Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 13 février 2017
N° CERTFR-2017-ACT-007

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2017-ACT-007

1 - Précautions à prendre avec le matériel d'occasion

Introduction

Lors de la mise au rebut ou de la revente, il est nécessaire de se préoccuper de l'effacement préalable des informations stockées sur tout dispositif comportant un support de stockage (ordinateur, serveur, téléphone, imprimante, clé USB, appareil photo numérique, récepteur GPS).

Il est tout aussi important d'appliquer ces règles d'hygiène lors de la réception d'un matériel d'occasion avant sa réutilisation.

La méthode choisie pour effacer les informations existantes sur le support informatique obsolète dépend de son niveau de sensibilité et du risque associé (voir Guide technique de lANSSI n 972-1/SGDN/DCSSI). Dans le cas particulier de données ou de matériels protégés par linstruction générale interministérielle 1300, une procédure stricte doit être appliquée par des personnels habilités.

Dans le cas de l'exportation de matériel hors de l'environnement sécurisé de l'entreprise, ou lors d'un transfert interne entre entités ayant des besoins de confidentialité distincts, la mesure la plus sûre reste l'extraction et la destruction physique des supports de stockage, puis leur remplacement lors de la remise en service.

Si cette destruction n'est pas envisageable, il existe, pour des composants type PC (comme les disques durs), des logiciels spécialisés destinés à effacer l'intégralité des données stockées. On peut citer le logiciel Blancco, dont la version 4.8 bénéficie d'une Certification de Sécurité de Premier Niveau délivrée par l'ANSSI.

Les imprimantes et photocopieurs multifonctions

Les imprimantes et photocopieurs multifonctions se comportent comme un ordinateur en intégrant souvent un navigateur web, une messagerie électronique, une connectivité Wifi et Ethernet, un accès USB et un disque dur. Le fonctionnement standard de ce type de matériel implique de stocker sur le disque dur les documents à imprimer ou à scanner. Selon vos activités ou votre mission, ce disque dur pourrait stocker des données confidentielles de votre entreprise. Un point d'attention particulier doit être porté sur les contrats de maintenance qui intègrent parfois un accès distant non contrôlé à léquipement depuis Internet.

Limprimante ou le photocopieur propose souvent des fonctionnalités de sécurité permettant l'effacement du disque dur ou la suppression des données liées aux impressions, copies, télécopies et numérisations pouvant être enregistrées sur le disque dur. Ce processus d'effacement peut parfois être activé automatiquement après chaque utilisation, ou programmé pour s'exécuter à intervalles spécifiés. Ces fonctionnalités ne garantissent pas toujours un effacement sécurisé des données considérées, et les périphériques de stockages internes et externes devront faire l'objet d'une procédure similaire aux autres équipements informatiques avant le décommissionnement de l'appareil. Attention toutefois, ces composants restent généralement la propriété de la société louant les appareils.

Lors de la réception d'un matériel de ce type, il conviendra de désactiver les fonctionnalités de stockage «dans le cloud» lors du paramétrage initial de l'appareil si celles-ci sont disponibles, et de s'assurer du niveau de mise à jour de l'appareil. Il faudra bien sûr maintenir ce niveau régulièrement afin de limiter l'exposition de son système d'information à des failles éventuellement apportées par cet équipement.

Les autres matériels informatiques

La plupart des matériels modernes intègrent des fonctions de restauration des paramètres d'usine. Il convient a minima de réinitialiser ainsi tout équipement entrant ou sortant de l'entreprise afin de supprimer par exemple certains mots de passes ou autres paramètres de configuration sensibles qui pourraient être stockés sur ces appareils.

Une réinitialisation permet également de se prémunir d'un éventuel piégeage logiciel simple de l'appareil par son précédent propriétaire.

Documentation

- Guide technique n 972-1/SGDN/DCSSI : Guide technique pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter.
  http://www.ssi.gouv.fr/archive/fr/documentation/Guide$_e ffaceur_V 1.12du040517.pdf$
- Instruction générale interministérielle n 1300 sur la protection du secret de la défense nationale :
  http://www.sgdsn.gouv.fr/IMG/pdf/IGI$_1 300.pdf$
- CSPN du logiciel Blancco :
  http://www.ssi.gouv.fr/entreprise/qualification/blancco-data-cleaner-version-4-8/

2 - Rappel des avis émis

Dans la période du 6 février au 12 février 2017, le CERT-FR a émis les publications suivantes :

- CERTFR-2017-AVI-046 : Multiples vulnérabilités dans Mozilla Firefox
- CERTFR-2017-AVI-045 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2017-AVI-044 : Multiples vulnérabilités dans le noyau Linux de Suse
- CERTFR-2017-AVI-043 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2017-AVI-042 : Multiples vulnérabilités dans le noyau Linux de Suse
- CERTFR-2017-AVI-041 : Multiples vulnérabilités dans les produits Citrix
- CERTFR-2017-AVI-040 : Multiples vulnérabilités dans Google Android (Nexus)
- CERTFR-2017-AVI-039 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2017-AVI-038 : Vulnérabilité dans Cisco Prime Home
- CERTFR-2017-AVI-037 : Multiples vulnérabilités dans VMware Airwatch
- CERTFR-2017-AVI-036 : Vulnérabilité dans Cisco WebEx Browser Extension
- CERTFR-2017-AVI-035 : Multiples vulnérabilités dans les produits Cisco

Gestion détaillée du document

13 février 2017 version initiale.