Surveillance des activités à privilèges : les 10 meilleures pratiques (Tribune)

Le facteur humain reste le maillon faible en matière de sécurité informatique dans l'entreprise. Ainsi, plus les utilisateurs ont des droits sur le système d'information, plus le degré de risque est élevé. Il est donc indispensable de mettre en place des outils de surveillance des accès et des activités sur le système d'information, en particulier pour les utilisateurs privilégiés.

Outre le facteur humain, selon leur secteur d'activité, certaines entreprises doivent adopter plusieurs réglementations de conformité telles que PCI-DSS, SOX, COBIT, Bâle II, HIPAA, ISO 2700X pour permettre la surveillance des activités des employés, principalement ceux qui disposent de comptes à privilèges.

Afin que cette surveillance soit efficace, il est nécessaire de respecter quelques bonnes pratiques :

1/ Adopter le principe du moindre privilège

C'est à dire attribuer au compte d'un utilisateur, uniquement les privilèges dont il a absolument besoin pour effectuer son travail.

2/ N'utiliser le « mode Dieu » qu'en cas d'urgence

En règle générale, les administrateurs système n'ont pas besoin de disposer d'un accès illimité aux systèmes pour en assurer le bon fonctionnement. Il est préférable de verrouiller les comptes « super utilisateurs » (racine, administrateur, système, etc.) et ne les utiliser qu'en cas de nécessité absolue.

3/ Personnaliser chaque compte

Il faut définir les responsabilités personnelles de chacun des utilisateurs privilégiés. La première étape consiste à réduire au minimum le nombre de comptes partagés. La seconde consiste à ne pas partager les mots de passe des comptes partagés. On peut ensuite définir des domaines fonctionnels, en détectant les incompatibilités et en effectuant la séparation des tâches.

4/ Limiter la quantité de systèmes entrant dans la portée des comptes privilégiés de chaque personne

Les administrateurs système doivent jouir des privilèges d'un « super utilisateur » uniquement sur les systèmes sur lesquels cela est nécessaire, en fonction des besoins commerciaux et opérationnels. Il s'agit là d'une recommandation d'audit tout à fait standard.

5/ Développer une infrastructure de surveillance de l'utilisateur centrale

La gestion des journaux ainsi que les solutions SIEM ne capturent pas toutes les informations nécessaires. La meilleure façon de supprimer ces angles morts consiste à utiliser une solution de surveillance d'activité privilégiée. Cette procédure augmente la taille des journaux existants en indiquant précisément ce que l'utilisateur a fait (et non les résultats techniques de ses actions).

6/ Mettre en place un dispositif de surveillance des activités indépendant et transparent

On évite ainsi que les informations auditées ne soient modifiées. Même l'administrateur du dispositif sera dans l'incapacité de modifier les pistes d'audit chiffrées. L'environnement IT existant ne nécessitera ainsi aucune modification et les utilisateurs pourront continuer à travailler comme à leur habitude.

7/ Utiliser une authentification et une autorisation renforcées pour les comptes privilégiés

Lorsque des privilèges de « super utilisateur » sont attribués à des comptes personnels, il faut protéger ceux-ci au moyen de méthodes d'authentification renforcées. Les administrateurs disposant de tous les privilèges doivent utiliser un niveau d'assurance élevé (ex : des clés publiques ou des jetons intelligents de type X.509). Afin d'éviter une mauvaise configuration accidentelle ou une erreur humaine, certains outils PAM prennent en charge le principe dit « 4 eyes authorization » (principe des 4 yeux). Pour cela, il est nécessaire d'autoriser le suivi des actions de l'administrateur sur le serveur.

8/ Contrôler dans le détail les accès distants

La manière la plus sécurisée consiste à surveiller dans le détail les informations et le moment auxquels les personnes peuvent accéder, en fonction du protocole utilisé. Il est alors possible de contrôler les transferts de fichiers ainsi que le trafic inhabituel. On peut ainsi autoriser ou refuser des canaux de protocole tels que le partage de disques, le transfert de ports ou les transferts de fichiers en fonction de l'appartenance d'un utilisateur à un groupe, ou encore de l'heure.

9/ Éviter les actions malveillantes en temps réel

Il faut en effet être en mesure de pouvoir surveiller le trafic des connexions distantes en temps réel et d'exécuter différentes actions si un schéma donné (par exemple une commande ou un texte douteux) apparaît sur la ligne de commande ou à l'écran. Ainsi, si l'utilisateur s'aventure à effectuer une action risquée, on doit pouvoir être alerté ou mettre immédiatement fin à la connexion. Il doit être également possible de bloquer la connexion avant qu'un administrateur doté de mauvaises intentions n'exécute une action sur le serveur.

10/ Améliorer les preuves informatiques au moyen d'une relecture et d'une recherche rapide

Etre en mesure de rejouer les sessions enregistrées, comme un film pour revoir parfaitement ce que les utilisateurs ont effectué, comme elles se sont produites sur leur écran permet d'apporter la preuve en cas de problème. En cas de problème (manipulation d'une base de données, arrêt inattendu, etc.), les circonstances dans lesquelles l'événement s'est produit sont à disposition dans les pistes d'audit, et la cause de l'incident peut ainsi être facilement identifiée.

Voir aussi :
Silicon.fr étend son site dédié à l'emploi IT
Silicon.fr en direct sur les smartphones et tablettes