# Tribune : Entreprise « trop étendue » ? Faites évoluer votre gestion d'identité

L'adoption rapide des appareils mobiles et des services cloud, combinée à la multiplication des partenariats et des applications clients, a repoussé les limites de l'identité dans les entreprises. Pour l'entreprise étendue, l'identité et la gestion d'accès (*Identity and Access Management*, IAM) va au-delà de la simple attribution d'une identité aux collaborateurs et d'un accès approprié aux ressources de l'entreprise.

Il s'agit en fait de la capacité à superviser les accès aux ressources des différentes populations – collaborateurs, partenaires et consommateurs – et à protéger les nombreuses ressources sensibles de l'entreprise (dont les données) qui peuvent résider dans ou à l'extérieur des locaux de l'organisation, tout en aidant à protéger l'entreprise contre des actes de cybercriminalité toujours plus sophistiqués et des fraudeurs toujours plus imaginatifs.

Malheureusement, les approches traditionnelles de l'IAM ne fonctionnent pas parce qu'elles ne sont pas en mesure de gérer les accès des consommateurs. Elles ne sont pas capables d'accompagner la rapide adoption des services cloud ou encore de sécuriser l'échange de données entre les différentes populations d'utilisateurs et n'offrent aucune aide pour se prémunir contre les nouvelles menaces.

Chez Forrester, nous avons construit un modèle « Zéro Confiance » (*Zero Trust Model*) relatif à la sécurité des informations. Ce modèle élimine la distinction entre les réseaux internes fiables et les réseaux externes non-fiables, et exige des professionnels de la sécurité de vérifier et de sécuriser toutes les ressources, de limiter et de strictement appliquer les contrôles d'accès et de surveiller et de tracer l'ensemble du trafic des réseaux.

**Zero Trust s'applique également parfaitement à la gestion des identités**. Il exige des professionnels de la sécurité de 1) se concentrer sur les applications et données sensibles, 2) unifier le traitement des accès des partenaires commerciaux, des différentes populations d'utilisateurs et des modèles externalisés et 3) se préparer pour l'interaction à l'échelle d'Internet. Appliquer le modèle Zero Trust Identity vous aide non seulement à améliorer l'agilité de votre entreprise et son respect des législations, mais peut aussi vous aider à renforcer l'expérience client et à faire avancer la stratégie de monétisation de votre organisation.

Le livre blanc **« Playbook Identity and Access Management » de Forrester** vous aidera à passer d'un modèle handicapé par le manque de souplesse généré par le lien entre authentification et contrôles d'accès, à une approche où vous déployez des services produisant et consommant des identités et des informations sur la base d'un couplage lâche. Elaborer une stratégie Zero Trust IAM pour une entreprise étendue exige un processus en quatre étapes :

1. **Découvrir** : identifier les tendances, justifier votre étude de cas et évaluer votre degré de maturité. Comprendre les objectifs métier de votre entreprise et ce que vous pouvez faire avec une approche Zero Trust IAM vous aidera à construire un scénario d'usage intégrant les bénéfices métiers, financiers et opérationnels. Une fois votre étude de cas bien

définie, évaluez vos capacités actuelles par rapport à votre scénario et identifiez vos lacunes pour mettre en place votre stratégie.

2. **Planifier** : élaborer une stratégie pour gérer l'IAM dans la durée. Pour que cette stratégie devienne réalité, vous devez identifier et influencer les parties prenantes tant du côté métier qu'informatique. Vous devez également documenter votre stratégie IAM et y inclure une description de la situation actuelle, une définition de votre projet, une feuille de route détaillée et vos recommandations sur la séquence de projets à mener pour faire de la stratégie une réalité.
3. **Agir :** recruter les bonnes ressources, gérer les règles, et implémenter les capacités IAM. Parce que les professionnels de l'IAM doivent souvent communiquer avec des utilisateurs issus des métiers, ils doivent détenir des compétences en matière de communication en plus de leurs connaissances techniques de l'IAM. Et parce que l'IAM couvre un spectre très large et demande une puissante gouvernance centrale, vous allez devoir recruter plusieurs types de professionnels de l'IAM, dont un VP ou quelqu'un à un niveau de direction, un architecte IAM et des techniciens de l'IAM. Vous aurez également à décrypter les avantages et inconvénients d'une multitude de solutions sur site et dans le cloud pour répondre à vos exigences techniques.
4. **Optimiser** : mesurer, contrôler et promouvoir les résultats de l'IAM. Vous aurez à mesurer et à contrôler l'efficacité de votre programme IAM et à diffuser les résultats en interne. Grâce à des métriques, les responsables IAM seront mieux préparés pour démontrer la valeur ajoutée du projet pour l'entreprise, développer une culture proactive, et aligner les priorités et le système de primes de performance avec la stratégie de l'entreprise. Vous serez également en meilleure position pour comprendre comment votre programme performe comparé à ceux de vos pairs.

Vous pouvez télécharger le résumé complet du playbook ici.

**Voir aussi**

Silicon.fr en direct sur les smartphones et tablettes