Gestion des identités et des accès : les grandes tendances de 2020

L'année 2019 a été jalonnée d'événements majeurs pour l'écosystème de la gestion des identités. On peut citer pêle-mêle la naissance de nouvelles réglementations sur la protection de la vie privée aux Etats Unis, les premières amendes significatives liées au non-respect du règlement RGPD dans l'Union Européenne, la croissance de l'open banking dans le monde entier, l'émergence de nouveaux standards d'authentification tels que WebAuthn et OpenID Connect CIBA, l'adoption généralisée du modèle de sécurité Zero Trust, ainsi que de nouvelles avancées dans le domaine du CIAM (la gestion de l'identité et des accès destinée aux clients) et l'importance croissante de l'IAM pour les entreprises 'cloud-first'.

Ce qui nous amène à nous interroger sur ce que nous réserve 2020 dans ces domaines. Il est clair que notre industrie a connu un profond bouleversement : le concept traditionnel de périmètre de sécurité a vécu, et la notion d'identité est désormais au cœur de la cyber sécurité.

Dans ce contexte, cinq tendances clés se distinguent pour l'année qui vient.

1. Les Etats Unis prennent au sérieux la protection des données personnelles

Les États-Unis font partie des rares pays développés qui ne disposent pas encore d'un standard national pour la protection des données personnelles.
Ceci non seulement affecte ce pays sur les plans économique et commercial, mais commence à générer de réelles inquiétudes sur le plan de la sécurité nationale et la protection des citoyens américains.
Le Congrès devrait enfin franchir le pas pour combler cette lacune et idéalement prendre l'initiative de protéger non seulement les données, mais aussi les identités numériques de tous les américains.

Pour savoir vers où nous allons en tant que nation, il suffit d'examiner ce qui se passe en Californie. Le California Consumer Privacy Act (CCPA), qui prendra effet au 1er janvier 2020, exige que toute entreprise en activité en Californie prenne « toutes mesures raisonnables pour protéger la sécurité des informations sensibles des consommateurs », et je m'attends à ce que d'autres États américains suivent et adoptent une législation similaire.

Toutefois, plus important encore, il est probable que le gouvernement fédéral, encouragé par le développement rapide des réglementations sur la sécurité des données, va prendre l'identité numérique sous son aile, en adoptant tout un ensemble de mesures de protection des données des consommateurs.

2. La protection des données personnelles devient un avantage concurrentiel

En 2019, nous avons assisté aux premiers cas d'entreprises présentant leurs pratiques en matière de protection des données personnelles de leurs clients en tant qu'avantage concurrentiel.
En 2020, cette tendance va prendre de l'ampleur, car les entreprises commencent à prendre en compte une nouvelle réalité : plus de 60 % des consommateurs considèrent que les entreprises sont entièrement responsables de la protection de leurs données.

Je pense qu'un nombre croissant d'entreprises suivront les traces d'Apple, qui se positionne dans l'esprit de ses clients comme un précurseur dans le domaine de la protection des données personnelles. Les initiatives d'Apple à ce sujet comprennent une mise à jour de son site web, qui insiste désormais sur la protection de la vie privée présentée comme un « droit humain fondamental », la mise en place de nouvelles fonctions de sécurité pour les clients telles que l'authentification Apple dans iOS13, et l'ajout d'une transparence complète (en plus d'importants moyens de contrôle pour l'utilisateur final) concernant le traitement des informations de localisation.

3. L'identité digitale se standardise

Il y a quelques années, les identités digitales relevaient encore de la fiction. Mais en 2020, des intérêts de nombreux secteurs d'activités (par exemple les services financiers, les réseaux sociaux, la santé) et des administrations publiques commenceront à se rejoindre pour créer des « standards d'identité digitale ».
Certains standards seront pour satisfaire les besoins du consommateur/citoyen, mais l'avenir dira si d'autres tenteront de capitaliser sur la valeur de ces identités digitales.

Des systèmes d'identification digitale ont déjà été créés en Norvège, en Estonie et en Australie. Il ne fait guère de doute qu'il est techniquement possible de développer un système national d'identité digitale sécurisé. Aux États-Unis, au fil de mes rencontres avec des responsables de départements fédéraux et de nombreux experts de la cyber sécurité et de la protection des données, où j'ai rencontré des responsables de ministères fédéraux ainsi que plusieurs personnalités de la cybersécurité et de la sécurité des informations, il est clair que l'avenir va dans cette direction.

4. Les consommateurs et les citoyens perdent patience

En 2019, des consommateurs et des citoyens ont commencé en masse à faire entendre leur voix contre les failles de sécurité à répétition de diverses entreprises, qui ont eu pour effet d'exposer leurs données, leurs finances, leurs familles et leurs services à des risques toujours plus grands. Les

consommateurs attendent des marques qu'elles protègent leurs données, et ils sont prêts à changer leurs comportements et ne plus faire appel à des entreprises s'ils considèrent qu'elles manquent à leurs obligations en matière de sécurité.

En 2020, nous assisterons à des conséquences réelles et substantielles pour les organisations qui ne protègent pas correctement leurs clients, leurs employés, leurs partenaires et leurs citoyens dans le monde digital.

Avec plus de 80 % des consommateurs qui indiquent qu'ils cesseraient de s'engager avec une marque en ligne après une fuite de données, il apparaît clairement que le citoyen moyen est prêt à cesser toute relation avec une entreprise qui ne fait pas ce qu'il faut en termes de protection des données personnelles.

5. L'authentification prend de plus en plus d'importance

Face à l'incapacité récente et continue des entreprises à sécuriser les accès des clients, 2020 connaîtra sans doute une recrudescence de l'adoption à grande échelle de l'authentification multi-facteur (MFA) par les entreprises et les utilisateurs finaux. Les entreprises désirant protéger à la fois leurs clients et leurs revenus seront amenées à adopter des méthodes d'authentification plus strictes pour atteindre ces objectifs.

L'un des secteurs précurseurs de cette tendance est celui des services financiers. Pour ce secteur, c'est l'expérience client – de l'inscription à l'accès aux services, aux préférences et au-delà – qui est devenue le principal facteur différenciant, et les établissements financiers y répondent en adoptant des technologies d'authentification qui améliorent cette expérience.
Par exemple, ils utilisent une authentification multi facteur personnalisée pour des interactions à haut niveau de risque, tout en conservant une authentification minimale pour des accès de routine.