Cloud et accès à privilèges : la protection des données au centre des enjeux

Selon les experts du cabinet Markess International, le marché français du cloud a enregistré une forte croissance ces dix dernières années, et serait passé de 900 millions d'euros en 2007 à 5,9 milliards d'euros en 2016.

Ils estiment qu'il devrait poursuivre sa croissance et connaître une progression de 18,6 % pour s'élever à près de 7 milliards d'euros cette année. En résumé, et sur le papier, le cloud se porte incontestablement bien.

Pourtant, bien qu'on en parle depuis longtemps, la véritable adoption du cloud est seulement en train de se produire ; les entreprises ont compris qu'elles ne pouvaient faire l'impasse pour rester compétitives. La Société Générale vient notamment d'annoncer que d'ici 2020, 80 % de son infrastructure sera sur des réseaux cloud internes et externes. Le fait que les banques embrassent le cloud, bien qu'elles manipulent des données à caractère sensible, ouvre la voie aux autres infrastructures critiques et d'importance vitale. Il est par conséquent indispensable qu'elles pensent la sécurité aux premiers stades du développement de leur stratégie de transformation digitale.

La digitalisation, nouvelle autoroute vers le vol de données

Ces dernières années ont en effet vu apparaître une forte appétence de la part des organisations pour les offres SaaS (Software-as-a-Service) et le cloud public telles qu'Amazon Web Services (AWS). Nous avons également observé un nombre croissant d'entreprises externaliser leur messagerie à travers des offres telles qu'Office 365. La raison ? Une recherche d'efficacité et de gain de temps afin de permettre aux équipes de déléguer les tâches à faible valeur ajoutée à ces outils, pour se concentrer davantage sur leurs coeurs de métiers.

Par essence, le cloud est géré en externe. Les organisations doivent donc faire confiance à des services tiers qui prennent en charge leurs données. Le fait que cette gestion soit externalisée ne permet donc pas aux entreprises de savoir de quelles manières leurs informations sont précisément traitées et sécurisées. Elles ont en effet besoin d'une visibilité totale sur ces activités et sur la gestion de leurs comptes à privilèges. Ces derniers permettant d'accéder à l'ensemble du système d'une organisation et d'en prendre le contrôle, il est essentiel d'en assurer le suivi de la manière la plus scrupuleuse possible.

Pour aider les entreprises à optimiser la flexibilité de leur infrastructure, de nombreux fournisseurs cloud ont donc mis en place des solutions de centralisation et d'automatisation des systèmes. Le but est ainsi de limiter autant que possible l'intervention humaine, souvent citée comme couteuse et potentiellement source d'erreurs. Ce qui permet également de répondre aux exigences du règlement européen de gestion des données personnelles** (RGPD, ou GDPR en anglais) dont l'entrée en vigueur est prévue en mai 2018. Cependant, toute mise en place d'un orchestrateur, soit un système permettant de gérer l'automatisation de toutes les opérations du cloud, induit une protection de ce

dernier. En effet, si un pirate informatique parvient à le compromettre et à en prendre le contrôle, il accède à tous les comptes à privilèges de l'organisation, bénéficiant alors des pleins pouvoirs sur l'ensemble des systèmes visés. Cela en fait ainsi une cible autant sinon plus sensible qu'un annuaire Active Directory, ne donnant par défaut que les clés de l'environnement Windows. Une question qui n'a pas échappé au règlement à venir qui prévoit de « s'applique[r] au traitement de données à caractère personnel, automatisé en tout ou partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier. » [Art.2]

RGPD : Légiférer pour mieux accompagner et protéger

Dans ce contexte, le RGPD « introduit l'obligation, pour les responsables du traitement et les sous-traitants, de conserver une trace documentaire des opérations de traitement sous leurs responsabilité » [Art.28], et insiste ainsi sur l'importance des personnes tierces - partenaires, fournisseurs de services cloud, consultant externes - qui accèdent aux données des organisations, soulevant ainsi la question de la répartition des responsabilités à travers la chaîne de distribution (supply chain) pour sécuriser et auditer les accès aux données personnelles.

Afin de répondre à cette problématique, le règlement prévoit notamment (mais pas uniquement) la mise en place d'une structure de gouvernance au travers de la désignation d'un acteur en charge du programme de protection des données au sein de l'entreprise (DPO - ou Data Privacy Officer). Mais au-delà de la définition des responsabilités, des contrôles fins sont nécessaires, raison pour laquelle il est également primordial d'adopter des mécanismes de contrôle et de traçabilité. Ces contrôles doivent permettre non seulement de protéger, mais également d'identifier les causes de failles afin de prendre les mesures correctives nécessaires quant à la protection des données personnelles.

En conclusion, la transformation digitale des organisations est en marche depuis plusieurs années mais s'accélère avec l'arrivée constante de nouvelles technologies et offres boostées par les avantages du cloud. Cela induit une augmentation drastique des données et crée un besoin pressant de pouvoir les gérer. Toutefois, les entreprises ne sont pas toujours équipées pour y faire face et n'ont pas toutes anticipé la protection de ces informations dans leurs stratégies. C'est donc à travers une étroite collaboration et en bonne intelligence que fournisseurs et entreprises pourront lutter ensemble contre les cyberattaques les plus avancées, et éviter ainsi une sanction si les règles édictées par le RGPD ne sont pas appliquées à compter de mai 2018 !