Effacement des supports de stockage de masse

- Informatique - Sécurité Informatique -

Date de mise en ligne : vendredi 28 mai 2010

Spyworld Actu

Plusieurs solutions d'effacement ou de surcharge de supports de stockage sont disponibles sur le marché. La tentation est forte d'utiliser ces outils pour recycler des supports de stockage ayant contenu des informations sensibles. L'efficacité de ces outils, leur intérêt et leurs limites sont pourtant parfois mal connus.

La présente communication a pour objet de préciser la position de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en matière d'effacement de supports de stockage magnétiques (disques durs ou bandes magnétiques) et non-magnétiques (clés USB ou cartes SD par exemple) ayant contenu des informations sensibles.

Présentation

La problématique de la réutilisation des supports ayant contenu 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 ; les procédés appelés « blanchissement » ou « 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 de « surcharge » est donc plus approprié, et il 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.

D'une manière générale, l'ANSSI ne saurait donc cautionner la seule utilisation de produits d'effacement dans le cas où les supports considérés ont contenu des informations très sensibles, car 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 magnétiques. Outre les risques de rémanence d'information magnétique 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 standards, alors qu'un attaquant ayant la connaissance d'éventuelles commandes constructeur spécifiques lorsqu'elles existent ou équipé de matériels adéquats pourrait retrouver les données qui y sont stockées.

Bien que les technologies employées soient différentes, l'utilisation d'un produit de surcharge 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.

Recommandations de l'agence en matière de réduction du risque de compromission d'informations suite au recyclage d'un support de stockage ayant contenu des données sensibles

Afin de prendre en compte la menace liée au recyclage des supports de stockage de données sensibles, il convient d'appliquer les recommandations suivantes :

1. Pendant la durée de vie du support, procéder à un chiffrement local des données sensibles, de préférence par un produit recommandé gérant correctement ses clefs de chiffrement. Il s'agit que les clefs sous forme claire soient uniquement présentes en mémoire et jamais sur le support lui-même. Ce chiffrement doit porter sur des volumes logiques entiers plutôt que sur des fichiers ou répertoires individuels, et si possible sur l'intégralité du support. Ce chiffrement intervient en complément des mesures de sécurité organisationnelles applicables, qui s'attacheront en

particulier à réduire la probabilité d'un vol. 2. Après utilisation, recycler le support en privilégiant une réaffectation dans un contexte de niveau de sensibilité comparable. 3. En cas de cession du support, et si possible dans tous les scénarios de réaffectation, procéder à une surcharge complète par un produit recommandé. 4. De façon complémentaire au point précédent ou a minima en cas de recyclage dans un contexte de niveau de sensibilité comparable, procéder à une passe de surcharge à zéro du support. L'efficacité de la surcharge pourra ensuite éventuellement être vérifiée par une relecture logique, secteur par secteur, du disque.

En effet, le chiffrement préalable des données réduit le risque de compromission de données sensibles même si les informations présentes sur le support ne sont pas toutes supprimées. Il constitue par ailleurs le principal moyen technique pour réduire l'impact d'un vol ou d'une perte du support. Les solutions de chiffrement simples d'emploi ayant pour la plupart des limites intrinsèques (risque de faiblesse du mot de passe utilisateur protégeant la clé, existence de données sensibles non chiffrées dans les fichiers temporaires ou le swap du système d'exploitation, etc., présence des clefs en mémoire), la surcharge en fin de vie reste recommandée en complément au chiffrement, selon un principe de défense en profondeur.

Produits recommandés

D'une manière générale, l'ANSSI recommande l'usage de produits ayant fait l'objet d'un contrôle indépendant et en particulier les produits pour lesquels l'agence a délivré une qualification au niveau standard ou élémentaire ou, à défaut, une certification de sécurité de premier niveau (CSPN).

La liste des produits de chiffrement et d'effacement ayant obtenu respectivement une qualification ou une certification de premier niveau, ainsi que leurs cibles de sécurité et rapports de certification sont accessibles aux liens suivants :

- Produits qualifiés
- Produits CSPN

Post-scriptum :

http://www.ssi.gouv.fr/site_article...