Les Echos
LE QUOTIDIEN DE L'ÉCONOMIE

PAYS :France
PAGE(S) :22
SURFACE :43 %
PERIODICITE :Quotidien

RUBRIQUE :High-tech et medias
DIFFUSION :129052
JOURNALISTE :Florian Dèbes

► 31 mars 2022 - N°23677

HIGH-TECH&MEDIAS

Les champions du cloud face au défi des failles de sécurité

- Alors que les cyberattaques se multiplient, les géants du cloud rivalisent désormais sur le terrain de la sécurité.
- Le récent rachat de Mandiant par Google est perçu comme le début d'une vague d'acquisitions dans le secteur.

CYBERSÉCURITÉ

Florian Dèbes
@FL_Debes

La sécurité informatique est au cœur des priorités du « cloud computing ». Le fait que deux des champions mondiaux de l'informatique en ligne, Google et Microsoft, se soient disputé, à prix d'or, l'acquisition de l'une des sociétés de cybersécurité les plus réputées du monde occidental, Mandiant, illustre cette prise de conscience de la nécessité, urgente pour les champions du cloud, de se protéger contre les failles de sécurité.

D'après les analystes, cette opération à 5,4 milliards – déboursés par Google – devrait marquer le début de grandes emplettes dans le secteur, en vue de sécuriser les clouds dans lesquels de plus en plus d'entreprises hébergent leurs précieuses données et leurs logiciels, comme le rappelle ce jeudi la journée mondiale de la sauvegarde des données. Face à la pénurie de talents, acheter des sociétés de cybersécurité permet aux plateformes de renforcer rapidement leurs effectifs sur ce front critique.

Alors que les cyberattaques se multiplient et n'épargnent plus les coffres-forts numériques d'Amazon, Microsoft et Google, la compétition acharnée entre ces trois acteurs dominants passe désormais par la sécurité. « *Puisque nos clients ont le choix entre plusieurs fournisseurs de cloud, nous devons leur inspirer confiance* », décrypte Bernard Ourghanlian, le directeur des technologies de Microsoft en France.

Microsoft quadruple son budget

L'entreprise de Redmond s'en est donné les moyens en mobilisant 20 milliards de dollars en cinq ans pour sécuriser ses produits, soit un quadruplement de son budget. Google consacrera la moitié de cette somme sur la même durée. Et cet investissement est déjà rentable. En douze mois, Microsoft génère plus de 15 milliards de dollars de chiffre d'affaires avec les logiciels qui protègent ses clients dans le cloud Azure et ses autres technologies, voire depuis quelques semaines les clouds de ses rivaux.

Amazon, le numéro un mondial de l'hébergement en ligne avec 40 % de part de marché, n'est pas en reste. Ses acquisitions n'ont pas l'ampleur de celle de Google mais sont significatives : sa filiale cloud AWS a acheté l'été dernier la messagerie sécurisée Wickr et avait déjà mis la main en 2018 sur Sqrrl, une société créée par des anciens des services secrets américains. Parmi les outsiders du marché, du français OVHcloud à Oracle, le même mantra revient : « *La sécurité est une priorité.* »

Alerte de l'Anssi

Car les cybercriminels s'attaquent de plus en plus aux clouds, à mesure que les entreprises sont nombreuses à y héberger des données. Dans un rapport paru début mars, l'Agence nationale de la sécurité des systèmes d'information (Anssi) prévient ainsi les entreprises et les administrations critiques des risques d'attaques liés à « *de nouveaux*

Les Echos
LE QUOTIDIEN DE L'ÉCONOMIE

PAYS :France
PAGE(S) :22
SURFACE :43 %
PERIODICITE :Quotidien

RUBRIQUE :High-tech et medias
DIFFUSION :129052
JOURNALISTE :Florian Dèbes

► 31 mars 2022 - N°23677

usages numériques souvent mal maîtrisés tels que le cloud ».

Les temps ont changé depuis que les vendeurs de cloud ont lancé dans les années 2000 leurs offres en mettant en avant l'argument de la sécurité contre les cyberattaques. Certes, les plateformes cloud restent dans la plupart des cas bien plus sécurisées que les salles informatiques des entreprises. Toutefois, les exemples récents des attaques contre SolarWinds et Kaseya – des logiciels utilisés pour surveiller les systèmes informatiques – et les serveurs de messagerie de Microsoft ont montré qu'aucune technologie n'est infaillible, surtout quand les attaquants peuvent être financés par des Etats.

Les hackers ont par ailleurs appris à repérer les banales erreurs de configuration du cloud. « *Dans le cloud, il y a des centaines de moyens de voler les données en utilisant les services légitimes des plateformes* », relève Avi Shua, le directeur général d'Orca Security. Ces derniers mois, ses équipes spécialisées ont découvert trois vulnérabilités critiques, deux chez AWS et une autre sur Microsoft Azure. Corrigées depuis, elles permettaient à un utilisateur de ces plateformes d'accéder aux données d'autres clients...

Face à ces bévues, les plateformes de cloud développent avec leurs clients un concept de « responsabilité partagée » : tandis qu'elles s'occupent de la sécurité du cœur de leur technologie, les clients sont priés de veiller au bon paramétrage des outils qu'ils utilisent. Mais un problème demeure : d'après une enquête Wavestone, le cloud est l'un des environnements technologiques pour lesquels les équipes de sécurité des entreprises françaises sont le moins préparées. ■

D'après Wavestone, le cloud est l'un des environnements technologiques pour lesquels les équipes de sécurité des entreprises françaises sont le moins préparées.

Shutterstock