Gestion des utilisateurs à privilèges :

les idées reçues ont encore de beaux jours devant elles

La sécurité périmétrique (firewall, IPS/IDS, VPN …) est souvent bien connue et maîtrisée mais pense-t-on suffisamment aux personnes ayant des droits de modifications sur un réseau (administrateur interne ou externe, prestataire etc.) ?

Voici cinq affirmations qui prouvent que cet aspect de la sécurité des SI est parfois méconnu ou pétri d'idées reçues.

WALLIX

TRACE, AUDIT & TRUST

1. Notre système vient d'être audité, **nous sommes conformes.**

L'idée reçue : un audit qui se conclue de façon positive n'est absolument pas synonyme d'imperméabilité aux attaques, en témoignent toutes les entreprises hackées ces dernières années des deux côtés de l'Atlantique.

Pourquoi ? Premièrement parce que la plupart des départements informatiques déploient généralement toute l'énergie nécessaire au moment des audits, mais ont tendance à perdre de vue la conformité le reste de l'année. Ensuite, les auditeurs ne savent pas toujours où rechercher des failles et peuvent tout à fait être mal aiguillés.

Les pirates ne préviennent pas avant d'attaquer un système et ils ne tomberont certainement pas sur les failles de sécurité de votre entreprise par hasard. Ils savent généralement exactement ce qu'ils cherchent et ils le trouveront fort probablement.

La réalité : ne concentrez pas toute votre attention sur l'audit en question. Ayez davantage en mémoire que la conformité est un travail de tous les instants. Toute faille de sécurité est à étudier et à résoudre sur le long terme, plutôt qu'un simple « trou » à combler à tout prix.

2. Nos politiques de sécurité prévoient une **réinitialisation régulière des mots de passe**

L'idée reçue : même si les identifiants des utilisateurs « lambda » sont régulièrement et automatiquement modifiés, les utilisateurs à privilèges, eux, ne sont pas concernés par ces process en place et leurs mots de passe sont, par conséquent, très rarement modifiés. Il est inutile de penser que, parce que les administrateurs changent les mots de passe manuellement, un périmètre de sécurité est en place. La tâche est tout simplement trop ardue, trop étendue et trop difficile à maintenir dans le temps.

Une personne se connectant physiquement à des machines ou même via des scripts pour changer les mots de passe et être en règle avec les normes de conformité rencontrera forcément, au mieux des difficultés, au pire des complications. Pensez à tous les services (souvent interconnectés) installés sur des machines accessibles à des utilisateurs à privilèges qui doivent être correctement arrêtés avant qu'un changement ne soit appliqué, puis redémarrés. C'est une mission difficile, source d'erreurs et très consommatrice de temps.

La réalité : avant de déployer un nouveau dispositif ou un programme sur votre réseau, assurez-vous que l'ensemble des mots de passe par défaut a été modifié. Ceci est plus facile à dire qu'à faire : il y a probablement plus d'identifiants partagés que vous ne l'imaginez.

3. Nos administrateurs système ont **chacun leurs identifiants pour les comptes à privilèges. Nous ne risquons rien.**

L'idée reçue : malheureusement, dans ce domaine, la facilité l'emporte sur la sécurité. Combien de sociétés étaient persuadées que les identifiants des comptes à privilèges étaient uniques mais se sont rendu compte que ça n'était pas le cas ? On a déjà vu des sociétés mères communiquer les identifiants aux comptes à privilèges à une filiale sans les modifier par la suite. Ainsi, l'équipe IT de la filiale peut, en toute liberté, accéder aux données de la société mère sans aucun réel contrôle ni aucune traçabilité.

La réalité : planifiez un changement de mot de passe de vos comptes à privilèges tous les 60 jours, maximum. N'oubliez pas de choisir des mots de passe uniques et complexes pour chaque compte.

4. Notre département informatique **contrôle les accès. Nous sommes à l'abri.**

Les mots de passe des comptes à hyper privilèges sont souvent intégrés directement aux applications ou communiqués à des prestataires externes. Ces identifiants étant partagés, il est absolument impossible de savoir exactement qui se cache derrière une connexion et ce qui a été fait pendant la session. De la même façon, ces mots de passe étant assez peu fréquemment modifiés, un employé ayant quitté la société ou un prestataire externe arrivé à échéance de son contrat pourra tout à fait utiliser ces crédences et pirater le système.

En ce qui concerne les comptes administratifs, ils sont très nombreux et les identifiants sont également partagés. Tous les utilisateurs à privilèges utilisant les mêmes identifiants pour accéder à une machine et intégrer des modifications, on ne sait jamais véritablement qui est l'auteur de ces changements ou même qui a eu accès à des données sensibles. Enfin, il faut également aborder le problème de la gestion du turn-over. Certains employés évoluent, changent de poste ou même quittent la société. Si leur identifiant ne sont pas modifiés après leur évolution ou leur départ, ils auront toujours accès à des informations qu'ils n'ont pas besoin de connaître ou à des services qui ne leur sont plus utiles.

5. Nous avons mis en place une **solution d'IAM.**

Notre réseau est sécurisé

Comme nous l'avons évoqué auparavant, les entreprises n'ont souvent rien mis en place pour contrôler les comptes à très haut privilèges utilisés pour les urgences ou les accès administratifs plus classiques. En d'autres termes, aucune solution de sécurité existante comme un firewall ou un logiciel d'IAM ne sait tracer et contrôler les accès à privilèges ; et à moins de posséder une solution dédiée au contrôle des utilisateurs privilégiés, ça ne sera jamais le cas.

La réalité : Mettez en place des outils capables de répertorier tous les comptes à privilèges, surveiller les actions douteuses, auditer l'ensemble des activités et contrôler leur administration.

WAB

Wallix AdminBastion

Wallix AdminBastion est une solution de traçabilité et de contrôle d'accès des utilisateurs à privilèges.

Elle couvre quatre aspects essentiels de la gestion des comptes à privilèges :

- Contrôle d'accès des utilisateurs à privilèges
- Traçabilité des sessions administrateurs internes ou externes
- Gestion des mots de passe
- Gestion post-mortem des incidents

Téléchargez une version d'évaluation sur www.wallix.fr

www.wallix.com

WALLIX FRANCE (HQ)
http://www.wallix.fr
Email : sales@wallix.com
118, rue de Tocqueville - 75017 Paris
Phone: +33 (0)1 53 42 12 90
Fax: +33 (0)1 43 87 68 38

WALLIX UK
http://www.wallix.com
Email: ukinfo@wallix.com
Lincoln House - 300 High Holborn - London WC1V 7JH
Phone: +44 (0) 3333 441120
Fax: +44 (0) 3333 441160

WALLIX USA
http://www.wallix.com
Email: sales-usa@wallix.com