce cas précis, des données peuvent persister sur le disque. Même si les blocs défectueux sont de taille réduite, ils peuvent contenir des informations importantes (clé de chiffrement par exemple). Il est recommandé dans ce cas de se référer à l'analyse de risques de l'entité concernant la sensibilité des données et d'adapter la procédure en conséquence.

De par leur conception, les médias de stockage de type mémoire flash (SSD, NVMe, SDcard, etc.) implémentent rarement les commandes *secure erase*, car leur utilisation peut réduire drastiquement leur durée de vie. Pour ce type de média, il est recommandé d'utiliser l'effacement cryptographique comme évoqué précédemment dans ce chapître. Les disques SSD qui implémentent ces commandes le font généralement en chiffrant les données en interne de manière transparente pour l'utilisateur, et en procédant à un effacement cryptographique de la clé secrète.

La norme NVMe prévoit néanmoins des commandes d'« effacement sécurisé », qui peuvent être utilisées lorsque le disque les supporte : *nvme-format* et *nvme-sanitize* (introduite dans la version 1.3). Lorsque le disque supporte les deux commandes, *nvme-sanitize* est à utiliser de préférence.

Par exemple en utilisant l'outil *nvme-cli* sous Linux, on peut realiser un effacement cryptographique à l'aide d'une des commandes suivantes :

```
nvme format /dev/nvme0 -s 2

nvme sanitize /dev/nvme0 -a 4
```

Il est recommandé de lire les pages de manuel de *nvme-format* et *nvme-sanitize* [5] pour choisir les options pertinentes au regard des fonctionnalités implementées par le disque a effacer.

Comme indiqué précédemment, l'effacement cryptographique ne sera pas pertinent si :

- le disque a contenu des données sensibles avant la mise en place du chiffrement ;
- il est impossible de garantir avec certitude que le média n'a pas contenu des données sensibles avant la mise en place du chiffrement sur celui-ci.

En dehors des disques, des données peuvent être stockées dans d'autres composants disposant de la mémoire (NVRAM UEFI, TPM, etc.). Ces données concernent généralement la configuration du système ou des secrets cryptographiques. Certains acteurs malveillants rachètent des ordinateurs pour obtenir de l'information sur l'entité, la configuration de ses postes, ses employés, etc.

R27

Effacer tous les composants mémoire

Tous les composants qui disposent de la mémoire doivent être effacés. Cette procédure s'effectue par l'intermédiaire du BIOS [9] et concerne notamment le fait de :

1. remettre la configuration UEFI aux valeurs d'usine (reset) ;
2. effacer la mémoire du TPM (commande dans l'UEFI ou via l'OS) ;
3. réinitialiser le lecteur d'empreintes digitales (supprimer les informations enregistrées).

Enfin, tous les supports amovibles qui ont pu être utilisés par l'entité doivent être retirés de l'ordinateur.

R28

Retirer les supports amovibles

Les supports amovibles tels que les cartes SIM et SD doivent être retirés avant cession des ordinateurs.

3.3 Dépersonnaliser les ordinateurs destinés à être cédés

En plus de rendre les données inaccessibles (par effacement cryptographique ou, à défaut, par effacement « sécurisé »), il est nécessaire d'assurer la traçabilité des ordinateurs destinés à être cédés et de révoquer leurs droits sur le système d'information de l'entité.

R29

Assurer la gestion du parc et révoquer les droits des ordinateurs cédés sur le SI de l'entité

Les ordinateurs doivent être décommissionnés du parc pour ensuite être cédés ou mis au rebut. Les éléments suivants doivent en autre être consignés : date de sortie, destinataire de la cession, prise en charge pour mise au rebut, parcours au sein de l'entité, etc. Il est également primordial de révoquer de toutes les bases d'accès les droits associés à ces matériels (802.1.x, liste d'autorisation d'adresses MAC, etc.).

9. Se référer à la documentation fournie par le constructeur

Par ailleurs, il arrive que les utilisateurs ou l'entité qui fournit les ordinateurs personnalisent les machines. Lors de la cession, ces éléments décoratifs ou de suivi interne (gestion de parc, etc.) peuvent fournir des indications plus ou moins précises aux attaquants (mail, entreprise ou administration, configuration, version logicielle ou *firmware*, etc.).

R30

Anonymiser les ordinateurs

Les autocollants, QR codes, codes barre, et autres signes distinctifs présents sur l'ordinateur et ses accessoires doivent être retirés.

Liste des recommandations

Bibliographie

[1] *En cas d'incident*.
Page web, ANSSI.
https://www.ssi.gouv.fr/en-cas-dincident/.

[2] *FaceDancer GitHub repository*.
Page web.
https://github.com/greatscottgadgets/facedancer.

[3] *LUNA : USB Multitool and Gateware Library*.
Page web.
https://luna.readthedocs.io/en/latest/.

[4] *One common charging solution for all*.
Page web, European Commission.
https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red/one-common-charging-solution-all_en.

[5] *Solid state drive/Memory cell clearing*.
Page web, ArchLinux.
https://wiki.archlinux.org/title/Solid_state_drive/Memory_cell_clearing.

[6] *LoJax : First UEFI rootkit found in the wild, courtesy of the Sednit group*.
Page web, ESET, sep 2018.
https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/.

[7] *Décret n° 2021-254 du 9 mars 2021 relatif à l'obligation d'acquisition par la commande publique de biens issus du réemploi ou de la réutilisation ou intégrant des matières recyclées*.
Référentiel, mar 2021.
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043231546.

[8] *Windows 11 System Requirements*.
Page web, aug 2021.
https://support.microsoft.com/en-us/windows/windows-11-system-requirements-86c11283-ea52-4782-9efd-7674389a7ba3.

[9] *xHCI Interoperability Test Procedures For Peripherals, Hubs and Hosts (Legacy, USB Type-C and Power Delivery)*.
Page Web Revision 1.0, Intel corporation, apr 2021.
https://www.usb.org/sites/default/files/3.2%20Interoperability%20Testing%20v1.0%20w%20USB%20Type-C.pdf.

[10] *Notice explicative du décret n° 2021-254 du 9 mars 2021*.
Référentiel, jan 2022.
https://www.ecologie.gouv.fr/sites/default/files/Notice%20explicative%20DCE%202021-254%20art%2058.pdf.

[11] *Recommandations de configuration matérielle de postes clients et serveurs x86*.
Note technique DAT-NT-024/ANSSI/SDE/NP v1.0, ANSSI, mars 2015.
https://www.ssi.gouv.fr/nt-x86.

[12] *Mise en œuvre des fonctionnalités de sécurité de Windows 10 reposant sur la virtualisation*.
Guide ANSSI-BP-039 v1.0, ANSSI, novembre 2017.
https://www.ssi.gouv.fr/windows10-vsm.

[13] *Recommandations de sécurité relatives à un système GNU/Linux*.
Guide ANSSI-BP-028 v2.0, ANSSI, octobre 2022.
https://www.ssi.gouv.fr/reco-securite-systeme-linux.

[14] *L'homologation de sécurité en neuf étapes simples*.
Guide ANSSI-PA-096 v1.0, ANSSI, août 2014.
https://www.ssi.gouv.fr/guide-homologation-securite.

[15] *Maîtrise du risque numérique - l'atout confiance*.
Guide ANSSI-PA-070 v1.0, ANSSI, novembre 2019.
https://www.ssi.gouv.fr/administration/guide/maitrise-du-risque-numerique-latout-confiance.

[16] *RGS Annexe B2 : Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques*.
Référentiel Version 2.0, ANSSI, juin 2012.
https://www.ssi.gouv.fr/rgs.

[17] *RGS Annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques*.
Référentiel Version 2.03, ANSSI, février 2014.
https://www.ssi.gouv.fr/rgs.

[18] *Licence ouverte / Open Licence v2.0*.
Page web, Mission Etalab, avril 2017.
https://www.etalab.gouv.fr/licence-ouverte-open-licence.

Version 1.0 - 30/06/2023 - ANSSI-PA-097
Licence ouverte / Open Licence (Étalab - v2.0)
ISBN : 978-2-11-167142-3 (papier)
ISBN : 978-2-11-167143-0 (numérique)
Dépôt légal : Juin 2023

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
www.ssi.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité