E2. Protéger et gérer l'accès au système d'information

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'entreprise et elle se mesure à l'aune de son maillon le plus faible. Chacun à son poste doit donc être pleinement mobilisé.

ORGANISATIONNEL

➤ Tenir à jour la liste précise de tous les équipements informatiques de l'entreprise qui peuvent se connecter au réseau (postes utilisateurs, serveurs, 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 des arrivées, des départs et des mouvements internes.

➤ Dédier les comptes d'administration à ces seules tâches.

➤ Limiter drastiquement le nombre d'utilisateurs disposant de **droits administrateurs**.

➤ S'assurer de la suppression effective des droits d'accès au système d'information lors du départ d'un collaborateur ou d'un personnel temporaire.

TECHNIQUE

➤ Privilégier une connexion au réseau par câble plutôt que par Wifi.

➤ Mettre en place une passerelle d'accès à internet sécurisée à travers par exemple la mise en place d'un **pare-feu**.

➤ Cloisonner les différents services au sein du réseau. En particulier, isoler les services exposés sur internet du reste du système d'information.

➤ Si le Wifi est utilisé, sécuriser l'accès en suivant les recommandations de l'Anssi.

➤ Vérifier qu'aucun équipement connecté au réseau interne ne puisse être administré via internet. Limiter, si possible, la télémaintenance. Cloisonner les fonctions d'administration du reste du système d'information.

➤ Ne pas laisser de prises d'accès physique au réseau interne accessibles à tous (salle d'attente, salle de réunion, etc.).

➤ Renouveler régulièrement les identifiants et mots de passe configurés sur tous les équipements (imprimantes, serveurs, etc.).

Mots clés

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

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.

Pour aller plus loin

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

- Guide des bonnes pratiques de l'informatique
- Guide d'hygiène informatique
- Sécuriser les accès Wi-Fi

➤ Service du Haut fonctionnaire de défense et de sécurité (SHFDS) du ministère de l'Économie, des Finances et de la Relance.