Tendances et recommandations

Gestion des identités et des accès

Dans un monde où le travail hybride ou à distance est devenu la norme, la gestion des identités et des accès (GIA) s'impose de plus en plus comme une priorité pour les responsables informatiques. KPMG propose un aperçu des principales tendances et recommandations clés dans ce domaine en 2022.

Cinq tendances en matière de GIA

1 **Automatisation des procédures d'orientation et de départ des employés « hybrides »**

2 **Gestion des identités et des accès dans le nuage**

3 **Protection accrue grâce aux gestionnaires de mots de passe**

4 **Stratégie de vérification systématique**

5 **Application du principe de l'accès minimal aux appareils externes**

La GIA fournit un cadre de politiques et de technologies qui permet aux organisations de déterminer, en connaissance de cause et en se fondant sur les risques, qui pourra accéder à certains renseignements ou actifs opérationnels précis, à quel moment et dans quel contexte. En cette ère où de plus en plus d'employés travaillent « en tout temps, n'importe où et sur n'importe quel appareil », les entreprises doivent être en mesure de suivre la prolifération de tous ces systèmes et identités. Voici cinq tendances et priorités à prendre en compte :

1 Automatisation des procédures d'orientation et de départ des employés « hybrides »

L'orientation et le départ des employés exigeaient jusqu'à maintenant de longues procédures manuelles. Avec l'adoption de modèles de travail à distance ou hybrides, il est essentiel d'offrir une expérience d'accueil rapide et transparente, car celle-ci donne le ton de la culture de l'entreprise.

Pour les entreprises qui disposent des outils de GIA appropriés, il suffit d'appuyer sur un bouton pour exécuter ces fonctions. Par exemple, le provisionnement automatique accorde aux employés les accès correspondant à leur poste et à leur niveau d'autorisation, de manière instantanée et sécurisée et le déprovisionnement automatique permet de s'assurer que les personnes quittant l'organisation ne laissent derrière elles aucun compte orphelin ou sans utilisateur associé.

2 Gestion des identités et des accès dans le nuage

Aucun chef d'entreprise n'aurait pu prévoir que tous ses employés seraient soudainement forcés de travailler à distance en raison d'une pandémie. La pression énorme qu'un tel changement a exercé sur l'infrastructure informatique interne a eu comme effet de ralentir les systèmes et de freiner la productivité. Les entreprises ont réagi en accélérant l'adoption d'applications et de services infonuagiques qui, outre la souplesse, offrent l'avantage d'une mise en œuvre rapide et facile et ne nécessitent plus de mises à niveau régulières (et souvent fastidieuses) comme c'est le cas des technologies traditionnelles.

Pour les entreprises, de plus en plus nombreuses à se tourner vers le nuage, un défi se pose, celui de trouver un moyen sûr et sécurisé de donner aux employés un accès direct aux ressources infonuagiques et SaaS. Une solution efficace

© 2022 KPMG s.r.l., société à responsabilité limitée de l'Ontario et cabinet membre de l'organisation mondiale KPMG de cabinets indépendants affiliés à KPMG International Limited, société de droit anglais à responsabilité limitée par garantie. Tous droits réservés

consiste à appliquer les capacités de contrôle déjà en place dans leur infrastructure à une approche infonuagique simple, mais offrant toute la sécurité nécessaire. Comme de nombreuses technologies existantes en matière de sécurité ont accru leurs capacités pour répondre à ce besoin, les organisations auraient avantage à tirer parti des outils qu'elles possèdent déjà et avec lesquels leurs équipes sont déjà familiarisées.

3 Protection accrue grâce aux gestionnaires de mots de passe

À mesure que les activités dans le nuage prennent de l'expansion, les employés doivent gérer des dizaines de comptes, chacun nécessitant un mot de passe unique et sécurisé. Or, s'il est difficile de mémoriser autant de mots de passe, l'utilisation du même mot de passe à plusieurs endroits augmente les risques pour la sécurité. Selon une étude d'IBM, les données d'identification compromises étaient responsables de 20 % des cyberintrusions en 2021, entraînant des coûts moyens de 4,37 millions de dollars américains. D'autres problèmes liés aux mots de passe, tels que les processus d'authentification ou le verrouillage, peuvent également ralentir les performances et la productivité.

C'est ici qu'entre en action un autre outil de GIA : le giad'un coffre-fort numérique chiffré qui crée des mots de passe robustes et uniques pour chaque application et chaque compte, et stocke ces informations en toute sécurité. En plus de rendre les données d'identification plus difficiles à pirater, un tel outil élimine le besoin de mémoriser un grand nombre de mots de passe. De nombreux employés utilisent déjà cet outil, mais il est préférable de mettre en place une plateforme normalisée à l'échelle de l'entreprise.

4 Stratégie de vérification systématique

Pour des raisons de sécurité, de plus en plus d'entreprises appliquent le principe de la confiance nulle « ne jamais faire confiance et toujours vérifier » qui commande une vérification systématique des droits d'accès des utilisateurs et de leurs appareils. Cette tendance risque de s'accentuer dans le contexte du travail à distance ou hybride, où les utilisateurs accèdent aux ressources par de nouveaux moyens et souvent avec des appareils dont l'intégrité n'est pas confirmée.

La confiance nulle est davantage un état d'esprit ou une stratégie qu'un outil ou une technologie. Les entreprises qui s'en inspirent conçoivent leur architecture de capacités selon le principe qu'une violation est toujours possible à l'intérieur ou à l'extérieur des périmètres de leur réseau et que tous les utilisateurs, applications, données et appareils doivent faire l'objet d'une vérification systématique et d'un contrôle permanent. Cette approche permet de segmenter les ressources, de fournir un accès juste à temps, de sécuriser les codes et de protéger les données.

5 Application du principe de l'accès minimal aux appareils externes

Le principe de l'accès minimal vise à limiter le droit d'accès des employés aux seules ressources dont ils ont besoin pour exécuter un travail ou une tâche spécifique. Par exemple, un responsable du marketing n'a pas besoin d'accéder aux états financiers de l'entreprise. Bien que cette approche soit déjà en place au sein de nombreuses organisations, il serait temps de l'appliquer également aux réseaux, aux comptes, aux périphériques, etc.

Confrontées à l'évolution rapide du milieu de travail, les organisations doivent maintenant étendre le principe de l'accès minimal à l'ensemble de leurs activités afin de mieux protéger leurs actifs de valeur, y compris les services et les terminaux externes, comme les ordinateurs portables, ce qui les aidera à bloquer les attaques par rançongiciels et les actions malveillantes internes. Elles peuvent aussi appliquer le principe du provisionnement « juste à temps » selon lequel les utilisateurs ne sont autorisés à accéder aux systèmes qu'au moment où ils en ont besoin.

© 2022 KPMG s.r.l.., société à responsabilité limitée de l'Ontario et cabinet membre de l'organisation mondiale KPMG de cabinets indépendants affiliés à KPMG International Limited, société de droit anglais à responsabilité limitée par garantie. Tous droits réservés

La GIA comme catalyseur des activités

Voici les principaux avantages d'un programme de GIA à grande échelle :

- Intégration rapide des nouveaux employés qui sont prêts à exécuter leurs tâches dès le premier jour, création d'une expérience positive et productivité accrue
- Diminution des demandes d'assistance au service des TI et réduction du temps d'attente des employés grâce aux outils en libre-service
- Protection des données contre les risques potentiels : les bonnes personnes obtiennent le bon niveau d'accès au moment précis où elles en ont besoin

Protection des renseignements personnels

Sous l'effet des nouvelles législations sur la protection de la vie privée, comme le projet de loi 64 au Québec et les réformes en cours dans d'autres provinces, la protection des renseignements personnels est plus importante que jamais et exige des ajustements de la part des entreprises. Voici certaines des fonctionnalités de la GIA qui peuvent les aider à cette fin :

- **Répartition des tâches** : veiller à ce que les tâches liées aux données personnelles soient effectuées par plusieurs personnes.
- **Besoin de connaître :** limiter l'accès aux données sensibles aux seules personnes qui en ont réellement besoin pour accomplir leurs tâches.
- **Attestation d'accès :** réévaluer régulièrement l'accès des employés aux systèmes traitant des informations personnelles.
- **Seuil d'authentification** : établir un niveau élevé d'authentification pour accéder aux informations sensibles.
- **Gestion des données non structurées :** contrôler soigneusement l'accès aux données non structurées contenant des renseignements personnels.
- **Automatisation du cycle de vie** : mettre en place des processus automatiques de révocation d'accès lorsqu'il n'est plus nécessaire.

Changement à l'horizon : la disparition des mots de passe

L'essor des techniques d'identification biométriques par empreintes digitales, reconnaissance faciale et autres a permis aux organisations de diversifier les facteurs d'authentification, passant de processus à un seul facteur de connaissance à l'authentification multifactorielle. Toutefois, cette augmentation exponentielle de la puissance de calcul a aussi aidé les fraudeurs à craquer plus rapidement les mots de passe, obligeant les entreprises à revoir leurs directives de sélection de mots de passe.

Cette tendance a favorisé l'émergence du processus d'authentification unique (SSO) qui a simplifié l'expérience utilisateur, mais souvent au détriment de la sécurité. Les organisations ont eu à gérer cette pression supplémentaire, leurs équipes des opérations devant constamment réinitialiser les mots de passe, une tâche qui, dans le contexte, devenait de plus en plus longue et complexe.

C'est pourquoi les entreprises ont accueilli favorablement l'arrivée d'outils en libre-service à plusieurs facteurs d'authentification qui, en cas de perte, permettent aux utilisateurs de réinitialiser leurs mots de passe au moyen d'une connexion sécurisée.

© 2022 KPMG s.r.l.., société à responsabilité limitée de l'Ontario et cabinet membre de l'organisation mondiale KPMG de cabinets indépendants affiliés à KPMG International Limited, société de droit anglais à responsabilité limitée par garantie. Tous droits réservés

Les quatre grands types de facteurs d'authentification

Facteur mémoriel (ce que l'on connaît)
information que seul l'utilisateur connaît (ex. : un mot de passe, un NIP ou la réponse à une question secrète)

Facteur matériel (ce que l'on possède)
appareil spécifique (téléphone intelligent, clé USB, RPV virtuel, etc.) identifié au moyen de certificats numériques

Facteur corporel (ce que l'on est)
données biométriques (reconnaissance faciale, empreintes digitales, empreintes rétiniennes ou voix)

Localisation
Contrôles de sécurité par géolocalisation visant à vérifier l'emplacement de l'utilisateur

Il est essentiel de trouver le juste équilibre entre sécurité, efficience opérationnelle et expérience utilisateur et c'est pourquoi nous pourrions assister, dans un avenir pas si lointain, à la disparition totale des mots de passe sous l'effet conjugué des progrès de la cryptographie, de l'échange de clés publiques et privées et de l'émergence de nouvelles normes d'authentification.

Les solutions sans mot de passe présentent de nombreux avantages pour les organisations, notamment :

- Réduction des coûts d'exploitation des centres informatiques dédiés à la réinitialisation des mots de passe
- Protection accrue contre le hameçonnage
- Augmentation de la productivité, car les utilisateurs perdent moins de temps à soumettre des demandes et à attendre la réinitialisation de leur mot de passe
- Conformité aux normes du National Institute of Standards and Technology (NIST) (niveaux 2 et 3 de certification des identifiants)

Changement à l'horizon : l'analyse prédictive

L'intégration de la GIA aux processus de gestion des risques a incité davantage d'entreprises à s'intéresser aux technologies d'analyse prédictive associées aux procédures de gestion des identités et des accès. Les modèles prédictifs analysent les données enregistrées par les outils de GIA, favorisant l'automatisation du processus décisionnel.

L'analyse prédictive offre notamment d'intéressantes possibilités dans les domaines suivants :

Approbation des accès : en fonction du partage (ou non) de certains attributs, les moteurs faciliteront, voire automatiseront, l'approbation de certains accès ou, s'il y a lieu, alerteront le responsable de l'approbation des risques.

Attestation des accès : selon le même principe régissant l'approbation des accès, les modèles prédictifs peuvent repérer les demandes d'accès qui nécessitent une plus grande attention et déclencher un processus de renouvellement prioritaire.

Séparation des tâches : en se fondant sur l'analyse intégrale des accès, les moteurs sont en mesure de détecter certaines incompatibilités, aidés à cette fin par l'accès de nombreuses solutions de GIA à des bibliothèques de règles d'incompatibilité par le biais de partenariats stratégiques (p. ex., SAP).

© 2022 KPMG s.r.l., société à responsabilité limitée de l'Ontario et cabinet membre de l'organisation mondiale KPMG de cabinets indépendants affiliés à KPMG International Limited, société de droit anglais à responsabilité limitée par garantie. Tous droits réservés

Protection des accès à l'avenir

Les moteurs d'intelligence artificielle détecteront les menaces en temps réel et détermineront avec un haut degré de précision le niveau de risque de l'utilisateur au moment de la demande d'accès. Les niveaux d'authentification et d'autorisation requis seront établis en conséquence. Par exemple, un utilisateur qui se connecte depuis un autre pays pourrait devoir fournir un facteur d'authentification supplémentaire et ses privilèges pourraient être réduits.

Sécurité des accès

Création d'une identité fiable, structurée selon un modèle évolutif, donnant accès aux ressources de l'entreprise selon un niveau de risque établi en temps réel

=

Niveau d'accès

Évaluation et révision en temps réel du niveau d'accès de l'utilisateur

+

Authentification

Authentification de l'utilisateur au moyen de plusieurs facteurs autres que les mots de passe

+

Détection des risques

Utilisation de l'intelligence artificielle et de l'apprentissage automatique pour détecter le risque représenté par l'utilisateur, par le recoupement de plusieurs sources de données

© 2022 KPMG s.r.l., société à responsabilité limitée de l'Ontario et cabinet membre de l'organisation mondiale KPMG de cabinets indépendants affiliés à KPMG International Limited, société de droit anglais à responsabilité limitée par garantie. Tous droits réservés

Nos six recommandations concernant la GIA

#01 Le tableau de la main-d'œuvre spécialisée en GIA se transforme radicalement. **Étendez votre recherche de talents** à d'autres communautés (les personnes neuroatypiques p. ex.) **et dans des domaines complémentaires,** comme la gestion des risques et des ressources humaines; vous pourriez aussi intégrer des spécialistes externes à votre équipe. Et rappelez-vous que la rétention des talents est tout aussi – sinon plus – importante que le recrutement.

#02 En gestion des identités et des accès, l'approche « prêt-tirer-viser » est à éviter. **Prenez le temps d'élaborer les récits d'utilisateur, les processus et les flux de données** de votre programme avec les parties concernées. Vous gagnerez ainsi un temps considérable lors du déploiement de la solution en plus d'améliorer son taux de réussite.

#03 De nombreuses organisations envisagent des solutions SaaS pour leur programme de GIA afin de profiter de la mise à niveau automatique et de réduire la charge de travail des équipes d'infrastructure. Il est important de connaître vos options et la façon de les intégrer à votre culture organisationnelle.

#04 Chaque jour, nous avons accès à de nouvelles technologies qui nous permettent d'améliorer nos capacités, mais sans résultats mesurables, celles-ci sont vouées à l'échec. **Des objectifs clairs sont essentiels pour guider le processus et le programme d'automatisation** et pourront servir par la suite de paramètres clés pour un suivi en continu.

#05 **Découvrez toutes les fonctionnalités des solutions technologiques.** Souvent, les organisations ne mettent en œuvre qu'une petite partie de la solution qu'elles achètent. Demandez de la formation et des conseils sur les autres fonctionnalités qui sont peut-être déjà comprises dans votre licence et voyez si elles peuvent être mises à profit dans le cadre de votre programme.

#06 Consacrez du temps à la formation. **Faites du développement de votre équipe une priorité** au sein de votre organisation et prévoyez du temps à cette fin dans le cycle d'évaluation annuel des employés. Les employés sont plus susceptibles de rester s'ils ont le sentiment d'être soutenus, mais il est difficile de donner la priorité au développement professionnel sans le soutien de la direction.

© 2022 KPMG s.r.l./S.E.N.C.R.L., société à responsabilité limitée de l'Ontario et cabinet membre de l'organisation mondiale KPMG de cabinets indépendants affiliés à KPMG International Limited, société de droit anglais à responsabilité limitée par garantie. Tous droits réservés

Communiquez avec nous

Thomas Davies
Associé, National
KPMG au Canada
416-468-7339
thomasdavies@kpmg.ca

Marc Chaput
Associé, Québec
KPMG au Canada
514-840-5674
mchaput@kpmg.ca

Imraan Bashir
Associé, Est du Canada
KPMG au Canada
613 212 2852
ibashir@kpmg.ca

Jamie Whynacht
Directeur, Toronto
KPMG au Canada
416-468-7170
jwhynacht@kpmg.ca

Erik Berg
Associé, Vancouver
KPMG au Canada
604-691-3245
erikberg@kpmg.ca

Robin Tong
Associé, Canada de l'Ouest
KPMG au Canada
780-429-7335
robintong@kpmg.ca

home.kpmg/ca/fr

L'information publiée dans le présent document est de nature générale. Elle ne vise pas à tenir compte des circonstances de quelque personne ou entité particulière. Bien que nous fassions tous les efforts nécessaires pour assurer l'exactitude de cette information et pour vous la communiquer rapidement, rien ne garantit qu'elle sera exacte à la date à laquelle vous la recevrez ni qu'elle continuera d'être exacte à l'avenir. Vous ne devriez pas y donner suite à moins d'avoir d'abord obtenu un avis professionnel se fondant sur un examen approfondi des faits et de leur contexte.

© 2022 KPMG s.r.l./S.E.N.C.R.L., société à responsabilité limitée de l'Ontario et cabinet membre de l'organisation mondiale KPMG de cabinets indépendants affiliés à KPMG International Limited, société de droit anglais à responsabilité limitée par garantie. Tous droits réservés. KPMG et le logo de KPMG sont des marques de commerce utilisées sous licence par les cabinets membres indépendants de l'organisation mondiale KPMG. 15050