Gestion des identités et des accès : l'importance de l'expérience client en environnements mixtes

Selon IDC, la pandémie du Covid-19 accélère la transformation numérique des entreprises. L'analyste prévoit une augmentation de 64 % des dépenses totales en matière d'infrastructures informatiques sur cinq ans. Lorsqu'une entreprise a besoin de déployer une solution informatique, les décisionnaires pèsent généralement les pour et les contre d'un développement en interne par rapport à l'achat d'un logiciel existant.

Dès lors, pour chaque fonctionnalité souhaitée dans sa pile technologique, une organisation doit décider s'il est préférable de développer la solution en interne, ou au contraire d'opter pour une solution externe, via un fournisseur tiers. Ce dernier gère ainsi ses outils, qu'il s'agisse de plateformes de communication à destination des équipes, ou de solutions de gestion des identités et des accès (IAM).

Or, pour de nombreuses entreprises, l'approche « développement vs achat » n'est pas nécessairement une réalité. Elles travaillent, la plupart du temps, avec une architecture traditionnelle qui combine de manière personnalisée un ensemble d'applications achetées et développées sur mesure, et évoluent donc en environnements mixtes.

La gestion des identités et des accès (IAM) comme facilitateur

Dans un environnement hybride, il peut se révéler difficile de garantir une expérience client sans couture ; la multiplication des applications dans une architecture augmentant les risques de perturber l'expérience de l'utilisateur. Par ailleurs, l'identité est répartie sur des plateformes et des dispositifs différents afin de garantir aux utilisateurs la possibilité de se connecter n'importe où et à partir de n'importe quel appareil.

Dès lors, il est particulièrement important de prendre en charge « l'identité fédérée » qui est liée à l'authentification unique (SSO) et permet de joindre l'identité électronique et les identifiants d'une personne stockés dans plusieurs systèmes de gestion d'identité distincts.

L'IAM allège ainsi les contraintes des entreprises qui peinent à gérer les identités en environnements mixtes. Son déploiement leur permet alors d'accroître la sécurité, de travailler plus efficacement et d'offrir une expérience client sans heurts, quels que soient les défis à venir et les freins inattendus.

Grâce à une solution IAM flexible, les équipes disposent de l'accès et des informations dont ils ont besoin pour accélérer l'innovation, et offrir plus de possibilités aux utilisateurs tout en renforçant un dispositif de sécurité existant. La gestion de l'identité améliore ainsi durablement la sécurité

d'un système informatique et permet de résoudre les problèmes d'identité actuels et futurs.

La personnalisation des environnements

Afin de répondre à l'évolution rapide des cas d'usages actuels, les entreprises sont invitées à ajouter une fonctionnalité moderne et novatrice à leur pile technologique. En conséquence, ce service est complété par l'intermédiaire de fournisseurs de micro-services tiers, notamment des sociétés de logiciels en tant que service (SaaS) basées sur le cloud.

Lorsqu'en parallèle, un environnement d'origine alimente une entreprise, les avantages d'une migration complète vers le cloud sont considérables mais impliquent d'éventuelles perturbations. La personnalisation apparaît donc comme la solution intermédiaire qui pallie la plupart des difficultés rencontrées sans pour autant engendrer des problèmes supplémentaires.

Les entreprises peuvent bénéficier de personnalisations qui s'intègrent facilement à leur système existant, ce qui leur permet d'augmenter leurs recettes et leur donne le temps d'adapter leur stratégie et de parvenir à un consensus, avant de passer à une transformation numérique à grande échelle. Ainsi, une solution adéquate, telle que l'IAM, permet de réduire au minimum les perturbations subies par les utilisateurs et les clients lors d'un changement de plateforme, ou tout autre transition, ce qui limite le roulement et les occasions manquées avec leurs clients.

Pour aller plus loin, la mise en œuvre d'une stratégie d'identité permet de clarifier les actions engagées par l'entreprise, à savoir saisir la structure et les besoins imposés dans une activité.
L'IAM encourage une meilleure logique commerciale tout en intégrant l'innovation au cœur même de la stratégie de l'organisation.

De surcroît, la création d'un produit flexible, extensible, personnalisable et réactif aux transformations, offre également la possibilité d'adopter cette approche pour les communications les plus sensibles. Lorsque les dirigeants fixent des objectifs commerciaux, il est alors possible de les réaliser rapidement, grâce à une solution d'identité qui accélère la mise sur le marché des produits.

Les logiciels soutiennent les processus opérationnels, et non l'inverse

Ces outils devraient appuyer les fonctions essentielles d'une entreprise. Par exemple, un fournisseur d'identité en tant que service (IDaaS) aide les entreprises à disposer des fonctionnalités et de l'extensibilité nécessaire leur permettant d'atteindre les objectifs de gestion du temps, tout en économisant les ressources mises à contribution lors de la résolution de problèmes. L'IAM offre la possibilité d'évoluer rapidement en fonction des besoins, tandis qu'une solution d'identité clé en main ou une plateforme d'authentification interne connaît, pour sa part, des limites.

Si le fait de confier son identité à un fournisseur d'IDaaS a une forte valeur commerciale, il ne faut toutefois pas négliger le pouvoir du code. En effet, une approche combinant l'IDaaS et le code offre le meilleur des deux mondes : des services d'identité gérés par un service facile à utiliser, auxquels

s’ajoutent les mêmes possibilités de personnalisation et de contrôle qui seraient proposées si l’ensemble de la solution avaient été codées de A à Z.

Les entreprises sont aujourd’hui submergées par des enjeux technologiques, ainsi elles doivent protéger leurs systèmes informatiques des intrusions tout en poursuivant leur transformation numérique. Il est donc essentiel qu’elles mettent en place des solutions sécuritaires, non chronophages, qui garantissent une expérience utilisateur protégée et optimale.