

SECURITE LOGIQUE

Contrôle d'accès (Poste de travail)

LOGI01

Contexte :

Le poste de travail, en réseau ou en mode autonome, permet à tout utilisateur en possession des connaissances suffisantes (éventuellement identifiant et mots de passe) d'accéder aux données, aux applications, aux programmes et aux fichiers.

Objectifs :

La mise en place d'une interface de contrôle d'accès permet d'authentifier l'utilisateur, de gérer et d'automatiser les connexions aux applications.

Elle permet d'assurer la cohérence des différents maillons de sécurité et de valider les différents niveaux d'accès aux systèmes et aux données.

Recommandations :

Les différents niveaux d'accès (en dispositif et en identifiant) représentent une vulnérabilité potentielle importante.

Les moyens de contrôle d'accès sont multiples, ils ont pour objet :

- d'identifier, d'authentifier et de sélectionner l'accès de l'utilisateur au poste de travail,
- de valider les connexions,
- d'autoriser et valider les transactions,
- d'assurer des fonctions d'horodatage et de traçabilité.

Les technologies utilisées vont des dispositifs autonomes de biométrie (contrôle des empreintes, rétine de l'œil, forme de la paume, reconnaissance de la dynamique de l'écriture, etc.), lecteurs de cartes à puces, déclencheurs infra-rouges, jusqu'à l'intégration des choix des accès aux applications et aux données du poste micro-informatique ou au système d'information complet (en liaison avec un serveur d'authentification).

Une des fonctions des dispositifs de contrôle d'accès est également de vérifier périodiquement la validité de l'autorisation d'accès pendant la durée d'une connexion. Cela permet en particulier de diminuer les risques d'attaques par écoute passive et usurpation d'identité.

Remarques :

Parmi les solutions de contrôle d'accès actuelles, celle de type SSO (Single Sign On) apporte une réponse satisfaisante aux exigences attendues des différents maillons de sécurité et permet une protection efficace des postes de travail.

Pour les postes de travail autonomes ou les petits réseaux bureautiques, des solutions de type logiciel et/ou matériel moins complexes et moins onéreuses sont présentes sur le marché. Les systèmes d'exploitation récents intègrent ces fonctionnalités.

La tendance actuelle est d'adjoindre le contrôle d'accès aux systèmes fédérateurs que sont les annuaires (LDAP) ou les méta-annuaires.



Les présentes recommandations ne sauraient mettre en cause la responsabilité du CLUSIF, elles ne présentent qu'un caractère indicatif et ne sauraient prétendre à l'exhaustivité.