



Aperçu des fonctions de sécurité des systèmes d'exploitation - WINDOWS

Introduction Un avantage important du système d'exploitation WINDOWS d'ordinateur de bureau (comprend Windows NT, Windows 2000, Windows XP et Windows Vista) est le soutien dont il bénéficie dans l'industrie et la disponibilité de solutions de tierces parties. Toutefois, cet avantage est associé à des risques pour la sécurité. Un ordinateur WINDOWS dans un environnement de réseau du GC peut être compromis par des maliciels ou autres menaces qui pourraient se propager aux autres réseaux du GC. Une installation non sécurisée de ce système peut exposer les renseignements du GC stockés dans l'ordinateur à du personnel non autorisé ou rendre de l'information essentielle inaccessible. Les ministères doivent donc s'assurer que le système d'exploitation WINDOWS est configuré et utilisé de façon sûre.

Cycle de vie On doit assurer la sécurité à chaque stade du cycle de vie du système d'exploitation : évaluation, configuration, déploiement, gestion et mise hors service.

Environnements de travail Les systèmes WINDOWS requièrent des contrôles de sécurité différents selon leur utilisation. Les environnements de déploiement varient des ordinateurs de production du GC (les plus sûrs) aux ordinateurs de développement du GC (moyennement sûrs) et aux ordinateurs mobiles (les moins sûrs) tels ceux que l'on retrouve dans les aires de réception, les salles de conférence et les zones d'impression.

Recommandations de base en matière de sécurité

Identification et authentification – Renommer le compte d'administrateur local des ordinateurs sur les bureaux et renforcer la sécurité des mots de passe.

Autorisation– Resserrer les permissions liées à tous les comptes d'utilisateur. Envisager l'application d'un niveau de privilège minimal obligatoire pour tous les comptes.

Contrôle d'accès – Désactiver l'accès anonyme, activer le verrouillage d'utilisateur, supprimer l'option « tous » de toutes les permissions de partage de fichiers par défaut.

Confidentialité – Envisager de renforcer les politiques liées au compte d'utilisateur (mot de passe robuste) et désactiver les paramètres « Temp Folder ».

Intégrité – Utiliser l'antivirus et l'antimaliciel les plus récents, désactiver Windows Messenger, désactiver les téléchargements automatiques et renforcer la politique liée à Internet Explorer.

Disponibilité – Utiliser la gestion de rustines la plus récente et limiter la connectivité du serveur de terminaux à UN.

Responsabilisation et non-répudiation – Améliorer la vérification en ajoutant les réussites et les échecs, les changements de politique, les événements de système et de connexion, et sécuriser les données de vérification et de journalisation, et assurer une synchronisation au moyen d'une source de synchronisation autorisée et sécurisée.

| Profil de sécurité | Environnement de travail |
|---|------------------------------------|
| Les moins dangereux (les plus sûrs) | Ordinateurs de production du GC |
| Moyennement dangereux (moyennement sûrs) | Ordinateurs de développement du GC |
| Dangereux (pas sûrs) | Ordinateurs partagés |
| Les plus dangereux (les moins sûrs) | Ordinateurs mobiles |