Concevoir un programme de gestion des identités et des accès optimisé pour votre entreprise

Quatre étapes clés pour gagner en maturité dès aujourd'hui

Points clés :

La gestion des identités et des accès nécessite une approche mûrement réfléchie pour pouvoir atteindre les objectifs de sécurité, de conformité ou de productivité, aussi bien à court terme qu'au fur et à mesure de l'évolution de l'entreprise.

Table des matières

Introduction

Dans les environnements informatiques complexes et distribués actuels, les programmes de gestion des identités et des accès (IAM) font plus que gérer les identités des utilisateurs et accorder des accès. De ce fait, peu d'initiatives informatiques ou de sécurité demandent une telle réflexion et un tel examen.

Un programme d'IAM réfléchi, optimisé pour les objectifs d'une entreprise et sa situation, permet de réduire le risque de violations des données impliquant les identités. Il peut favoriser la productivité et la collaboration, générant de ce fait un réel avantage concurrentiel sur le marché. De plus, il permet de veiller au maintien d'une bonne gestion de la conformité réglementaire, tout en réduisant les coûts liés à la réalisation d'audits.

Malheureusement, bon nombre d'entreprises ne parviennent pas à atteindre un ou plusieurs de ces objectifs car leurs programmes d'IAM ont été développés au fil du temps à l'aide de solutions technologiques qui les rendent hétérogènes, peu évolutifs et incomplets. Résultat : les entreprises s'exposent à un risque de pertes considérables et ne disposent pas de l'avantage concurrentiel qu'offre une force de travail agile et connectée.

Mener une réflexion approfondie sur un programme d'IAM existant peut générer des bénéfices ayant un impact positif direct sur les performances de l'entreprise et sa sécurité. Cette approche peut réduire les coûts via l'automatisation, améliorer l'efficacité opérationnelle grâce à un cadre technologique intégré et favoriser la réussite des mises en œuvre grâce à une planification appropriée.

60 % des attaques sont réalisées par des utilisateurs internes

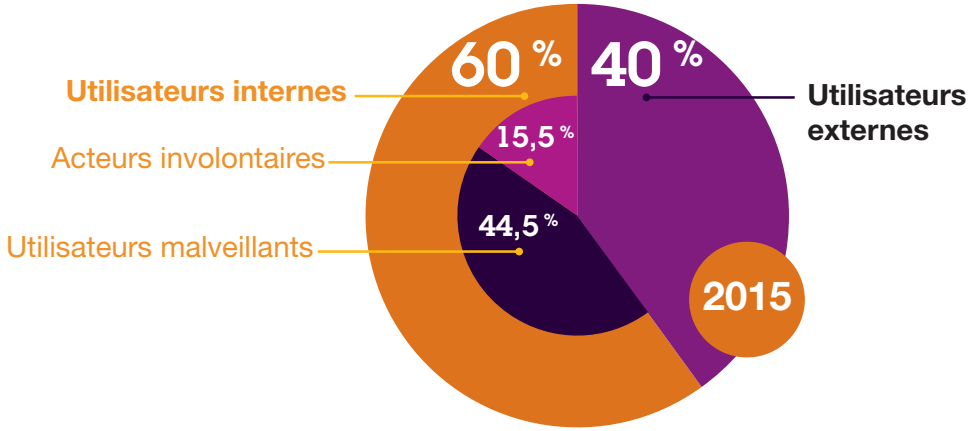

Figure 1 : Qui sont les utilisateurs malveillants ?

Aller au-delà d'une vision manichéenne

Les solutions d'IAM actuelles doivent faire plus que « laisser les gentils entrer et garder les méchants dehors ». En effet, les violations de sécurité découlent de plus en plus souvent des actions des utilisateurs internes, qu'elles soient intentionnelles ou non. Lorsque les collaborateurs communiquent leurs mots de passe ou perdent des données d'entreprise, ou que des tiers mettent des informations en danger en raison de protections inappropriées, même les utilisateurs de bonne foi mettent la sécurité en péril.

Un rapport IBM® X-Force® a révélé que les utilisateurs internes étaient responsables de 60 pour cent des attaques étudiées.[1] Sur ce chiffre, 15,5 % en étaient des acteurs involontaires. Souvent « recrutés » à leur insu par d'autres utilisateurs aux intentions malveillantes, ils jouent alors un rôle important dans des attaques extrêmement dommageables, et potentiellement prolongées. Et comme ce sont des utilisateurs internes, ils agissent sans lever le moindre doute, en se connectant sur un réseau social à partir d'un dispositif relié au réseau d'entreprise ou en ouvrant un e-mail provenant d'un contact professionnel paraissant légitime.

Les 44,5 pour cent restants sont des utilisateurs internes malveillants, dont les actions ne sont pas du tout innocentes. La vérité, aussi déconcertante soit-elle, est que ce n'est pas parce qu'il s'agit d'utilisateurs internes qu'ils sont au-delà de tout soupçon. Il est donc important de garder à l'esprit que les situations et les relations changent au fil du temps, et pas toujours pour le mieux.

1 IBM Cyber Security Intelligence Index 2016 http://www-03.ibm.com/security/data-breach/cyber-security-index.html

Les piliers d'un programme d'IAM réfléchi

Un programme d'IAM, optimisé pour les besoins spécifiques à chaque entreprise, aide à renforcer les capacités de gestion de la conformité réglementaire, à accorder un accès simple aux utilisateurs autorisés et à protéger les données de valeur. Chaque entreprise aura des exigences différentes en termes de maturité technologique, et donc des programmes d'IAM distincts.

Néanmoins, tous les programmes d'IAM couronnés de succès partagent un trait commun : l'assurance des identités, les renseignements sur les identités et la gouvernance dont ils disposent fonctionnent de façon intégrée et cohérente dans l'environnement informatique d'une entreprise. Par conséquent, une entreprise peut atteindre des niveaux appropriés de contrôles d'accès et de sécurité sans nuire à la productivité des utilisateurs ni leur imposer des expériences de connexion pénibles.

Optimisation de l'assurance des identités dans un monde à plusieurs périmètres

De nombreuses entreprises continuent à s'appuyer sur de simples mots de passe comme preuve d'identité. Mais les mots de passe sont statiques et intrinsèquement faibles. Les utilisateurs sont généralement partisans du moindre effort et optent pour des mots de passe simples à retenir qui peuvent être facilement volés, craqués ou compromis, ce qui expose un système à des attaques frauduleuses. Dès lors qu'un attaquant déchiffre un mot de passe statique, c'est ensuite un jeu d'enfant de se faire passer pour l'utilisateur d'origine et d'accéder à de nombreux types de données confidentielles. Étant donné que de nombreux utilisateurs se servent d'une connexion unique ou réutilisent le même mot de passe sur différents systèmes d'entreprise, les données stockées dans des applications se trouvant loin de la violation initiale peuvent également être compromises. Les mots de passe statiques sont également vulnérables à de nombreuses attaques par hameçonnage et par cheval de Troie.

Pour éviter les accès frauduleux, les utilisateurs doivent pouvoir prouver leur identité en contexte. Ce contexte peut concerner le type de dispositif dont ils se servent, leur emplacement ou leur modèle d'activité. Les technologies de sécurité les plus récentes peuvent se servir de ces informations contextuelles pour déterminer si un utilisateur spécifique est autorisé à accéder à telle ou telle ressource.

En s'appuyant sur les analyses de données contextuelles pour analyser les risques, les entreprises peuvent concéder un accès en fonction d'une évaluation dynamique de la transaction et de l'utilisateur en question. Par exemple, si une employée américaine utilise tout à coup son dispositif mobile en Afrique, le logiciel détecte un changement inhabituel dans le contexte et peut demander à l'utilisatrice de présenter une autre preuve d'identité, comme un mot de passe ponctuel. Dans certaines situations, l'utilisateur peut se voir refuser l'accès à certaines ressources informatiques car le risque de sécurité est estimé trop élevé.

En demandant à un utilisateur de s'authentifier de plusieurs façons, l'entreprise veille à ce qu'il ait accès aux ressources protégées appropriées, et que ces ressources soient protégées des utilisateurs qui ne devraient pas y avoir accès. Outre le renforcement de la sécurité d'une demande d'accès, l'utilisation du contexte permet aussi de fluidifier l'expérience de l'utilisateur final, tout en favorisant sa productivité. Dans les tentatives à faible risque, l'expérience de l'utilisateur peut ne subir aucune variation.

L'assurance des identités des utilisateurs peut être renforcée en combinant différentes méthodes d'authentification, de la biométrie à la notification push optimisée pour mobile, en passant par les jetons matériels, avec un moteur de règles sophistiqué ou, dans l'idéal, un moteur de risques. Un moteur de règles permet aux administrateurs de définir des règles spécifiques pour chaque demande d'accès, et implique un long cheminement pour assurer des identités vérifiées. Un moteur de risques va plus loin : lorsqu'un utilisateur demande d'accéder à une ressource protégée, le système calcule un score de risque et détermine si l'accès est autorisé, refusé ou permis sous condition.

Intégration des renseignements sur l'identité au processus

Les menaces de sécurité deviennent de plus en plus sophistiquées et les pressions concernant les risques et la conformité continuent à s'accroître. C'est pourquoi les entreprises recherchent de plus en plus une nouvelle approche proactive à la gestion des identités, une approche qui intègre véritablement le contrôle des risques. Les solutions actuelles les plus efficaces en matière de gestion des identités combinent une gestion des droits d'accès à un contrôle des privilèges et des renseignements de sécurité « en contexte ».

Intégration avec la gestion des identités privilégiées

Un identifiant privilégié désigne tout compte disposant d'autorisations spéciales ou supplémentaires pour accéder aux ressources d'entreprise, telles que les serveurs, les dispositifs réseau, les systèmes de base de données et les applications de planification des ressources d'entreprise. La menace de compromission que font peser les attaquants sur un identifiant privilégié représente bien évidemment un grand risque. Seulement, ce risque ne s'arrête pas là. Les utilisateurs autorisés disposant de comptes privilégiés peuvent également mettre en péril la sécurité de l'infrastructure informatique. En parallèle, les entreprises délèguent davantage de tâches administratives au personnel et aux sous-traitants, ce qui ouvre la voie à une exposition accrue des comptes privilégiés.

Les utilisateurs autorisés disposant de comptes privilégiés peuvent également mettre en péril la sécurité de l'infrastructure informatique.

C'est pourquoi, il est primordial que les entreprises :

- établissent les priorités concernant les identités privilégiées ;
- identifient et surveillent les utilisateurs présentant les risques les plus élevés ;
- sachent qui a accès aux systèmes et aux données sensibles ;
- définissent un comportement normal de référence.

Pour satisfaire ces exigences, le moyen le plus pratique est d'utiliser un système sophistiqué de gestion des identités qui permette au personnel informatique de partager les identifiants privilégiés. Il est impératif que ce système intègre les éléments suivants :

- un coffre de données d'identification pour stocker les données d'identification des comptes privilégiés en toute sécurité ;
- un mécanisme d'extraction/restitution permettant à un utilisateur privilégié d'extraire un identifiant (avec un mot de passe) pour une utilisation exclusive pendant une période de temps limitée, si nécessaire, puis de restituer cet identifiant une fois terminé, et le mot de passe changera alors automatiquement ;
- un moyen d'assurer la mise à disposition et la gestion centralisées des identifiants sur plusieurs ressources ;
- les rôles et les stratégies indiquant les relations utilisateurs/identifiants ;
- un processus qui permette aux utilisateurs de demander accès à des identifiants et aux responsables d'approuver les demandes ;
- des journaux d'audit intégrés qui alimentent une solution de renseignements de sécurité afin de consigner toutes les activités d'extraction/restitution et de savoir quels utilisateurs ont accédé à quels identifiants sur une période spécifique.

C'est une solution qui permet aux entreprises de :

- éviter la prolifération des identifiants privilégiés associés à leurs ressources ;
- autoriser les utilisateurs privilégiés à bénéficier d'un identifiant privilégié s'ils en ont besoin, lorsqu'ils en ont besoin et sous réserve qu'ils en aient besoin, aussi longtemps que cet identifiant leur est nécessaire ;
- rendre les utilisateurs responsables des identifiants dont ils ont été propriétaires ou qu'ils ont extraits ;
- déléguer la gestion des stratégies concernant les identifiants et les accès aux propriétaires respectifs des ressources ;
- recueillir les attributs des identités et utiliser ces données conjointement aux événements et aux règles des données de flux réseau pour fournir des renseignements de sécurité « en contexte ».

Intégration avec les renseignements sur les identités

Plusieurs solutions de renseignements de sécurité (comprenant les systèmes de gestion des événements et des informations de sécurité) peuvent fournir des fichiers journaux et des métriques utilisables aidant à identifier les anomalies, mettre en avant les comportements à risque ou inappropriés, et favoriser la génération de rapports sur la conformité. En intégrant la gestion des identités et des accès à ces solutions, les entreprises peuvent combiner ces résultats aux événements et aux données de flux réseau pour générer des renseignements de sécurité « en contexte ». Grâce à une vue étendue des activités dans les différents domaines de sécurité de l'entreprise, et en recoupant les données de gestion des identités et des accès avec d'autres événements importants de sécurité, les entreprises peuvent mettre plus rapidement au jour les comportements inappropriés ou suspects des utilisateurs (notamment les menaces internes) et réduire les temps de réponse aux menaces de façon drastique.

Satisfaction des exigences de conformité avec la gouvernance des identités et des accès

Pratiquement tous les secteurs sont soumis à des exigences de conformité à un certain niveau. Les innombrables réglementations gouvernementales du monde entier soulignent à quel point la visibilité et le contrôle sur les droits et privilèges d'accès des utilisateurs sont importants.

La sécurité et la confidentialité étant des enjeux prioritaires, notamment avec une attention renouvelée au niveau de la supervision et de la gouvernance, les mesures de gestion des risques et de conformité sont désormais pilotées au premier plan de l'entreprise. Par conséquent, les entreprises doivent prouver qu'elles disposent de contrôles d'accès solides et cohérents pour répondre à la fois à leurs propres exigences de conformité et à celles de leurs partenaires commerciaux.

Les violations de sécurité et les problèmes de conformité ont plus de risque de se produire lorsque les utilisateurs disposent de niveaux d'accès obsolètes ou inappropriés, et augmentent le risque de menaces d'initiés. Les attaquants extérieurs recherchent souvent une « proie facile » qui peine à contrôler et à gérer les accès utilisateur que les programmes offrent. Il ne s'agit pas simplement de mettre au point un programme solide de gestion des identités et des accès, encore faut-il le faire fonctionner correctement.

Étude de cas : Un leader mondial en gestion de clientèle rationalise et améliore son programme de gestion des identités et des accès

Les récentes fusions et acquisitions, accompagnées de remaniements organisationnels, ont révélé que la société avait besoin d'une solution de gestion des identités et des accès plus robuste, agile et mise en œuvre de façon cohérente.

IBM a évalué les priorités de la société et a identifié les forces et les faiblesses de sa gestion des identités et des accès, qu'elle a confronté ensuite aux normes et aux meilleures pratiques du secteur afin d'établir une feuille de route stratégique claire et adaptée pour améliorer la gestion des identités et des accès de la société.

Avec IBM Identity and Access Management Services, l'entreprise a consolidé sa gestion des identités et des accès en mettant fin aux cloisonnements administratifs grâce à la création d'un cadre commun conçu pour réduire les coûts et la complexité via l'utilisation de composants, technologies et services réutilisables, basés sur les normes. Résultat : la société était plus à même d'éviter et d'atténuer les risques de conformité.

Réduction des risques via la gouvernance
La gouvernance des identités et des accès fournit des conseils sur la définition des rôles utilisateur, ainsi que sur la mise à disposition, la gestion et l'application des accès tout au long du cycle de vie des utilisateurs.

Les solutions conçues pour gérer les exigences liées aux accès utilisateur avec responsabilité et transparence vous aident à régir et à appliquer les accès utilisateur de façon plus efficace. Ces outils peuvent aider les administrateurs à vérifier que les comptes et les privilèges des utilisateurs sont mis à jour et adaptés à leurs rôles. En outre, la gouvernance des identités et des accès peut aider les entreprises à contrôler de façon plus précise et cohérente qui peut faire quoi avec quelles ressources.

Pour tout programme de gestion des identités et des accès, une approche basée sur des règles doit inclure :

- la planification d'une stratégie ;
- la définition de normes, processus et contrôles ;
- la mise en œuvre ;
- la surveillance, la mesure et la génération de rapports sur l'efficacité.

Quand le système ne fonctionne pas

Pour bon nombre d'entreprises, les investissements dans les solutions d'IAM remontent à bien longtemps. Ces entreprises se sont ensuite efforcées de les moderniser avec plus ou moins de succès. Bien que ces mises en œuvre conséquentes constituent une bonne base et qu'elles disposent souvent d'éléments des piliers décrits ci-dessus, au fil du temps, elles ne parviennent pas à suivre l'évolution du paysage informatique des entreprises. Par conséquent, elles ne sont plus prémunies contre les menaces internes ou les fraudes d'identité, ou elles ont des difficultés pour assurer la conformité.

Plusieurs facteurs participent à ce phénomène. Souvent, les différentes fonctions métier adoptent des applications cloud de façon cloisonnée, les accès étant gérés en parallèle (parfois même sans que le service informatique ne soit au courant). De ce fait, elles ne sont pas automatiquement incluses dans le système central de gestion des stratégies. Comme les entreprises se complexifient en raison des fusions et acquisitions, des réorganisations ou tout simplement de la croissance organique, ces problèmes prennent rapidement de l'ampleur. De plus, les utilisateurs ont tous des besoins d'accès très différents. Les groupes d'utilisateurs finaux gérés par un programme d'IAM peuvent inclure des collaborateurs, des partenaires, des sous-traitants et même des clients, qui apportent parfois leurs propres dispositifs voire même leurs propres identités via leurs comptes de réseaux sociaux.

La plupart des entreprises tentent de faire face à ces changements en utilisant des solutions ponctuelles, pour répondre à chaque besoin ou défi qui se présente. Mais au fil du temps, cela conduit finalement à un système d'IAM fragmenté qui ne répond plus aux objectifs. A contrario, le fait de prendre du temps pour réfléchir à la conception d'un programme d'IAM optimisé pour des objectifs spécifiques apporte de nombreux avantages.

Une transition bien étudiée vers la maturité

La gestion des identités et des accès nécessite une approche mûrement réfléchie pour pouvoir atteindre les objectifs de sécurité, de conformité ou de productivité, aussi bien à court terme qu'au fur et à mesure de l'évolution de l'entreprise. Les entreprises peuvent voir leurs investissements dans les solutions d'IAM évoluer, passant d'une simple fonction minimale à la création d'une valeur réelle pour leurs utilisateurs et pour leurs résultats financiers.

Une approche réfléchie permet également aux entreprises d'établir les priorités de leurs feuilles de route afin de résoudre les problèmes les plus pressants. Sur le long terme, les coûts peuvent être réduits grâce au retrait des équipes des cycles de dépenses réactives.

Figure 2 : Un programme d'IAM adapté à votre entreprise prend en charge les objectifs que vous vous êtes fixés

Adaptez votre programme d'IAM à l'avenir

Optimisez votre feuille de route

Tirez le maximum de votre budget

Figure 3 : Avantages d'une approche réfléchie en termes de gestion des identités et des accès

Par ailleurs, avec cette méthode, les entreprises évitent la coûteuse erreur de passer trop vite à la sélection de fournisseurs. Les projets d'IAM impliquent un gros travail de restructuration. En ciblant trop tôt la sélection des technologies, l'attention est détournée des activités principales qui alignent étroitement les solutions d'IAM aux objectifs de l'entreprise.

Une approche réfléchie comprend trois étapes. La première consiste à **évaluer** l'état du programme actuel, en identifiant les principales lacunes de l'IAM ainsi que leur impact sur l'entreprise, et sa capacité à atteindre les objectifs métier et informatique. La deuxième étape porte sur la **conception** d'une stratégie d'IAM à exécuter pour prendre en compte les besoins à long terme de l'entreprise, ainsi que d'une feuille de route d'IAM avec des priorités, des exigences de temps et de budget, pour appliquer cette stratégie en contexte. Une fois ce travail stratégique terminé, il peut servir de base solide pour la troisième étape : l'**exécution** d'après le plan, pour regrouper les produits, processus et personnel nécessaires pour donner vie à la stratégie.

Étape 1 : Évaluation

Démarrer par l'évaluation d'un programme d'IAM existant présente de nombreux avantages. Tout d'abord, cette évaluation permet aux entreprises de réaliser un véritable bilan de santé en identifiant les vulnérabilités et les points problématiques les plus pressants, plutôt que de simplement faire ressortir les problèmes suscitant le plus d'attention. Bien que bon nombre d'entreprises se cantonnent à cette première étape, cette approche vise à aller plus loin : ces vulnérabilités ne sont pas étudiées de façon indépendante, mais bien dans le contexte d'objectifs plus élevés, en général un certain équilibre entre les exigences de sécurité, de conformité et de productivité. Cette approche concentre les efforts et la hiérarchisation des priorités sur les points problématiques les plus importants, tout en veillant à ce que les solutions déployées soient celles qui œuvrent dans le sens des objectifs de l'entreprise, en plus de résoudre les problématiques pressantes actuelles.

Par ailleurs, prendre le temps de préparer une vision pour l'avenir peut permettre à une entreprise de passer d'une position réactive à une position plus stratégique, en s'assurant qu'un système ne fait pas simplement qu'éviter les problèmes. Au lieu de faire des pieds et des mains pour corriger un programme d'IAM à chaque fois qu'un point problématique impossible à éviter se présente, il devient possible de mieux anticiper les défis à venir et de garder le contrôle.

Souvent, l'un des avantages supplémentaires de cette pratique est la capacité à articuler clairement la connexion entre le budget alloué à un programme d'IAM et un retour sur investissement significatif. Une augmentation de la productivité des utilisateurs finaux peut diminuer les coûts et accroître les revenus, et un risque réduit de violations peut être quantifié, tout comme les efforts de conformité.

Lors du développement de cette vision future, il est important de prendre en compte la situation spécifique à chaque entreprise. Les besoins fluctueront selon les types d'utilisateurs demandant un accès, le degré de variation de leurs demandes d'accès, leur nature et l'emplacement où sont stockées leurs identités. Les pressions en termes de conformité sont également très différentes d'un secteur ou d'un pays à l'autre. Les facteurs de risques de violations de données varient également en fonction des informations protégées, ce qui a donc un impact sur les obligations de sécurité.

Il appartient à chaque entreprise de décider si elle doit adopter les nouvelles tendances, et à quel rythme. Les applications Software-as-a-Service (SaaS), l'Internet des Objets (IdO), les programmes Bring your Own Device (BYOD) et Bring your Own Identity (BYOI), entre autres, proposent un ensemble presque infini d'options pour la personnalisation, ce qui permet aux entreprises d'optimiser leurs choix en fonction de leurs propres besoins et de leur propre situation.

Étape 2 : Conception

Une fois que la situation actuelle d'un programme d'IAM est clairement comprise et que la situation future ciblée a bien été définie, il est possible de concevoir une feuille de route qui définit un délai et un budget raisonnables pour passer d'une situation à l'autre.

Dans ce cadre, les ressources existantes peuvent être évaluées pour optimiser leur valeur, réduire les inefficacités et gagner en rentabilité. Un plan de déploiement des nouvelles solutions peut être mis en place, en gardant toutefois l'intégration à l'esprit de sorte que les contrôles soient appliqués de façon cohérente et que les cloisonnements de l'IAM soient supprimés. Pour sélectionner les fournisseurs et technologies adaptés lors des futurs achats, il est possible d'identifier les critères à respecter.

Résultat : une feuille de route établissant les priorités avec un calendrier clair pour veiller à ce que les technologies existantes soient exploitées et que les nouvelles technologies soient mises en œuvre dans le bon ordre. Le taux de mises en œuvre de projet réussies avec un retour sur investissement positif n'en sera que plus élevé.

Étape 3 : Exécution

A ce stade, le temps passé et le soin apporté à l'évaluation du programme d'IAM actuel et à la conception de l'état futur répondant aux exigences de l'entreprise portent leurs fruits. Les propositions de projet et de dépenses peuvent être approuvées plus rapidement et plus facilement, étant donné que les demandes disposent d'une structure et d'une finalité qui les relient aux impératifs globaux de l'entreprise. Par ailleurs, il existe désormais des mesures claires et quantifiables de succès pour chaque déploiement et chaque mise en œuvre. Pour finir, les coûts de déploiement des produits d'IAM peuvent être considérablement réduits, car les exigences et les processus métier sont pleinement compris et simplifiés au fil du temps.

Avec l'adhésion, les attentes et la préparation appropriées, il est possible de procéder méthodiquement au rassemblement des collaborateurs, processus et technologies nécessaires à l'exécution réussie de la stratégie.

Étape 4 : Agir maintenant

Bien qu'un grand nombre d'entreprises aujourd'hui disposent de stratégies à long terme pour protéger leurs systèmes, applications et données, des accès non autorisés, celles-ci ne sont souvent pas exhaustives. Toutefois, maintenant que la problématique des identités est clairement apparue comme un enjeu de sécurité, qui nécessite des contrôles pour gérer, appliquer et surveiller les droits d'accès et les accès des utilisateurs, il est temps de prendre des mesures.

IBM Identity and Access Management Services peut vous aider grâce à une approche holistique offrant les services et les technologies qui ont fait la réputation d'IBM comme leader dans le développement et la distribution de solutions de sécurité. Nos services en gestion des identités et des accès mettent l'accent sur les principaux enjeux de sécurité auxquels sont confrontés les responsables informatiques et métier aujourd'hui. Ils les aident à :

- préserver l'intégrité des interactions mobiles, cloud et sociales ;
- éviter les menaces internes et les fraudes d'identités ;
- simplifier les cloisonnements d'identités et les intégrations cloud ;
- offrir une garantie intelligente des identités et des accès.

Nous proposons des services professionnels et gérés, dont :

- ***Services d'évaluation et de stratégie des identités et des accès :*** Conseils métier et technologiques pour aider les clients à concevoir un programme d'IAM adapté aux besoins de leur entreprise. L'offre est conçue pour fournir un plan réalisable afin d'améliorer les capacités de gestion de la conformité réglementaire, de concéder un accès pratique aux utilisateurs autorisés et de protéger les données de valeur.

  Cette approche, qui utilise un modèle de maturité méthodique et robuste, aide les clients à optimiser leur programme d'IAM avec une liste des projets prioritaires à accomplir dans un délai raisonnable, conformément à leurs contraintes budgétaires.

- ***Services de conception et de mise en œuvre de gestion des identités et des accès :*** Cadre et méthodologie éprouvés, conformes aux bonnes pratiques, pour concevoir et mettre en œuvre des solutions afin de maintenir le contrôle de la sécurité sur les dispositifs mobiles, atténuer les menaces internes et externes, réduire les risques de sécurité dans les environnements cloud et automatiser la gestion de la conformité.

- ***Services gérés de gestion des identités et des accès :*** Modèles sur site, hébergés ou basés sur le cloud, proposant un éventail complet de capacités, notamment fourniture des accès utilisateur, gouvernance des cycles de vie, connexion unique, services de registre d'utilisateurs de l'entreprise, fédération et authentification à plusieurs facteurs.

Figure 4 : IBM propose des solutions de bout en bout pour soutenir vos besoins en IAM, depuis l'évaluation et la conception d'une stratégie jusqu'à son exécution.

IBM est depuis longtemps reconnue comme leader en matière de solutions de sécurité. La société est l'une des seules à fournir ce type de solutions de bout en bout en gestion des identités et des accès, depuis l'élaboration d'une stratégie, jusqu'à la conception, la construction et la gestion. Nos spécialistes de la sécurité travaillent en collaboration avec vous pour répondre à vos besoins spécifiques et vous fournir les solutions adaptées aux objectifs de votre entreprise.

Pour en savoir plus

Pour en savoir plus sur la façon dont IBM Security Services peut vous aider à réduire les coûts et renforcer votre protection contre les menaces sophistiquées, veuillez prendre contact avec votre représentant IBM ou votre partenaire commercial IBM et visiter le site suivant : ibm.com/services/security

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produit aux Etats-Unis
Juillet 2016

Recyclable.

SEW03038-FRFR-01