

**Définition de périphérique :**

Est considéré périphérique tout appareil connecté à un ordinateur dans le but d'y ajouter une ressource ou un outil.

Il peut s'agir d'un dispositif d'entrée (clavier), de pointage (souris), de sortie (écran), de stockage (disque dur externe ou clé USB) ou encore d'ajout de ressource (carte graphique externe).

**Risques liés aux périphériques :**

Pour commencer, il ne faut jamais se fier à du matériel qui aura été prêté ou trouvé. Il existe de nombreux accessoires (câbles, clés USB, etc) ayant été modifiés de sorte à injecter du code lors de leur utilisations, ou même capable de dégrader physiquement notre matériel (USB killer)

Ensuite, veillez à utiliser du matériel à jour, il n'est pas rare de voir des failles de sécurité apparaître sur des micrologiciels non maintenu/dont le support a été arrêté.

Des rootkits peuvent être utilisés/appliqués au travers d'un firmware (micrologiciel) et si celui-ci n'est plus mis à jour par la société qui l'a produit, cela ouvre une grande faille de sécurité.

**Comment me protéger ?**

Évaluez votre matériel : Lorsque vous achetez (ou votre entreprise) des périphériques, renseignez-vous sur la chaîne de production et d'approvisionnement.

Faites preuve de prudence lorsque vous utilisez du matériel ne vous appartenant pas (en cas de conférence il arrive souvent que le matériel soit préparé à l'avance par l'hôte). Lisez attentivement les demandes d'autorisations et les avertissements lorsque vous branchez un périphérique que VOUS ne connaissez pas.

Il existe des outils permettant de tester, d'identifier et de confirmer la sécurité d'un périphérique avant de s'en servir. (Il est par exemple possible de vérifier la signature électronique d'un périphérique disponible sur le réseau.)

Gardez toujours vos périphériques sous clés et à l'abri afin qu'ils ne puissent être modifiés ou remplacés à votre insu.

Pour tout périphérique nécessitant l'utilisation d'identifiant, obligez-vous à modifier ceux-ci. Il n'est pas rare de trouver sur le réseau des périphériques dont les identifiants sont encore admin/admin ou root/root.

Mettez à jour vos appareils et appliquez les correctifs de sécurité.

Désactivez les fonctionnalités de connexion et d'installation automatique des nouveaux périphériques.