

Gestion des identités et des risques

Se préparer à un monde nouveau

À PROPOS DE CETTE ARTICLE

Dans le domaine de la gestion des identités et des risques, l'époque du statu quo est révolue. La vitesse croissante avec laquelle le Web 2.0, l'informatique en nuage et la mobilité s'imposent désormais dans les activités d'une entreprise l'exige.

Les organisations doivent penser autrement si elles souhaitent maintenir leur avantage concurrentiel. Il ne suffit plus d'évaluer les enjeux liés aux TI, comme la sécurité, d'un point de vue purement technique. En effet, une approche viable et durable de gestion des identités et des risques doit provenir de la haute direction, de leaders, qui comprennent et mettent en œuvre une approche de gouvernance solide afin de composer avec un environnement où les interactions de « plusieurs à plusieurs » sont monnaie courante.

Cette étude aborde la façon dont les leaders peuvent se préparer à ce monde nouveau auquel on peut accéder grâce à différents canaux et à de multiples dispositifs, pour améliorer la sécurité et mieux atténuer les risques.

La gestion des identités et des risques comporte son lot de nouveaux défis pour les organisations gouvernementales et les entreprises. Toutefois, plusieurs d'entre elles travaillent toujours comme il y a 10 ans. L'époque des interactions d'affaires gérées efficacement selon une approche de « un à plusieurs », où la norme consistait en un nom d'utilisateur et un mot de passe sur un réseau local, est révolue. Aujourd'hui, on observe un virage vers un environnement de « plusieurs à plusieurs » intervenants grâce à Internet.

Dans ce nouvel environnement complexe, alimenté par le Web 2.0, l'informatique en nuage et les services mobiles, les partenaires d'affaires, les fournisseurs de services et les clients sont souvent répartis partout dans le monde. De plus, les données internes des organisations deviennent plus vulnérables aux intrusions, et des préoccupations surgissent quant à l'identité des tiers avec lesquels ces dernières partagent des données.

À la lumière de ces nouveaux défis, rares sont les organisations qui peuvent se permettre de poursuivre leurs activités sans s'adapter. De plus, ces organisations ne peuvent plus envisager les enjeux liés à la sécurité, plus précisément la gestion des identités et des risques, d'un point de vue purement technique.

Gestion des identités et des risques : une nouvelle réalité

Nombre d'industries doivent composer avec cette nouvelle réalité.

Prenons les soins de santé. Auparavant, les professionnels de la santé avaient accès aux renseignements sur les patients au sein d'un seul établissement. Aujourd'hui, grâce aux dossiers médicaux électroniques, ces professionnels jouissent d'un accès instantané aux renseignements de patients qui ne sont pas les leurs, et ce, avec ou sans le consentement du client, tout dépendant de la juridiction.

Dans le domaine des services publics, des entreprises comme Orange en France acceptent désormais les profils publics de leurs clients, comme ceux générés sur Windows Live, Google ou Yahoo, dans leur propre environnement d'identité fédérée. Il s'agit d'une évolution majeure par rapport à l'époque où les bases de données privées de clients constituaient la norme.

Enfin, parlons gouvernements, où dans la plupart des cas, le partage des données et la cybersécurité, plus particulièrement la gestion des identités, de l'authentification et des autorisations, constituent des sujets d'actualité. En effet, les organismes gouvernementaux se penchent de plus en plus sur les façons de valider les identités de façon récurrente et interopérable. L'initiative américaine

FICAM (Federal Identity, Credential and Access Management) reflète cette préoccupation.

Ce virage vers les échanges de « plusieurs à plusieurs » dans plusieurs secteurs d'activité illustre la nécessité d'une nouvelle approche en matière de gestion des identités et des risques. Alors que, auparavant, une organisation n'avait qu'à fournir un mot de passe à usage unique, de type SecurID, pour sécuriser l'accès d'un utilisateur à un réseau d'entreprise, le processus de vérification de l'identité atteint maintenant un tout autre niveau de complexité et permet de valider l'identité d'une personne avant de lui donner accès aux actifs informationnels de l'organisation.

Cadre de gouvernance de la gestion des identités : mis de l'avant par la haute direction

La mise en place d'un cadre de gouvernance de la gestion des identités doit constituer la première étape à franchir pour relever les défis d'aujourd'hui en matière de gestion des identités et des risques.

Plus que jamais, la haute direction doit comprendre que c'est elle, et non son service technique, qui est ultimement responsable des actifs informationnels et des données de son organisation. Toutefois, il arrive trop souvent qu'elle adopte aveuglément une solution technique livrée par un produit en vogue sans d'abord réaliser une analyse coût-avantage. Cette approche compromet souvent l'efficacité et entraîne des coûts.

De 80 % à 90 % des approches efficaces en matière de gestion des identités et des accès mettent l'accent sur la stratégie d'affaires. L'aspect « identité » requiert des procédures, des processus et des bases juridiques, lesquelles doivent reposer sur un cadre de gouvernance des identités solide, élaboré sous la gouverne de la haute direction, et qui respecte la législation, la réglementation, les normes et les pratiques de l'industrie en question.

Finalement, le cadre de gouvernance détermine quels sont les individus qui doivent se soumettre à un processus d'identification rigoureux et disposer d'une authentification forte. Par exemple, si une organisation utilise des renseignements publics ou peu sensibles, elle n'aura pas besoin d'un processus d'authentification forte. Toutefois, si celle-ci œuvre dans les domaines de l'information médicale ou du renseignement criminel, elle doit absolument se doter d'un cadre de gouvernance bien articulé. Pour être efficace, un cadre de gouvernance doit se référer aux exigences légales et à la catégorisation d'actifs pour déterminer le niveau de confiance requis des tiers voulant y accéder. L'organisation applique alors le processus de gestion de l'identité prévu dans son cadre de référence en matière d'identification et d'authentification.

ÉLABORER UN CADRE DE GOUVERNANCE DES IDENTITÉS

L'élaboration d'un cadre de gouvernance des identités s'avère indispensable pour mieux relever les défis que comporte la gestion des risques et des identités.

Ce type de cadre de gouvernance requiert une participation de la haute direction, et doit énoncer avec clarté les rôles et les responsabilités grâce à un modèle d'imputabilité et une vision claire quant au choix des personnes devant faire l'objet d'une identification et d'une authentification forte.

Web 2.0, mobilité, informatique en nuage : connaître les défis

Tout cadre efficace doit être en mesure de composer avec trois types de défis, soit le Web 2.0, la mobilité et l'informatique en nuage. Tôt ou tard, une organisation aura sans doute recours à ces services, et il sera essentiel qu'elle comprenne la valeur de la gestion des identités au sein de chacun de ces environnements.

Dans le contexte du Web 2.0 (plus précisément les médias sociaux), une organisation peut facilement être victime de vols d'identités ou de fuites de données, et ce, non seulement par l'entremise de stratagèmes techniques sophistiqués. Pour commettre de tels vols, les criminels peuvent simplement utiliser une approche « amis d'amis » afin d'obtenir l'accès à des renseignements privilégiés ou sensibles.

Si vous êtes cadre dans un organisme gouvernemental ou une entreprise, méfiez-vous de la facilité avec laquelle vos employés peuvent être identifiés sur le site Web de tout grand média social et, par extension, la facilité avec laquelle ces mêmes employés peuvent être utilisés pour obtenir des renseignements relatifs à la propriété intellectuelle ou à la stratégie de l'entreprise.

Par exemple, le seul fait pour un employé de mentionner sur sa page Facebook qu'il travaille pour un organisme d'application de la loi, ou que cette information soit mentionnée sur la page d'un ami Facebook, pourrait nuire au résultat d'une intervention policière. Cette vulnérabilité, qui s'applique à tout type d'organisation, fait en sorte que la mise en place d'un cadre uniforme régissant l'utilisation des médias sociaux au sein de votre entreprise ou votre organisme gouvernemental s'avère essentielle. Ce cadre devrait clairement indiquer qu'aucun employé ne peut divulguer des renseignements, peu importe leur importance, par l'entremise des médias sociaux.

Les appareils mobiles soulèvent également des problèmes de sécurité. En effet, avec des appareils tels que les iPhone, iPad et BlackBerry, les données essentielles à la mission d'une entreprise ne sont souvent qu'à un doigt de l'écran. Bien que la flexibilité en tout lieu et en tout temps offerte par de tels appareils alimente une main-d'œuvre mobile, cette caractéristique peut également entraîner des conséquences fâcheuses pour les entreprises si ces appareils sont perdus ou volés alors qu'ils contiennent des données essentielles non protégées. En conséquence, il s'avère primordial qu'une organisation soit en mesure d'identifier non seulement la personne qui utilise l'appareil, mais aussi l'appareil lui-même, et soit capable de le localiser et de le désactiver, le cas échéant.

L'informatique en nuage comprend ses propres exigences en matière de sécurité, surtout au sein de certaines industries, comme les soins de santé, où les renseignements médicaux peuvent être stockés dans le nuage. De quelle façon une organisation peut-elle savoir où une personne donnée accède à ses renseignements essentiels? Et au moyen de quel réseau de communication? Toute organisation doit se doter d'un niveau d'authentification additionnel allant au-delà des mesures traditionnelles utilisées lorsque les données étaient simplement stockées sur un système interne.

AUTHENTIFIER POUR L'AVENIR

Trois tendances fortes se profilent en ce qui a trait à la façon de relever les défis que comporte la gestion des identités :

1. **L'approvisionnement** pour assurer la gestion de l'identité des utilisateurs (employé, sous-traitant, tiers, etc.), et l'accès aux systèmes, aux applications et aux ressources, et ce, dans toute l'organisation.
2. **L'authentification** pour mettre en place des authentifiants (et les gérer facilement) afin de prouver les identités, et à permettre une utilisation dans des environnements Web standards, de même que dans des environnements Web 2.0, mobiles et d'informatique en nuage.
3. **L'authentification forte et les signatures numériques** pour assurer l'imputabilité des tiers accédant à de l'information sensible et pour assurer l'irrévocabilité (non-répudiation) des transactions en ligne.

Afin d'atteindre cet objectif, les organisations doivent s'assurer que le fournisseur se conforme aux normes de l'industrie. Par exemple, il importe que le site où les données seront stockées selon un modèle d'informatique en nuage respecte des normes généralement reconnues, comme la conformité SAS 70 de niveau 2 pour les centres de traitement de données et une architecture SaaS, assortie d'un degré de maturité de 1 à 4, selon les besoins d'affaires de l'organisation. Le fournisseur doit habituellement être en mesure de démontrer qu'il se conforme aux niveaux de sécurité et de maturité exigés par une organisation.

Gestion des identités : connaître les tendances émergentes

Trois tendances fortes se profilent en ce qui a trait à la façon de relever les défis que pose la gestion des identités : l'approvisionnement, l'authentification, et l'utilisation d'une authentification forte pour assurer l'imputabilité des tiers accédant à de l'information sensible et de la signature numérique pour assurer l'irrévocabilité (non-répudiation) des transactions en ligne.

L'approvisionnement sera requis lorsqu'une personne deviendra employé, fournisseur ou partenaire d'affaires d'une organisation. Par exemple, si une entreprise embauche régulièrement des sous-traitants, elle doit s'assurer qu'ils sont dûment approvisionnés, et ce, au bon moment.

Dans la vague de décentralisation des données qui déferle actuellement, l'approvisionnement constitue une étape essentielle. Dans un environnement d'informatique en nuage, les données d'une entreprise pourraient tout simplement se retrouver n'importe où sur la planète. Si une organisation confie à un tiers la tâche d'assurer la confidentialité de ses renseignements, elle doit s'assurer qu'aucune autre entité ne puisse y accéder, à l'exception des personnes autorisées.

L'authentification exigera qu'une entreprise soit en mesure de fournir des authentifiants (et de les gérer facilement) pouvant être utilisées dans des environnements Web standards ainsi que dans des environnements Web 2.0, mobiles et d'informatique en nuage. Si une organisation souhaite valider l'identité d'une personne avant d'émettre un authentifiant, elle doit choisir entre utiliser une source autoritaire de données, comme une source gouvernementale ou commerciale relative à l'identité, ou encore rencontrer la personne, obtenir ses renseignements personnels et, dans certains environnements précis, prélever ses empreintes digitales.

Au moment d'authentifier la personne en question, une organisation doit utiliser des authentifiants reposant sur des standards de l'industrie et disposant d'un niveau de sécurité suffisant. L'authentification forte peut comprendre un certificat d'identification numérique, jumelé à un ou à plusieurs autres facteurs d'authentification, en fonction de la nature des actifs informationnels que l'organisation souhaite protéger. Si une organisation utilise le certificat d'identification numérique comme facteur d'authentification, cette dernière peut s'assurer que toute personne en l'utilisant sera imputable de ses faits et gestes et

À PROPOS DE CGI

La raison d'être de CGI est de satisfaire ses clients. Chef de file de services en TI et en gestion des processus d'affaires, CGI regroupe 31 000 professionnels répartis dans 125 bureaux dans le monde.

Travaillant en partenariat avec des clients depuis 35 ans, CGI possède une vaste expérience de tous les aspects de la gestion des TI, des services-conseils aux services d'intégration de systèmes et à la gestion complète des fonctions informatiques et d'affaires (impartition).

Ce savoir-faire nous confère une position unique pour aider les clients à mettre en œuvre des solutions efficaces en matière de gestion des identités et de l'accès afin de gérer et d'atténuer les risques.

Pour en savoir davantage, visitez www.cgi.com ou écrivez-nous à info@cgi.com.

sera irrévocablement liée aux transactions qu'elle effectue ou aux documents qu'elle signe sur la base de cette identité.

Comme les entreprises continuent de rendre accessible leur base de données à d'autres tiers, en partageant par exemple des renseignements médicaux dans le secteur de la santé, l'authentification s'avère particulièrement importante. En ouvrant son « domaine de confiance » aux autres, une organisation doit être en mesure d'authentifier les personnes ayant accès à l'information qu'il contient. De plus, si des personnes soumettent de l'information pour alimenter un actif informationnel en particulier, l'organisation doit s'assurer qu'il s'agit bel et bien de la bonne personne avant de l'autoriser à le faire.

Enfin, l'utilisation de l'authentification forte et de la signature numérique ne fera que croître dans un contexte rempli de nouveaux défis en matière de gestion des identités et des risques. L'essor de la virtualisation (dématérialisation) des transactions accentue ce besoin. Si un contrat est signé numériquement, l'organisation doit être en mesure de valider l'identité du signataire (et de conserver sous une forme électronique), tel un médecin délivrant une ordonnance électronique ou un policier signant un rapport électronique.

Gestion des identités : voir au-delà des systèmes patrimoniaux

Les secteurs juridiques et des soins de santé un peu partout dans le monde ont introduit avec succès la gestion de l'identité dans leur secteur d'activité. Ce succès repose sur une règle d'or : voir au-delà des systèmes de sécurité propriétaires ou patrimoniaux pour améliorer l'efficacité de la gestion des identités et des risques.

La stratégie est maintenant claire : adopter les standards, s'en tenir à ces derniers et éviter tout excès de personnalisation.

Le savoir constitue également un élément clé. Des secteurs comme les soins de santé et les banques mettent au point leurs propres modèles de gouvernance. Une entreprise doit disposer des moyens lui permettant de se conformer aux normes, de les utiliser et de les intégrer à son cadre de gouvernance et à son environnement. En revanche, si une organisation exploite un système patrimonial qui ne répond pas aux nouvelles normes, elle doit trouver des moyens d'interfacer ces systèmes de manière à ce qu'ils répondent aux normes ou, dans certains cas, qu'ils s'y conforment.

Ces leçons apprises s'avèrent particulièrement pertinentes pour les organismes gouvernementaux. Plusieurs d'entre eux exploitent toujours en arrière-plan des ordinateurs centraux et d'anciennes technologies qui ne peuvent supporter ces standards. Dans de tels cas, il serait judicieux qu'elles externalisent l'authentification et, selon les besoins, les processus d'autorisation pour ces applications. De plus, elles devraient utiliser une interface normalisée pour authentifier les personnes et les autoriser à accéder à ces applications patrimoniales.