Quand la sécurité du cloud surpasse celle des modèles de déploiement traditionnels

La course est lancée entre les modèles de déploiement de services dans le cloud et hors du cloud, et les fournisseurs de services cloud ont un avantage évident : leur envergure.

 # PAIEMENT
 # CONNECTIVITÉ
 # CONTRÔLE D'ACCÈS
 # IDENTITÉ
 # VOYAGE
 # JUSTICE ET SÉCURITÉ PUBLIQUE

POSTÉ LE 26.01.23

Toute organisation individuelle dispose d'une capacité fixe d'investissement dans la sécurité. A l'inverse, dans le cloud, il n'y a pas de limite. Les fournisseurs de services cloud combinent les ressources de toutes les entreprises faisant appel à leur réseau, ce qui leur permet d'investir des milliards pour rester en tête de la course à la sécurité.

L'évolution des déploiements dans le cloud

Depuis la création du cloud il y a plus de dix ans, environ deux tiers des entreprises ont migré vers celui-ci. Pour le tiers restant, une grande partie de leur réticence tient au fait qu'elles ne sont pas suffisamment au courant de l'évolution qu'ont connus les environnements cloud pendant la dernière décennie. Au sein des secteurs public et privé, les derniers récalcitrants ont encore tendance à assimiler le cloud d'aujourd'hui au cloud des débuts. Or, **le cloud a énormément évolué au cours des dix dernières années**, notamment en termes de sécurité.

La sécurité du cloud public est un impératif business, et elle a fait ses preuves

Les principaux fournisseurs de services cloud sont là depuis le début, et leur taille et leur expertise n'ont cessé de grandir au fil du temps. En se développant et en prenant un rôle de plus en plus important, ils ont dû faire face à un nombre croissant d'attaques et à **une surveillance accrue** de la part des acteurs étatiques et industriels. En conséquence, ils ont investi massivement dans la sécurité du cloud public et pour développer leur expertise afin de parer aux attaques. En effet, toute atteinte à la sécurité du cloud met en jeu leur réputation, et la viabilité de leur activité. **Atténuer l'impact d'attaques à grande échelle est devenu une activité ordinaire** pour ces acteurs majeurs. Ils sont devenus capables, mieux que quiconque, de sécuriser les services de cloud computing à grande échelle.

Leur capacité à **atténuer les attaques DDoS (par déni de service distribué)** le démontre clairement. Ces attaques sont généralement perpétrées avec des milliers de bots qui injectent du trafic indésirable pour saturer les réseaux des

centres de données et paralyser complètement l'accès aux services. Pour limiter l'impact de ces attaques, il faut les disperser en s'appuyant sur un réseau de grande envergure et suffisamment résistant pour éviter la saturation. Il est pratiquement impossible pour des centres de données indépendants de rivaliser dans ce type de **guerre asymétrique**, une guerre qui coûte seulement quelques milliers de dollars par mois à ceux qui la déclenchent, mais qui nécessite plus de 100 000 dollars par mois pour se défendre. A contrario, les principaux fournisseurs de services cloud opèrent à une échelle qui leur permet de **répartir le poids de l'investissement** sur une base de millions de clients. AWS et Azure ont tous deux repoussé des attaques supérieures à 2 térabits par seconde (Tbps) en 2020 et 2022[1], ce que très peu d'entreprises peuvent revendiquer.

La résilience du cloud

L'envergure des fournisseurs de services cloud les rend également particulièrement aptes à garantir la résilience de leurs réseaux. Par exemple, les centres de données traditionnels ont des centaines d'équipements en service à tout moment, mais ils n'ont tout simplement pas le temps ou les ressources nécessaires pour les tester et détecter les pannes tous les jours. Les fournisseurs de services cloud, en revanche, ont des millions d'appareils en service, ce qui, statistiquement parlant, signifie qu'ils sont confrontés quotidiennement à des pannes. La différence tient au fait que les fournisseurs de services cloud ont **des équipes qui se consacrent exclusivement à la prévention et à la résolution des pannes**. Pour eux, il s'agit tout simplement d'une activité ordinaire.

L'approche granulaire de la sécurité du cloud public

Un autre aspect clé qui permet à la sécurité du cloud public de surpasser celle des centres de données traditionnels est la manière dont ils abordent celle-ci. Les centres de données sur site (*on-prem data centers*) et leurs processus ont été conçus à l'origine autour de la notion de périmètres physiques et logiques, autrement dit de « murs ». Ces murs peuvent être très solides, mais une fois franchis, ils peuvent ouvrir une large surface d'attaque.

À l'époque, la technologie permettant de déployer une sécurité granulaire n'existait même pas et la mettre en place aujourd'hui dans un centre données traditionnel s'avérerait extrêmement complexe, long et coûteux. Une fois encore, il s'agit d'une question d'échelle. Une seule organisation ne dispose pas des ressources nécessaires pour appliquer la sécurité avec une très forte granularité. Les modèles de déploiement dans le cloud, en revanche, ont été **conçus dès le départ pour assurer la sécurité à tous les niveaux**. Cela signifie que chaque élément, chaque serveur, chaque application et chaque service peut être configuré avec son propre contexte de sécurité et ses propres « murs ». C'est ce qu'on appelle la **sécurité en profondeur**. Celle-ci permet de protéger des informations très sensibles avec plusieurs couches de sécurité. Si une couche est compromise, il y en a une autre, et encore une autre derrière.

Qui est responsable de la sécurité dans le cloud public ?

Bien que la sécurité du cloud public s'améliore en continu, les organisations qui opèrent des services sur les réseaux des fournisseurs de services cloud **ne peuvent pas se fier aveuglément à eux** pour la sécurité dans le cloud. Après tout, les fournisseurs de services cloud ne sont responsables que de la sécurité de l'infrastructure.

Ces organisations doivent **s'assurer qu'elles font leur part pour sécuriser les services et les applications** de leurs clients. Cela implique d'expliquer les rôles et responsabilités à leurs clients, d'analyser les spécificités des services, et de partager et d'appliquer les meilleures pratiques en conséquence.

Les fournisseurs de services cloud définissent clairement les limites de leur champ d'action dans le cadre d'un « **modèle de responsabilité partagée** ». Cela permet aux fournisseurs de services s'appuyant sur leur réseau de savoir ce qu'ils doivent mettre en œuvre dans l'environnement cloud, en plus de la base solide que leur offre l'envergure du cloud public. La sécurité fournie par les principaux fournisseurs de services cloud tels qu'AWS, Azure ou Google est souvent appelée **sécurité *du* cloud**, tandis que la sécurité supplémentaire qui relève de la responsabilité des fournisseurs de services qui gèrent des services critiques pour des gouvernements ou des industries hautement réglementées est appelée **sécurité *dans* le cloud**.

Qu'il s'agisse de se protéger contre des attaques DDoS, de se prémunir contre la perte ou l'altération de données ou plus généralement de profiter des avantages majeurs qu'offre le cloud, les modèles de déploiement dans le cloud permettent aux entreprises de tirer parti des outils, des processus, des investissements et de l'expertise des principaux fournisseurs de services cloud afin de **garder une longueur d'avance dans la course permanente à la sécurité**.

---

[1] https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/; https://www.zdnet.com/article/microsoft-heres-how-we-stopped-the-biggest-ever-ddos-attack/
