Cloud : cinq conseils pour réussir un projet de gouvernance des identités

A l'heure ou 3 entreprises sur 5 s'attendent à subir une violation des données dans les mois à venir, la sécurité des données en entreprise est devenue plus qu'une priorité.

Dans un objectif d'une meilleure gouvernance des entreprises, l'accent est mis sur la traçabilité des décisions prises par les salariés de l'entreprise et donc, par extension, sur les droits et autorisations donnés aux utilisateurs du Système d'Information (SI). Dans ce contexte, la gestion des identités et des accès (IAM, Identity and Access Management) est un élément clé de sécurisation du SI. Si votre entreprise envisage de transférer des technologies critiques telles que la gestion des identités dans le cloud, certains facteurs sont à prendre en considération, comme l'évaluation et la sélection de la solution optimale de gouvernance pour votre organisation.

Etape n° 1 : identifier vos besoins en IAM d'un point de vue global

Qu'il s'agisse d'une mise en oeuvre initiale ou d'une transition depuis une solution IAM existante sur site, il est nécessaire d'analyser toutes les conditions dans lesquelles vos activités se déroulent. Il peut être tentant de démarrer le programme de gouvernance des identités à l'aide d'une solution tactique comme l'outil SSO (Single Sign-On) afin de fournir des services simples aux utilisateurs. Un outil comme le SSO résout un problème essentiel côté utilisateurs, mais ne répond pas aux besoins de votre entreprise en termes de sécurité et de conformité aux exigences réglementaires. Plutôt que de résoudre les problématiques à court terme, il est indispensable d'adopter une vision holistique de l'entreprise et de raisonner sur le long terme pour répondre à la problématique suivante : à quoi devrait ressembler votre système idéal et comment doit-il fonctionner ?

Afin d'atteindre vos objectifs de sécurité, de conformité et de croissance commerciale, il faudrait commencer par établir un plan clair, démontrant comment l'ensemble des services de l'IAM vont répondre aux besoins de l'entreprise. Il faut ensuite choisir et intégrer des solutions qui répondent à la plupart des services dont l'entreprise a besoin. Si plusieurs solutions sont choisies, il est important d'évaluer leurs compatibilités en amont pour éviter une lourde tâche d'intégration. Une approche globale vous permettra d'éviter de vous confronter à ce type de problème par exemple.

Etape n° 2 : préparer les bases du projet de gouvernance

Débuter le projet avec des données d'identités bien gouvernées soutiendra et renforcera tous les composants de votre solution d'IAM au fur et à mesure de leur déploiement. Même si votre entreprise a déjà investi dans un programme d'IAM, il n'est pas trop tard pour établir les bases de votre gouvernance. Par exemple, si l'entreprise a commencé à normaliser la gestion des accès dans le cadre d'une offre PaaS (Platform-as-a-Service), cela ne doit pas empêcher d'établir une stratégie de gouvernance des identités. Au contraire, cela accentue la nécessité de déterminer rapidement « qui doit avoir accès à quoi » selon les besoins commerciaux et la politique opérationnelle.

Grâce au déploiement d'une gestion des accès existants selon un modèle de gouvernance sécurisée, vous avez la certitude que les « bons » utilisateurs ont le « bon » accès, au « bon » moment. La plateforme d'IAM doit non seulement répondre à l'intégralité des exigences de l'organisation, mais aussi lui permettre d'accéder à l'ensemble de ses ressources.

Etape n° 3 : des solutions ouvertes et extensibles

La gouvernance des identités étant un fondement critique de la gestion des identités, il est important de sélectionner une solution facilitant l'interopérabilité et dotée d'outils et de technologies complémentaires. Une architecture ouverte permet aux solutions de gouvernance des identités de travailler de manière complémentaire avec d'autres composants opérationnels, de sécurité et d'infrastructure pour que les décisions prises soient conformes aux règles, lorsqu'il s'agit d'accorder ou de modifier un accès, de modifier des mots de passe, et de fournir une visibilité de l'accès utilisateur à l'échelle de l'entreprise.

Etape n° 4 : configurer plutôt que personnaliser

S'il est vrai que la personnalisation permet de modeler un logiciel en fonction de besoins spécifiques, elle peut aussi retarder le déploiement de l'IAM de façon significative, augmenter les coûts de mise en oeuvre de manière exponentielle et être très difficile à mettre à niveau ou à ajuster selon l'évolution des besoins de l'entreprise. Éviter la personnalisation est l'un des principes clés des solutions SaaS de nouvelle génération. C'est pourquoi les véritables solutions de gouvernance des identités basées dans le cloud sont conçues pour minimiser la personnalisation au bénéfice d'une configuration efficace. Combiner un jeu par défaut de bonnes pratiques prêtes à l'emploi dès le premier jour, avec la bonne solution apportera à l'entreprise une plus-value immédiate et évitera les personnalisations chronophages qui peuvent freiner vos projets.

Etape n° 5 : s'assurer que la solution réduira vraiment le TCO

L'une des raisons principales pour lesquelles les entreprises choisissent une solution basée dans le cloud est la réduction du coût total de possession, le TCO (Total Cost of Ownership). Avec les solutions SaaS, vous payez un abonnement mensuel ou annuel aussi longtemps que vous utilisez la solution, ce qui vous permet de diminuer sensiblement les coûts d'acquisition et de déploiement du projet. Les frais d'infrastructure, de maintenance et de mises à niveau étant supportés par le fournisseur SaaS, l'entreprise peut complètement éliminer le coût du logiciel et du matériel de la plate-forme, de l'infrastructure réseau, des outils de surveillance de tierce partie, des outils de test et des produits de sécurité.

Le rythme d'adoption du cloud en entreprise ne cesse de s'accélérer, et Gartner estime même que 90% des entreprises auront un environnement hybride dans les années à venir. Le cloud change notre façon de travailler - les employés peuvent désormais travailler d'où ils veulent, sur le périphérique de leur choix - mais cela présente aussi quelques nouveaux défis. Ces utilisateurs - les identités - sont ceux qui ont accès aux informations sensibles d'une organisation, et c'est sur eux que vous devez centrer votre sécurité. L'identité est ce qui alimente le cloud et qui permet aux organisations d'adopter de nouvelles technologies sécurisées tout en étant toujours capables de voir et de contrôler intégralement qui a accès aux informations sensibles, et quelles genres de données sensibles. Si la gouvernance des identités émane du cloud lui-même, elle apporte la sécurité, la

conformité et l'automatisation cruciales dont les organisations ont besoin, tout en offrant tous les avantages d'une solution basée dans le cloud. Qu'il s'agisse de gagner en compétitivité, de rechercher de nouvelles opportunités de croissance ou d'offrir une meilleure expérience aux clients, les bénéfices apportés par la gouvernance des identités permettent aux entreprises d'envisager leur avenir, en toute confiance.