Comment limiter simplement les risques de piratage informatique en entreprise ?

Comment limiter simplement les risques de piratage informatique en entreprise ?

La plupart du temps, les entreprises redoutent les cyberattaques provenant de l'extérieur. Pourtant, le personnel opérant dans les murs disposent souvent de droits d'accès excessifs par rapport à leurs rôles, et constituent le vecteur le plus probable de défaillances de sécurité, que ce soit en s'impliquant activement dans des activités malveillantes ou, plus souvent, en devenant inconsciemment les fournisseurs de comptes piratés et des droits associés. Entre 50% et 70 % des attaques réussies sont attribués à des utilisateurs internes. D'où la nécessité d'adopter un système IAM pour gérer dans les règles de l'art les identités des utilisateurs, et surveiller en permanence leurs droits d'accès aux ressources informatiques.

En collectant l'ensemble des informations liées à la structure d'autorisations, les solutions d'Identity and Access Intelligence offrent une vue d'ensemble des droits d'accès et des risques associés. Ces solutions disposent d'une ergonomie moderne et intuitive pour explorer, manipuler et restituer les données. S'appuyer sur des analyses approfondies et exhaustives facilite très largement le contrôle et l'audit des risques, la prise de décision et la gouvernance.
Ce guide pratique revient sur les principes de base de l'Identity and Access Intelligence. Il fournit un cadre simple pour aider votre entreprise à identifier les risques associés aux utilisateurs et liés à leurs droits d'accès.

1. Analyser les données de droits d'accès et évaluer les risques associés
Les solutions d'Identity and Access Intelligence s'appuient sur les technologies de business intelligence pour collecter les données d'identités et d'accès existantes, et les convertir en informations qualitatives facilitant la prise de décision. Elles fournissent à leurs utilisateurs une vue à 360° de toutes les informations liées aux droits d'accès (utilisateurs, rôles, groupes, ressources…) qui permet de naviguer de manière active au sein de ces données. Ils pourront les analyser depuis de multiples angles et axes à l'aide d'une interface graphique optimisée. Les systèmes les plus avancés proposent des analyses prêtes à l'emploi ainsi que des analyses ad-hoc pour construire ses propres requêtes.
Les solutions d'Identity and Access Intelligence permettent également d'identifier les risques potentiels associés aux utilisateurs et liés à leurs droits d'accès : utilisateurs à haut risque, comptes orphelins, failles de sécurité… Grâce à des indicateurs de risque et de conformité, l'entreprise peut se concentrer sur l'essentiel et dispose d'une aide précieuse au pilotage. Elle est alors en mesure de corriger plus rapidement des incohérences et des erreurs d'attribution de droits, et de mieux protéger ses ressources informatiques contre des interventions non autorisées et potentiellement dangereuses. En s'appuyant sur des faits démontrés, l'entreprise dispose des moyens nécessaires pour prouver l'efficacité des procédures de contrôle mises en place.

2. Adapter les informations à chaque type d'utilisateur
Le plus souvent, les solutions d'Identity and Access Intelligence intègrent des fonctionnalités d'exploration des données, comme l'analyse verticale et transversale, qui facilitent la recherche d'information et l'obtention de réponses pertinentes. La présentation graphique et intelligible des informations est adaptée à toutes les populations de l'entreprise : administrateurs informatiques, équipes métiers, auditeurs, direction générale…
Les RSSI et les auditeurs souhaitent visualiser les données de sécurité dans le moindre détail. Ils disposent d'un outil de surveillance dynamique à 360 degrés qui leur permet de déterminer le niveau de risque et le type de risque associés à un utilisateur. Ils peuvent aussi créer des rapports ad-hoc personnalisés pour croiser les informations comme bon leur semble et visualiser les données de sécurité qui les intéressent.
Les responsables métiers ont besoin de rapports standards prêts à l'emploi pour identifier rapidement les risques liés aux habilitations de leurs équipes et se concentrer sur les zones à haut risque. Pour aller à l'essentiel, la direction générale peut accéder à des tableaux de bord reprenant les principaux indicateurs de risque pondérés et hiérarchisés. Ils offrent un point de départ synthétique vers une analyse en profondeur si nécessaire. En pilotant l'évolution des indicateurs dans le temps, les décideurs déterminent les actions correctives à mener pour réduire le niveau de risque et améliorer la gouvernance à l'échelle de l'entreprise.

3. Réaliser un examen historique complet des droits d'accès
Les systèmes les plus avancés permettent de reconstituer tous les changements de droits ayant eu lieu au préalable, grâce à une historisation des modifications. Les changements de droits sont alors identifiés, tracés et consultables en toute simplicité.
Cette fonctionnalité est précieuse pour les auditeurs, car elle leur donne les moyens d'établir des pistes d'audit et de réaliser des investigations forensiques approfondies et exhaustives. En fonction de leurs besoins, ils passent en revue les droits d'accès d'un utilisateur à une date spécifique dans le passé, ou contrôlent ses changements successifs d'habilitations pendant une période donnée. Ainsi, l'historisation des droits d'accès est une fonctionnalité nécessaire pour détecter toute modification suspecte, identifier la source d'un problème, et réduire l'impact d'une fraude.

4. Identifier les utilisateurs à haut risque
Les solutions d'Identity and Access Intelligence offrent une visibilité à la demande sur les données de droits d'accès. Les informations relatives aux risques et aux habilitations sont mises à disposition dans un format compréhensible et intelligible, ce qui facilite très largement l'identification des groupes d'utilisateurs présentant le plus haut niveau de risque.
Une des recommandations de base de l'IAM est d'appliquer le principe du moindre privilège qui consiste à limiter les droits d'accès des utilisateurs au minimum requis pour leurs fonctions dans l'organisation. C'est pourquoi l'entreprise devra se concentrer sur la surveillance des utilisateurs à risque et évaluer régulièrement la pertinence de leurs droits d'accès spécifiques… [Lire la suite]

Réagissez à cet article

Source : *Bastien Meaux, Beta Systems : Le guide pratique de l'Identity and Access Intelligence – Global Security Mag Online*