Précautions à prendre avant de se débarrasser du vieux matériel informatique

	Précautions à prendre avant de se débarrasser du vieux matériel informatique

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 l'ANSSI n° 972-1/SGDN/DCSSI). Dans le cas particulier de données ou de matériels protégés par l'instruction 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 l'équipement depuis Internet.

L'imprimante 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_effaceur_V1.12du040517.pdf
• Instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale :
http://www.sgdsn.gouv.fr/IMG/pdf/IGI_1300.pdf
• CSPN du logiciel Blancco :
http://www.ssi.gouv.fr/entreprise/qualification/blancco-data-cleaner-version-4-8/

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement..
(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Bulletin d'actualité CERTFR-2017-ACT-007