ADMINISTRATION

Surveillance | ADMI03

Contexte :
Les réseaux d'entreprise sont de plus en plus ouverts vers l'extérieur et complexes dans leur architecture et dans leur supervision.

Objectifs :
S'assurer de l'intégrité et de la disponibilité du réseau, répondre aux alertes de sécurité et parer aux tentatives d'intrusion.

Recommandations :
Les ressources disponibles pour la surveillance et l'administration des réseaux d'entreprise sont des programmes, des utilitaires, des journaux (logs) et des commandes.

Postes de travail et serveurs :
- Journaux d'évènements et d'audit (messages et traçabilité des connexions réseau avortées, anormales, conflit d'adresses IP, ouverture anormale de certains ports de communication)
- Commandes MSDos (netstat, ping …)

Serveurs :
- L'observateur d'évènements pour les messages d'erreur Windows,
- Un serveur syslog pour Unix et les éléments actifs de télécommunication

Une stratégie d'audit qui s'appuie sur les processus systèmes automatisés permet de surveiller si toutes les tâches sont bien exécutées conformément à la prévision.
Des contrôles d'intégrité des systèmes d'exploitation peuvent être activés.

Équipements actifs du réseau (switchs/Hubs/routeurs)
La surveillance visuelle de ces équipements permet de détecter en fonction de l'état des voyants (éventuellement émission de bips sonores) si l'accès réseau est en erreur ou en bon fonctionnement.

Pour du trafic anormal ou des saturations du réseau, il faut un programme spécifique (en général appelé Agent) dans les équipements pour remonter les alertes vers la station d'administration ou de surveillance.
Dans les dernières technologies, les programmes embarqués ont aussi une fonction Web qui permet d'accéder plus facilement à la surveillance à partir de n'importe quel poste de travail avec un navigateur web (Internet Explorer, Netscape …). On veillera à modifier impérativement les logins et mots de passe définis par défaut par les constructeurs.

Les applications spécifiques de surveillance :
- Détection de virus, *Alertes virales (cf. fiche LOGI03…)*
- Détection d'intrusion
- Firewall, Proxy
- Détection de courriers non sollicités (Anti-Spam)
- Filtrage et contrôle de trafic et bande passante
- Détection des vulnérabilités des serveurs (sous réserve d'assurer la continuité de service)

Ces fonctions sont complémentaires et peuvent être installées sur des postes de travail ou sur des serveurs dédiés.

La veille technologique :
Abonnement aux listes de diffusion des alertes de sécurité proposées par les CERT, éditeurs …
Recherche, test et mise en œuvre des correctifs adéquats.

Remarques :
Une surveillance permanente est possible, il faut prévoir des ressources de centralisation des alertes (serveur ou station de travail supportant des logiciels tels HP OpenView, Netview, Tivoli, TNG Unicenter …) dédiées à la fonction de plate-forme d'administration et de surveillance des réseaux et des systèmes.
Si possible, il faut éliminer les anciennes versions et systèmes d'exploitation trop vulnérables.