CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

SI-400

Station de travail administrative dédiée

Juill. 2026

Votre gouvernement

Québec

SI

Intégrité des systèmes et des données

System and Information Integrity

SI-400 — Station de travail administrative dédiée (PbM-)

Énoncés :

Exiger que les opérations administratives ou de superutilisatrices ou superutilisateurs soient réalisées à partir d'une station de travail physique dédiée à ces tâches précises et isolée des autres fonctions et réseaux. La station ne devrait pas, entre autres, avoir accès à Internet.

Responsable : Aucun

Discussion :

Une station de travail administrative dédiée (STAD) est typiquement constituée d'un terminal d'utilisateur et d'une très petite sélection de logiciels conçus pour interfacer avec le système cible. Aux fins du présent contrôle, une station de travail est un système à partir duquel les tâches d'administration sont réalisées, par opposition au système cible. La STAD doit être renforcée pour le rôle afin de réduire la probabilité qu'un point d'extrémité de superutilisateur ou d'administrateur soit compromis par un auteur de menace (ce qui entraînerait logiquement la compromission du système cible). Les outils bureautiques typiques ne sont pas nécessaires sur la STAD. Toutes les applications et tous les services non essentiels doivent être supprimés. Les STAD n'ont pas de jonction de domaine, ne peuvent pas télécharger de correctifs à partir d'Internet et ne peuvent pas mettre à jour la documentation dans les applications en réseau. Les serveurs bastion ne sont pas une substitution à l'exigence imposant le recours à des STAD. Les connexions par l'entremise d'un serveur bastion doivent être effectuées à partir d'une STAD. Les serveurs bastions permettent de centraliser la journalisation des activités administratives, de simplifier l'isolation réseau des serveurs critiques et de fournir un point de transfert commun pour les administratrices et administrateurs avec séparation des tâches (par exemple, où les correctifs d'un logiciel sont préparés par une administratrice ou un administrateur afin d'être installés par une ou un autre). Si un RPV est utilisé pour fournir la connectivité réseau, celui-ci doit automatiquement exclure tous les autres accès réseau à l'exception du RPV. La STAD doit être en mesure d'accéder à d'autres réseaux que celui-ci qu'elle administre. L'interface de gestion du système cible doit se limiter à la gestion du réseau et ne pas être accessible aux réseaux plus vastes, comme les réseaux locaux des stations de travail de l'organisation ou Internet. Si plusieurs réseaux cibles sont administrés par la même STAD logique, tous les réseaux doivent avoir le même profil de sécurité (par exemple, une seule STAD ne peut pas administrer un réseau SECRET et un réseau PROTÉGÉ B). Les logiciels de terminaux virtuels qui émulent un terminal simple devraient également résider sur une STAD.