Transformer la charge de la conformité en avantage concurrentiel

Les services bancaires ne se limitent plus aux quatre murs d'une agence. En France, 40 % des consommateurs utilisent désormais une application bancaire. Ce chiffre monte à 75 % chez les 25 à 34 ans, public de plus en plus habitué à la facilité d'accès et aux commodités attenantes.

Mais cela n'est pas sans inconvénients. Les fonctionnalités mobiles, l'intégration de la blockchain et l'émergence de la banque en tant que service ont conduit à un nombre croissant de cybermenaces pour les organisations, mais aussi à une charge plus importante des exigences de conformité. Le RGPD aurait généré 182 millions d'euros d'amendes rien qu'en 2020 - en plus de l'évolution des réglementations de la FCA (Financial Conduct Authority, autorité de régulation dédiée).

Cependant, le respect des exigences de conformité ne doit pas nécessairement être une lourde perte de temps. Avec la bonne technologie en place, cela peut signifier un avantage concurrentiel - en rationalisant les opérations, en favorisant l'efficacité et en comblant les lacunes en matière de sécurité. L'utilisation de la sécurité de l'identité, qui permet d'automatiser les processus et les autorisations en fonction de l'évolution des rôles et des responsabilités, est essentielle à cet égard.

Risque élevé

Les services financiers ont l'un des taux les plus élevés de violations de données par des initiés, qui ont généré un coût de 14,5 millions de dollars rien que l'année dernière. Qu'il s'agisse d'un employé mécontent agissant dans une intention malveillante ou d'un employé cliquant accidentellement sur un lien sans méfiance, le niveau d'accès du personnel aux informations sensibles d'une entreprise en fait une vulnérabilité potentielle.

Cette menace est d'autant plus grande que le secteur bancaire est particulièrement sujet à des structures d'entreprise complexes et à des cloisonnements départementaux - autant d'éléments qui entravent la visibilité d'une organisation sur les différents rôles, responsabilités et accès aux données. Si l'on ajoute à cela la dépendance continue du secteur à l'égard des feuilles de calcul et des processus manuels pour le suivi de l'accès aux données et des identités des utilisateurs, on obtient la recette parfaite pour les inexactitudes et les incohérences.

En plus de créer un cauchemar en matière d'audit et de reporting, cela crée des failles dans le système qui peuvent être exploitées par des acteurs de la menace désireux de mettre la main sur les actifs lucratifs du secteur.

Séparation des tâches

Le contrôle de l'accès est également essentiel étant donné l'importance de la séparation des tâches dans les services bancaires et financiers pour réduire le risque d'erreur et de fraude. Aucun individu ne peut contrôler plus d'une partie de la transaction. Par exemple, un employé ne peut pas à la fois créer et payer des factures. Empêcher l'accès à une ou plusieurs de ces activités est crucial pour prévenir le détournement de fonds.

La séparation des responsabilités est un concept bien ancré, mais dans la réalité, elle peut s'avérer

difficile. Les banques définissent généralement des rôles qui ne peuvent pas se chevaucher, mais avec le nombre croissant d'applications et de systèmes, l'administration peut devenir complexe et source d'erreurs. Sans parler du personnel qui passe d'un rôle à l'autre par le biais de promotions et de transferts latéraux, ce qui peut entraîner une "sur-autorisation" ou une "dérive des droits". Si l'on ajoute à cela les différents logins pour les diverses licences et abonnements auxquels différents employés ont accès au cours de leur carrière dans une organisation, la situation peut rapidement devenir incontrôlable, ce qui accroît la vulnérabilité des systèmes à l'exploitation.

L'identité est le nouveau périmètre

La mise en place de conditions d'accès appropriées doit être une priorité absolue pour les organisations. Il s'agit non seulement de se protéger contre les cybermenaces, mais aussi de satisfaire aux exigences de conformité et de rationaliser les opérations. Pour y parvenir, les institutions financières doivent disposer de la bonne technologie qui leur offre une visibilité sur qui a accès à quelles informations et quand.

Grâce à la sécurité de l'identité alimentée par l'IA et l'apprentissage automatique, les processus peuvent être automatisés et l'accès accordé selon le principe du besoin de savoir uniquement, en fonction des rôles et des responsabilités des personnes - ni plus, ni moins. Un système automatisé peut non seulement trouver et désactiver les comptes d'ex-employés, mais aussi rectifier l'accès des utilisateurs existants qui n'est plus approprié, en fonction des mouvements au sein d'une organisation. Il est essentiel de pouvoir découvrir rapidement les menaces potentielles et d'en atténuer les effets, par exemple en identifiant et en mettant fin à un comportement inhabituel et suspect, à l'image d'un utilisateur non autorisé qui tenterait d'accéder à des fichiers sensibles.

Garder une longueur d'avance

L'automatisation réduit également la charge des tâches manuelles répétitives, libérant ainsi les équipes informatiques qui peuvent se concentrer sur des activités à forte valeur ajoutée plutôt que de trier les réinitialisations de mots de passe ou les accès supplémentaires aux données. À ce titre, elle constitue donc une solution rentable. L'automatisation garantit l'exactitude et l'exhaustivité des ensembles de données, qui sont essentielles pour assurer la conformité.

Ainsi donc, le respect des exigences de conformité ne doit pas être un casse-tête pour les organisations. Grâce à la sécurité des identités, garder le contrôle peut se traduire par un avantage concurrentiel à plus d'un titre : protéger le périmètre de l'entreprise, rationaliser les opérations et garantir que toutes les données et tous les utilisateurs sont correctement comptabilisés.