

Panne de Gmail et Office 365 : les RSSI appellent à la cyber-résilience

Le climat se tend entre les responsables des systèmes d'information et les plateformes de Cloud. En décembre dernier, les DSI de l'association EuroCIO publiait une étude de satisfaction, menée auprès de ses membres, [très critique](#) sur les contrats passés avec les fournisseurs.

Aujourd'hui, c'est le Club des Experts de la Sécurité de l'Information et du Numérique (CESIN) qui réagit après [les pannes successives](#) de Gmail et d'Office 365. Une occasion de rappeler son nouveau mot d'ordre, largement diffusé lors du [FIC 2019](#) : « la cyber résilience ».

Actant le recours massif au Cloud, le club de RSSI relève que « l'offre en apparence pléthorique (...) repose en pratique sur une poignée d'acteurs du Cloud public majoritairement américains. » et que leurs entreprises françaises se sont ainsi rendus dépendantes du niveau de service qu'ils proposent.

Mesurer les risques du « Cloud first »

« C'est la situation qu'ont connu ces derniers jours un ensemble d'entreprises européennes, victimes d'une panne prolongée de leur messagerie Office 365, avec un impact métier important ; quelques jours après Gmail a également connu un incident d'ampleur. Or l'état vulnérable de ces systèmes ultra concentrés se conjugue avec la cybercriminalité, car à la complexité et la vulnérabilité intrinsèques des architectures s'ajoutent les risques liés aux cyberattaques et à l'espionnage industriel. » s'inquiète le [Cesin](#).

Pas question pour autant de remettre en cause la stratégie

« Cloud first » déployée par de nombreuses entreprises.

Son questionnement est centré sur les enjeux pour sécuriser un système d'information de facto externalisé.

» Les entreprises (...) ne pouvaient plus assumer des infrastructures concentrées en propre. Mais leur risque s'est déplacé et est monté d'un cran au niveau des fournisseurs de cloud. Il convient maintenant à chaque entreprise de l'adresser en développant sa résilience, en limitant les solutions trop monolithiques, en cassant les trop fortes dépendances à un nombre restreint d'acteurs, en introduisant certaines rusticités et solutions de repli alternatives, en créant des zones de respiration des SI et en conservant la maîtrise de quelques éléments fondamentaux, nécessaires à une reconstruction, afin de ne jamais se retrouver en total déséquilibre. » détaille Alain Bouillé, Président du Cesin et RSSI de la Caisse des Dépôts.

Le risque de la concentration du marché

L'association des RSSI pointe deux risques majeurs : la disponibilité/intégrité des systèmes et la concentration du marché sur quelques grands fournisseurs qui « fait évoluer les systèmes d'information vers de nouvelles formes de fragilité ».

Son constat va au delà de la question de la cybersécurité et pointe les dangers d'une trop grande dépendance des entreprises à des fournisseurs de Cloud devenus omnipotents.

« La taille, la complexité et les interdépendances rendent les réparations difficiles à orchestrer dans des délais satisfaisants et compatibles avec les besoins opérationnels, quelles que soient les promesses inscrites dans les contrats. Lorsque le déséquilibre de ces systèmes s'installe, les moyens de secours sont insuffisants face au risque réel et il devient long et complexe de rétablir le fonctionnement nominal. »

Reste à chaque entreprise de trouver sa réponse, le Cesin ne prodigue officiellement aucun conseil.