O RGANISATIONNEL
T ECHNIQUE

Protéger et gérer l'accès au réseau

fiche 9

Le réseau informatique d'un acteur économique est désormais la principale porte d'entrée pour l'accès à l'information. Sa sécurité peut s'avérer vitale pour l'établissement. Mais celle-ci se mesure à l'aune de son maillon le plus faible. Chacun à son poste doit donc être pleinement mobilisé.

O

- Tenir à jour la liste précise de tous les équipements informatiques de l'établissement qui peuvent se connecter au réseau (ordinateurs personnels, imprimantes, photocopieurs, etc.).
- Identifier nommément chaque utilisateur, supprimer minutieusement les comptes anonymes et génériques.
- Attribuer des droits d'accès (répertoires, calendriers, etc.) de façon graduée et adaptée strictement aux besoins. Actualiser ces droits lors de mouvements internes.
- Limiter drastiquement le nombre d'utilisateurs disposant de **droits administrateurs**.
- S'assurer de la suppression effective des droits d'accès au réseau lors du départ d'un collaborateur ou d'un personnel temporaire.

T

- Privilégier une configuration d'accès à internet par câble plutôt que par WiFi.
- Si le WiFi est le seul moyen d'accéder à internet :
  - sécuriser l'accès en modifiant le nom d'utilisateur et le mot de passe attribué par défaut lors de la configuration initiale ;
  - vérifier que la *box* dispose du protocole de chiffrement **WPA2** et l'activer ;
  - remplacer la clé de connexion par défaut par un **mot de passe robuste** qui ne sera divulgué qu'à des tiers de confiance et changé régulièrement ;
  - activer et configurer les fonctions **pare-feu**/routeur. Ne pas hésiter à contacter l'assistance technique du **fournisseur d'accès**.
- Désactiver le signal WiFi de la borne d'accès lorsqu'il n'est pas utilisé.
- Vérifier qu'aucun équipement connecté au réseau interne (intranet) ne puisse être administré *via* internet. C'est souvent le cas des imprimantes, des serveurs, des routeurs, ainsi que d'équipements industriels ou de supervision. Limiter, si possible, la télémaintenance.
- Ne pas laisser de prises d'accès physique au réseau interne accessibles au public.
- Renouveler régulièrement les identifiants et mots de passe configurés par défaut sur tous les équipements (imprimantes, serveurs,…).

Avril 2014

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Délégation interministérielle à l'intelligence économique

MOTS-CLÉS

Droits administrateur :
faculté d'effectuer des modifications affectant tous les utilisateurs (modifier des paramètres de sécurité, installer des logiciels, etc.).

Fournisseur d'accès :
prestataire proposant une connexion à internet.

Mot de passe robuste :
la robustesse d'un mot de passe dépend en général d'abord de sa complexité, mais aussi de divers autres paramètres (Recommandations de sécurité relatives aux mots de passes – http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf). Choisir des mots de passe d'au moins 12 caractères de types différents :majuscules, minuscules, chiffres, caractères spéciaux.

Pare-feu (firewall) :
logiciel et/ou matériel protégeant un équipement ou un réseau informatique en contrôlant les entrées et sorties selon des règles définies par son administrateur.

WEP et WPA2 :
protocoles de sécurité permettant de fournir aux utilisateurs de réseaux locaux sans fil une protection contre le piratage. Le WPA2 devrait se substituer au système WEP jugé insuffisant.

POUR ALLER PLUS LOIN

Deux méthodes simples pour choisir les mots de passe :

- la **méthode phonétique** : « J'ai acheté 5 CD pour cent euros cet après-midi » : ght5CD%E7am ;
- la **méthode des premières lettres** : « Un tiens vaut mieux que deux tu l'auras » : 1tvmQ2tl'A.

Agence nationale de la sécurité des systèmes d'information (ANSSI)

- Guide d'hygiène informatique – http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf
- Recommandations de sécurité relatives aux mots de passe – http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf

RÉFÉRENT

- **ANSSI**