

# Sécurité des postes de travail

La protection des postes de travail représente une priorité majeure pour toute entreprise. Ces dispositifs constituent des points d'entrée potentiels vers le SI et l'outil de travail fondamental pour beaucoup de services. Ainsi, il est impératif de garantir leur sécurité contre toute menace potentielle.

## Risques de sécurité liés aux postes de travail

Parmi les risques possibles :

- / **Malwares** : Comprenant virus, vers, chevaux de Troie et ransomwares, ces programmes ont la capacité d'infecter les postes de travail, dérober des données sensibles, perturber les opérations et même bloquer l'accès au SI.
- / **Vulnérabilités logicielles** : Les logiciels obsolètes ou non patchés représentent des failles exploitables par des cybercriminels.
- / **Perte ou vol d'équipements** : Pouvant entraîner une exfiltration de données sensibles, leur publication sur des sources non contrôlées, une atteinte à la sécurité de l'entreprise, la récupération de données commerciales, l'obtention d'informations personnelles sur les utilisateurs, ...
- / **Utilisation de supports amovibles non sécurisés** : Les supports tels que les clés USB infectées présentent des risques pour les postes de travail dès leur introduction aux systèmes.

## Ressources pertinentes

- **Veille Cyber** sur les éventuelles vulnérabilités des postes de travail, notamment via le **CERT FR** [[Site WEB](#)] ou le **CERT Santé** [[Site WEB](#)].
- **La CNIL** qui fournit une fiche de sensibilisation autour des bonnes pratiques de sécurité des postes de travail [[Site WEB](#)].



## Bonnes pratiques

Il est essentiel de mettre en place des bonnes pratiques de gestion, notamment :

- **Centralisez la gestion des postes de travail** via des outils tels que des systèmes de gestion des correctifs, des solutions de gestion des configurations et des outils de gestion des stratégies GPO.
- **Gérez les privilèges selon la politique du moindre privilège** en limitant les autorisations des utilisateurs aux personnes qui en ont besoin dans le cadre de leurs tâches.
- **Installez un logiciel antivirus** sur tous les postes de travail afin de détecter les logiciels malveillants et opérer un blocage élémentaire
- **Configurez des pare-feu locaux** sur les postes de travail pour filtrer les flux entrants et sortants, et bloquer les communications suspectes.
- **Installez et maintenez à jour les logiciels et les systèmes d'exploitation** en définissant une politique de mise à jour structurée
- **Activez le chiffrement des disques durs** sur tous les postes pour sécuriser les données en cas de perte ou de vol.
- **Mettez en place des filtres web** pour empêcher l'accès aux sites malveillants et frauduleux (liste noire).
- **Introduisez des postes type « station blanche » et des procédures de nettoyage** pour se prémunir des risques liés aux supports amovibles type clés USB infectées.
- **Organisez régulièrement des sessions de sensibilisation** pour promouvoir de bonnes pratiques d'utilisation des postes de travail.