vigi@net
vigilance pour internet et les systèmes d'information
Bulletin du service du Haut fonctionnaire de défense et de sécurité

**n° 03**
**Juillet 2010**

## Focus !

### Les clés d'une dématérialisation sécurisée des services et des échanges entre administrations et usagers : le référentiel général de sécurité.

*Isabelle MOREL, fonctionnaire de sécurité des systèmes d'information (F.S.S.I.)*

*Le référentiel général de sécurité (RGS), publié au Journal Officiel n°113 du 18 mai 2010, définit un ensemble de règles de sécurité qui s'imposent aux autorités administratives et qui les assistent dans leur démarche de sécurisation des systèmes d'informations et télé-services. Les administrations doivent se mettre en conformité dans un délai de trois ans pour les systèmes d'information existants, douze mois pour les systèmes qui seront déployés dans les prochains six mois.*

*Le RGS a été élaboré conjointement par l'agence nationale de la sécurité des systèmes d'information (ANSSI) et la direction générale de la modernisation de l'Etat (DGME). L'ensemble des documents constituant le RGS est disponible sur : www.ssi.gouv.fr ou www.references.modernisation.gouv.fr*

*Le RGS a été créé par l'article 9 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives*

- *www.legifrance.gouv.fr*

*Ses conditions d'application ont été fixées par le décret n° 2010-112 du 2 février 2010*

- *www.legifrance.gouv.fr*

### ► Les messageries privées gratuites ne sont pas sûres ! N'utilisez pas des messageries privées gratuites dans le contexte professionnel.

Les messageries gratuites privées sont vulnérables. Les données sont souvent hébergées à l'étranger, et on en ignore souvent la localisation, ce qui pose le problème de risques de fuites de l'information, de perte des données et d'usurpation d'identité. Deux universités des Etats-Unis ont renoncé à utiliser la messagerie Gmail. Les responsables s'inquiétaient de la confidentialité des correspondances et considéraient que le réseau social Google buzz intégré à Gmail, présente un risque pour la protection de la vie privée et pour la sécurité. De manière concomitante, des administrations, parmi lesquelles des services sensibles, continuent d'utiliser des adresses de messagerie privées comme yahoo.com ou hotmail.com

> Recommandation : L'utilisation de comptes de messagerie fournis par l'administration doit être la norme pour les activités professionnelles.
> Si le recours à des messageries privées s'avère nécessaire, il doit prendre en compte la sécurisation des données et doit être maîtrisé.

### ► Danger des connexions Wi-Fi non protégées !

Les données personnelles peuvent être interceptées à partir de connexions Wifi non protégées. A la suite d'une enquête diligentée par les autorités allemandes, Google a admis que les « Google cars », chargées de photographier les rues de nombreux pays en Europe, récupéraient depuis 2007 des informations privées sur les réseaux Wifi.
La Chine vend sur des sites internet et des marchés locaux de produits électroniques des kits de connexion et d'intrusion de réseaux Wifi pour 24 $, ils sont composés d'une clé USB Wifi, d'un logiciel de cassage de clé de chiffrement de réseaux Wifi, et d'un manuel utilisable par les novices.

Recommandation : Ces deux informations illustrent la nécessité de protéger les réseaux Wifi par un chiffrement robuste autre que le WEP et un renouvellement régulier des clés.

### ► Les clés USB peuvent propager des virus !.

Des clés USB infectées ont été distribuées lors d'une conférence sur la sécurité des systèmes d'information, par une organisation internationale en charge de la sécurité des systèmes d'information.

Recommandation : La remise d'un support électronique doit s'accompagner au préalable d'une vérification de non-infection.

### ► Les pertes de données seraient majoritairement issues de serveurs.

De nombreuses entreprises ignorent où se trouvent précisément leurs données (serveurs, prestataires....). Si les serveurs sensibles sont généralement bien protégés, les attaquants peuvent récupérer les données en les atteignant à travers des postes d'employés ou en profitant de copies situées sur des serveurs moins sécurisés.

Recommandation : Afin de se prémunir contre des attaques de plus en plus sophistiquées, il est fortement recommandé d'effectuer un audit régulier du parc informatique et du contenu de l'ensemble des serveurs.

### ► Les disques durs des photocopieurs sont truffés de secrets d'entreprises !

Ces dernières ignorent que leurs anciens appareils conservent une importante quantité de données sensibles sur un disque dur accessible aux personnes malintentionnées. Les copieurs actuels, à l'instar des imprimantes réseau, constituent de véritables machines de stockage de données de l'entreprise sur le réseau.

Recommandation : Il convient de sécuriser les photocopieurs, notamment ceux qui sont en réseau, de les contrôler et de les mettre à jour, et, avant de s'en séparer, il est recommandé de retirer et de détruire le disque dur.

### ► La sécurisation des systèmes d'information dans les installations d'importance vitale.

Un ordinateur d'une station de traitement des eaux dans l'Oregon (USA) a été dérobé. Il contenait les logiciels de surveillance des pompes à eaux, des réservoirs et des niveaux de chlore de la station d'épuration.

Recommandation : La protection physique des machines dédiées à l'exploitation d'infrastructures critiques doit être prise en compte dans la politique de sécurité des systèmes d'information, au même titre que les systèmes à vocation bureautique.

---

**Source :** cette publication est une sélection des articles de la synthèse sur la sécurité des systèmes d'information réalisée et diffusée bi-hebdomadairement par la l'agence nationale de la sécurité des systèmes d'information.

**Glossaire** (sur le portail de la sécurité informatique de l'agence nationale de la sécurité des systèmes d'information)
www.securite-informatique.gouv.fr/gp_rubrique33.html

**Si vous voulez recevoir la newsletter, cliquez sur le lien et envoyer le message :**
**< Abonnement >**

**Pour vous désabonner de la newsletter, cliquer sur le lien et envoyez le message :**
**< Désabonnement >**

**Nous écrire :**
hfds@recherche.gouv.fr ou hfds@education.gouv.fr

**Retrouvez ce bulletin sur :**
www.pleiade.education.fr/portal/pleiade/hfds