Gestion des risques d'accès : comment s'adapter aux nouveaux environnements digitaux

Le nombre de sites digitaux, d'identités et de points de contact avec les clients qu'une entreprise doit gérer a explosé ces dernières années. Parallèlement, de plus en plus de consommateurs utilisant Internet pour faire leurs achats, gérer leurs transactions bancaires et échanger des données sensibles - à la fois à des fins professionnelles et personnelles, la quantité et les types données clients que les organisations doivent protéger s'est accrue de façon exponentielle. Ces dernières doivent certes impérativement poursuivre leur transformation digitale, mais elles doivent aussi mieux gérer les données client qu'elles récoltent, stockent et utilisent. Ce qui génère pour elles de nouveaux défis et de nouveaux risques.

Au fur et à mesure que s'accélère la transformation digitale, les données client se retrouvent souvent dispersées dans différentes applications et différents répertoires. Elles sont également accédées par toujours plus d'individus par des canaux toujours plus divers. Ce qui tout à la fois met les données sous la menace de vulnérabilités de cyber sécurité et soumet l'entreprise à des risques de non-conformité aux réglementations.

Cette situation altère également la réactivité des organisations et leur capacité à s'adapter à un environnement économique en constante évolution. Lorsque leurs données client sont dispersées dans diverses applications et divers répertoires, elles ne peuvent rapidement ou facilement réagir et prendre les mesures nécessaires.

Contrôle d'accès : les attributs plutôt que les rôles

Aucun de ces risques n'est plus acceptable aujourd'hui en raison des menaces croissantes de cyber sécurité, d'un cadre réglementaire de plus en plus complexe et d'un environnement économique toujours plus concurrentiel.

Pour les éviter le plus efficacement possible, la meilleure option pour elles est aujourd'hui d'abandonner les règles traditionnelles de contrôle d'accès basées sur des rôles ou fonctions, communément appelées RBAC (Role Based Access Control), et d'adopter un contrôle d'accès basé sur des attributs (ABAC ou Attribute Based Access Control) complété par l'autorisation dynamique.

L'office des standards américain (NIST) reconnaît que la contrôle d'accès ABAC est un meilleur choix que le contrôle d'accès RBAC pour les entreprises qui doivent gérer des opérations très diverses tout en garantissant la sécurité, et en se protégeant contre les cyber menaces. Le contrôle ABAC fournit la souplesse nécessaire pour gérer des permissions d'accès provenant des situations, d'utilisateurs et d'environnements différents, tout en centralisant le contrôle des permissions.

Les limites du contrôle d'accès basé sur les rôles (RBAC)

De nombreuses organisations utilisent toujours un contrôle RBAC aux côtés de systèmes

d'authentification LDAP pour gérer les autorisations et les accès aux données. Comme son nom l'indique, le contrôle RBAC autorise l'accès aux ressources et aux informations sur la base des rôles des utilisateurs. Ces rôles peuvent être définis par des fonctions, des départements, des sites et/ou des responsabilités spécifiques.

Le contrôle RBAC peut être une bonne solution dans le cas de logiques d'accès simples et statiques. Par exemple, si l'on souhaite garantir que les managers du département marketing aient accès simplement aux outils dont ils ont besoin, un système RBAC autorise ce contrôle.

Mais en dehors de ces cas simples, un contrôle RBAC est incapable d'offrir la gouvernance et les autorisations d'accès au cas par cas nécessaires pour protéger les données client dans les environnements digitaux complexes d'aujourd'hui.

Quelle que soit la façon dont les rôles et les groupes d'utilisateurs sont définis et gérés, le contrôle RBAC doit s'appuyer sur les applications elles-mêmes pour décider ce qu'un utilisateur peut ou ne peut pas faire. Cette approche est risquée car elle s'appuie sur le rôle de l'utilisateur comme contexte unique pour les décisions d'accès. Il est certes théoriquement possible d'intégrer d'autres données contextuelles, telles que la géolocalisation, le type de terminal utilisé ou des préférences de consentement au contrôle RBAC pour réduire cette vulnérabilité, mais il s'agit d'une opération coûteuse et fastidieuse.

ABAC : un contrôle d'accès modulaire, flexible et en gestion centralisée

Les solutions de contrôle ABAC adoptent une approche beaucoup plus souple pour les décisions d'autorisation, en permettant à des informations supplémentaires (c'est-à-dire les attributs) d'informer les politiques d'accès. En allant au-delà des simples rôles, le contrôle ABAC autorise l'utilisation d'attributs granulaires, dont des attributs contextuels, pour autoriser l'accès des individus au cas par cas.

Le principe clé du contrôle ABAC est qu'il n'est plus possible d'avoir des règles d'accès statiques pour chacune des applications, distribuées et dupliquées dans toute l'entreprise. Au lieu de cela, les règles d'accès doivent être basées sur des attributs définis au cas par cas.

Mais allant encore plus loin, l'autorisation dynamique suppose que les seuls attributs ne sont pas suffisants, et que le contexte de la demande en temps réel doit aider à prendre de meilleures décisions d'accès.

Optimiser le contrôle ABAC avec l'autorisation dynamique

L'autorisation dynamique est un complément du contrôle ABAC qui est encore plus précis et granulaire. Elle assemble les attributs clés qui doivent être pris en compte au moment de la transaction et évalue la validité de la demande d'accès en temps réel. Ceci à la différence de nombreuses solutions ABAC qui sont certes capables de prendre en compte n'importe quel attribut mais nécessitent une logique extérieure pour les agréger et les exploiter.

Bien que dans les deux cas, le critère pur évaluer la validité de la transaction soit inscrit dans des règles centralisées, l'ajout de l'autorisation dynamique aide les solutions ABAC à aller plus loin en créant des interfaces ergonomiques qui permettent aux administrateurs de construire et de tester rapidement et facilement des règles tenant compte de nombreux attributs contextuels, et ainsi de

garantir que les bonnes personnes aient accès aux bonnes ressources au bon moment.