Ligne directrice sécurité de l'information & vie privée :

effacement des supports d'information électroniques

(BLD ERASE)

TABLE DES MATIÈRES

1. Introduction

Le présent document fait intégralement partie de la méthodologie relative à la sécurité de l'information et à la vie privée au sein de la sécurité sociale. Le présent document est destiné aux responsables, aux sous-traitants de données, au conseiller en sécurité de l'information (CISO) et au délégué à la protection des données (DPO) de l'institution publique de sécurité sociale (IPSS).

Le présent document décrit les responsabilités d'une organisation au niveau de l'effacement de supports magnétiques (tels des disques durs ou des bandes magnétiques) et de supports non magnétiques (tels les clés USB, les CD, les DVD ou cartes SD) pouvant contenir des données professionnelles, confidentielles ou sensibles.

2. Effacement de supports d'information

Toute organisation souscrit la politique suivante relative à la sécurité de l'information et à la vie privée pour l'ensemble des informations et systèmes d'information relevant de la responsabilité de l'organisation:

1. Le chiffrement est la mesure préventive de base en cas de vol, d'abus ou de perte du support d'information et constitue un élément essentiel permettant d'entraver le décodage éventuel des données après l'effacement du support. Pendant la durée de vie du support d'information et, en particulier pour les supports d'information mobiles, un chiffrement local de l'ensemble des données est toujours réalisé au moyen d'un produit agréé et moyennant la gestion correcte des clés de chiffrement. Les clés de chiffrement ne peuvent jamais être présentes de manière visible sur le support même. Ce chiffrement doit être appliqué à des volumes logiques dans leur ensemble (et non à des fichiers ou répertoires individuels). Ce chiffrement sert de complément aux mesures applicables sur le plan de l'organisation et aux procédures visant à prévenir des abus.
2. En cas de réutilisation, le support d'information est réutilisé dans un niveau de classification des données au moins comparable.
3. Afin de déterminer la méthode appropriée[1] pour l'effacement d'un support de données, il est nécessaire de réaliser une évaluation des risques.
4. Lorsque le risque résiduel[2] de retrouver des données consécutivement à l'effacement n'est pas acceptable pour l'organisation, le support doit être détruit physiquement, même si le risque résiduel est hypothétique.
5. Lorsque l'organisation utilise des supports de données qui ne sont pas sa propriété (par exemple, dans le cadre du leasing ou du disaster recovery), les mesures appropriées pour l'effacement des données doivent être fixées dans un contrat. Ceci est aussi le cas lorsque l'organisation ne maîtrise pas la technologie d'accès à l'ensemble des niveaux du support d'information (par exemple, dans le cadre du cloud computing).

[1] Voir l'annexe D

[2] La probabilité d'un impact négatif, malgré les mesures prises pour influencer (limiter) le risque (inhérent)

Annexe A: Gestion documentaire

Gestion des versions

Date	Auteur	Version	Description du changement	Date approbation	Date entrée en vigueur
2011		V2011	Première version	21/12/2011	01/01/2012
2017		V2017	Intégration UE GDPR	07/03/2017	07/03/2017

Erreurs et omissions

Si à la lecture du présent document, vous constatez des erreurs ou des problèmes, vous êtes invité, en tant que lecteur, à transmettre une brève description de l'erreur ou du problème et de sa localisation dans le document ainsi que vos données de contact au conseiller en sécurité de l'information (CISO) / délégué à la protection des données (DPO) de l'organisation.

Définitions

Pour garantir la cohérence en ce qui concerne la terminologie et les notions utilisées à travers les divers documents de politique, toutes les définitions relatives à la sécurité de l'information et à la protection de la vie privée sont regroupées dans un document spécifique : "Définitions sécurité de l'information et protection de la vie privée".

Annexe B: Références

Ci-dessous figurent les documents qui ont servi de source d'inspiration pour le présent document:

- ISO, “ISO/IEC 27001:2013 Information Security Management System Requirements”, september 2013, 23 p.
- ISO, “ISO/IEC 27002:2013 Code of Practice for Information Security Management”, september 2013, 80 p.
- ISO, “ISO/IEC 27040: 2015 Security techniques – storage security”, januari 2015, 111 p.
- ISACA, “COBIT 5 for Information Security”, Mei 2012, 220 p.
- NIST, “guidelines for media sanitization”, December 2014, 64 p.

Ci-dessous figurent les références aux sites web qui ont service de source d'inspiration pour le présent document:

- http://www.iso.org/iso/iso27001
- https://www.iso.org/standard/54534.html
- https://www.iso.org/standard/54533.html
- https://www.iso.org/standard/44404.html
- https://dban.org/
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
- http://www.ccb.belgium.be/nl/documents
- http://www.isaca.org/cobit
- https://www.safeonweb.be/nl
- https://www.cybersimpel.be/nl

Annexe C: problématique de l'effacement de données

La problématique de la réutilisation de supports contenant des informations sensibles est un sujet extrêmement complexe. Hormis la destruction physique, aucune solution technique ne garantit l'effacement total des données sur un support magnétique ou autre. Les procédés d' « effacement » consistent à écrire sur le support magnétique une ou plusieurs séries de caractères, déterminées ou aléatoires, en vue de rendre extrêmement difficile la récupération des données initiales. Le terme « réécriture » est donc plus approprié et traduit mieux le fait que l'information est toujours potentiellement présente sur le support du fait des limites du positionnement du dispositif mécanique d'écriture ou de l'algorithme sous-jacent.

Il est en pratique peu réaliste de garantir qu'il ne reste aucune trace exploitable par des laboratoires équipés de moyens importants ou dotés d'une connaissance fine du mode de fonctionnement des supports. Dans le domaine du magnétisme pur, outre les risques de rémanence d'information résiduelle, les disques modernes, de plus en plus variés et complexes, présentent en effet un nombre croissant de fonctionnalités (rattrapage de secteurs défectueux, masquage de partitions, etc.) qui contribuent à rendre des portions entières du disque inaccessibles via des commandes standard. Un attaquant ayant la connaissance des éventuelles commandes constructeur spécifiques ou équipé du matériel adéquat pourrait retrouver les données qui y sont stockées.

Bien que les technologies utilisées soient différentes, l'utilisation d'un produit de réécriture logique à des fins d'effacement d'un support de stockage non magnétique (clés USB, cartes à mémoire, mémoires FLASH) présente strictement les mêmes limites.

Les institutions devraient exiger que l'ensemble des données sur les supports numériques soient supprimées avant que ce support ne puisse être désassemblé, réaffecté (en interne ou en externe) ou réparé. Malheureusement, cela peut s'avérer impossible lorsque le dispositif est défectueux, et quiconque possède les ressources de laboratoire nécessaires pourrait recouvrer les données qui y sont stockées. Il y a lieu de réaliser une évaluation des risques pour chaque cas. Par ailleurs, il y a lieu de tenir compte de la valeur des données et de l'impact éventuel de leur divulgation. Lorsque le risque est moyen ou élevé, l'institution doit s'assurer que le support demeure sous son contrôle. Sinon, l'institution doit détruire le support conformément aux méthodes de destruction approuvées.

Annexe D: Méthodes de chiffrement, de suppression ou d'effacement des supports d'information

2.1. Chiffrement

Le chiffrement préalable des données réduit notablement le risque de compromission des données professionnelles, confidentielles et sensibles, même si toutes les données présentes sur le support d'information ne sont pas toutes supprimées. Il constitue par ailleurs le principal moyen technique pour réduire l'impact d'un vol, d'un abus ou d'une perte du support. La réécriture en fin de cycle de vie du support est toujours recommandée car le chiffrement ne peut garantir la protection des données que pendant une période limitée liée aux technologies utilisées. Ces solutions ont pour la plupart des limites intrinsèques telles que le risque de faiblesse du mot de passe/ de la phrase de passe protégeant la clé, l'existence de données sensibles non chiffrées dans les fichiers temporaires des outils ou du système d'exploitation, la présence des clefs en mémoire.

L'efficacité du chiffrement pour ce qui est d'assurer la protection permanente des données repose sur trois facteurs, à savoir la force du schéma de protection cryptographique mis en place, la qualité de la gestion de la clé de chiffrement par l'utilisateur et l'évitement des éléments de motivation d'attaque. S'il en a l'occasion et le temps, un adversaire compétent peut recouvrer les données s'il est suffisamment motivé à consentir l'effort requis. Les méthodes de chiffrement doivent être suffisamment dissuasives et faire en sorte que le niveau d'effort requis pour recouvrer les données soit supérieur à la valeur des données à recouvrer.

2.2. Réécriture

La réécriture du support d'information permet de supprimer ou d'effacer des données sur la base de trois techniques:

- CLEAR: supprimer des données au moyen d'un logiciel par des commandes standard ou le retour aux paramètres de fabrication. Ce retour aux paramètres de fabrication est souvent la méthode conseillée pour les appareils mobiles et les routeurs/commutateurs.
- PURGE: dans ce cas, des techniques de laboratoire sont appliquées de manière logique (techniques de chiffrement) afin de supprimer des données sur des médias au moyen de logiciels ou de matériel spécialisés (démagnétisation)
- INSTALL: en cas de réutilisation d'appareils, il suffit généralement de réaliser une nouvelle installation binaire (bits de données « 1 » et (ou) « 0 » dans toutes les zones d'enregistrement type Ghost, Bare Metal) étant donné que celle-ci écrase les données existantes de manière destructive.

L'efficacité de cette méthode est liée au nombre de cycles de réécriture (pour limiter le phénomène de rémanence en bordures de piste), à la compétence et aux connaissances de la personne qui exécute le processus, et aux fonctions de vérification du logiciel de réécriture. Celles-ci aident à s'assurer que la réécriture s'effectue sur tout l'espace de stockage accessible du support.

Norme "Secure Erase": Depuis environ 2001, tous les disques durs ATA (IDE) et SATA satisfont à la norme « Secure Erase ». Dans ce type de disque dur, le gestionnaire du disque dispose d'une commande "Secure Erase" qui, lorsqu'elle est activée, provoque un effacement (par écrasement) de l'ensemble des blocs du disque. L'intérêt majeur de cette solution est qu'elle est a priori plus fiable qu'une solution logicielle de plus haut niveau. Plus l'ordre d'effacement est donné à un niveau proche de la couche matérielle, plus il y a de chances que cet ordre soit exécuté avec l'effet souhaité. Selon certains, cette solution « Secure Erase » n'est cependant pas sûre si l'on envisage le cas où il existerait des commandes non documentées permettant d'accéder aux données prétendument effacées. Il y a lieu de tenir compte de cette éventualité, sachant que l'on a auparavant envisagé la possibilité d'une reconstitution de données écrasées par cette technique (MFM - Magnetic Force Microscopy). On notera cependant que le NIST ("National Institute of Standards and Technology") américain recommande dans plusieurs cas cette méthode d'effacement.

Toutefois, les disques durs « SCSI » et « Fiber Channel » ne répondent pas à cette norme. Ils peuvent uniquement être écrasés à l'aide de produits logiciels tiers. Il est préférable d'utiliser un logiciel qui a fait l'objet d'une analyse de laboratoire indépendante et qui donne accès à toute la zone de stockage connue du disque.

Gutmann a déjà conseillé en 1996 d'effectuer 35 passes consécutives pendant l'écrasement afin d'éviter tout risque de réparation des données. Ces 35 passes ont pour objet de prendre en compte toutes les techniques d'encodage des disques durs qui ont existé durant les 3 dernières décennies. Gutmman reconnaît que pour les technologies contemporaines (utilisant la reconnaissance du signal magnétique par la technique "PRML" – "Partial Response Maximum Likelihood"), quelques passes d'écriture de données aléatoires sont probablement suffisantes.

Une triple réécriture est généralement acceptable en tant que méthode de destruction de l'ensemble des données professionnelles et confidentielles. La triple réécriture de données ne convient pas comme méthode de destruction des données pour les supports magnétiques contenant des informations sensibles. Combinée à d'autres méthodes de destruction telles la désintégration ou le déchiquetage, cette triple réécriture offre une garantie complémentaire de destruction au-delà de tout espoir raisonnable de recouvrement.

Quant aux supports de stockage non magnétiques tels les clés USB, les cartes à mémoire, les mémoires FLASH, des algorithmes spécifiques d'écriture sont mis en place pour notamment gérer certains phénomènes de dégradation. Ceci induit la création de « copies » multiples qui augmentent les possibilités de récupération après effacement. Pour ce type de support d'information, non seulement le chiffrement des données, mais aussi la destruction physique du support d'information sont essentiels pour une protection maximale.

2.3. Démagnétisation

La démagnétisation consiste à appliquer une force magnétique d'une puissance suffisante pour effacer toutes les données d'un support magnétique particulier. L'efficacité de cette méthode est liée à l'intensité relative de la force magnétique offerte par l'appareil de démagnétisation et aux propriétés magnétiques du support de données.

2.4. Destruction physique

La destruction physique doit toujours être appliquée pour les médias défectueux et les médias WORM (write once, read many). Cette destruction doit être réalisée par des firmes spécialisées. Après destruction, il y a lieu de demander une « attestation de destruction garantie » ou la destruction doit au moins être enregistrée. Le délai de conservation de l'enregistrement est de 2 ans au moins.

2.4.1. Déformation physique

La déformation physique consiste à utiliser des outils tels une masse, une cloueuse, un étau, etc., pour causer à un support des dommages matériels extrêmes dans le but de retarder, gêner ou détourner toute tentative de recouvrement des données de la part d'un attaquant. Dans le cas des disques magnétiques, l'efficacité de cette méthode est liée à l'importance des dommages causés à la surface de chaque plateau (incluant la déformation de la surface plate) dans le but de rendre très difficile toute analyse de laboratoire. Pour les disques optiques, on peut utiliser une machine servant à appliquer aux disques une pression et une chaleur qui permettent de les étirer et de les courber aisément. Le but est de détruire les sillons optiques du disque afin de détruire effectivement les données.

2.4.2. Déchiquetage

Le déchiquetage est une forme de destruction qui consiste à réduire le support en petites pièces de taille et de format uniformes. Normalement, on utilise les déchiqueteuses uniquement avec les supports minces tels les CD-ROM, les DVD et les cartes SSD.

2.4.3. Désintégration

La désintégration consiste à utiliser un mécanisme non uniforme de découpage et de déchiquetage (p. ex. des lames rotatives dans une enceinte close, certaines centrifugeuses, moulin à marteaux) qui réduit le support en petites pièces de taille et de format aléatoires.

2.4.4. Broyage

Le broyage consiste à utiliser des appareils capables de réduire la couche porteuse de données d'un disque optique en fine poussière tout en laissant intact le disque lui-même qui sera recyclé ou éliminé. Toutefois, on ne peut utiliser cette méthode pour les DVD puisque leur couche porteuse d'information est prise en sandwich au centre.

2.4.5. Incinération

L'incinération consiste à détruire les supports d'information dans des incinérateurs adéquats.

2.4.6. Destruction chimique

Certains agents chimiques sont à même d'attaquer les supports de données et de les détruire.

Annexe E: Lien avec la norme ISO 27002:2013

Nous vous renvoyons ici aux principales clauses de la norme ISO 27002:2013 en rapport avec le sujet du présent document.

Norme ISO 27002:2013	
Politique de sécurité	
Organisation de la sécurité de l'information	
Sécurité des ressources humaines	
Gestion des actifs	
Protection de l'accès	
Cryptographie	**Oui**
Protection physique et protection de l'environnement	**Oui**
Protection des processus	
Sécurité de la communication	
Maintenance et développement de systèmes d'information	
Relations avec les fournisseurs	
Gestion des incidents de sécurité	
Aspects de la sécurité de l'information dans la gestion de la continuité	
Respect	

***** FIN DU DOCUMENT *****