

B3.3 : Sécuriser les équipements et les accès utilisateurs

Le référentiel

Les équipements des utilisateurs et leurs usages constituent sans doute un des maillons les plus vulnérables de la sécurité des systèmes d'informations. Il s'agit donc ici d'informer sur les risques et les menaces et de construire les savoirs opérationnels pour mettre en œuvre les bonnes pratiques permettant de sécuriser les équipements et les usages de l'utilisateur.

Cette compétence pourra être complétée avec l'enseignement de CEJMA pour mettre en évidence les principaux enjeux des nouvelles modalités de travail qui se développent dans les entreprises.

Cette compétence doit amener l'étudiant à :

- recenser les risques et les menaces ;
- repérer les comportements à risque ;
- préconiser les bons usages ;
- sécuriser l'accès physique au poste fixe, nomade ou mobile (protection physique, séquence de démarrage, chiffrement disque, supports amovibles, verrouillage, contrôle des canaux de connexion réseau, wifi, bluetooth...);
- sécuriser l'accès logique au poste fixe, nomade ou mobile (ouverture de session, mot de passe, pare-feu, antivirus, automatisation des mises à jour...);
- durcir le système en limitant les logiciels installés et les utilisateurs configurés ;
- restreindre les privilèges et gérer les habilitations ;
- établir des connexions nomades sécurisées ;
- auditer la sécurité d'un poste de travail.

Des ressources

Les liens ci-dessous renvoient vers des ressources qui permettent d'améliorer la sécurité des usages utilisateurs et des équipements.

- Configurer Keepass pour contraindre la complexité des mots de passe :
https://github.com/onSec-fr/Keepass-Enhanced-Security-Configuration/blob/main/KeePass_Secure_Auto_Install.ps1

From:

<https://wiki.sio.bts/> - **WIKI SIO : DEPUIS 2017**

Permanent link:

<https://wiki.sio.bts/doku.php?id=cybersecuriser>

Last update: **2023/12/05 16:52**

