Faille dans le Cloud : à qui la faute ?

Jeudi dernier (26/08/2021) Microsoft a annoncé avoir corrigé une importante faille de sécurité dans son service Cloud Azure Cosmo DB. Cette vulnérabilité, découverte par des chercheurs de la société Wiz, permettait d'obtenir les clés d'accès aux bases Cosmo DB. Ainsi en l'exploitant, un attaquant aurait pu consulter, modifier ou même supprimer les données des clients de ce service SaaS entrainant ainsi une violation de données à caractère personnel.

Cette affaire pose la question de la responsabilité entre clients et fournisseurs. Dans le cas d'une violation de données à caractère personnel, suite à une faille de sécurité liée non pas à un mauvais paramétrage du client mais à une vulnérabilité critique du service SaaS : à qui incombe la responsabilité selon le RGPD ?

J'ai posé il y a quelques jours la question sur Linkedin et voici l'avis des 132 personnes qui ont bien voulu répondre à ma question :

La question me paraissait relativement facile mais visiblement, au vu des résultats très disparates, elle ne l'était pas. J'ai donc décidé de rédiger cet article pour donner la réponse et surtout pour l'expliquer…

Si nous étions avant le 25 mai 2018, date d'entrée en application du RGPD, la seule et unique bonne réponse aurait été le client (réponse n°2). En effet sous le régime juridique précédent, issu de la directive européenne 95/46/EC transposée en France en 2004, seul le responsable du traitement était responsable aux yeux de la CNIL même lorsque la faute incombait uniquement au fournisseur. La CNIL a par exemple sanctionné la société Hertz en 2017 pour une divulgation de données alors qu'il était clairement établit que c'était son sous-traitant qui avait commis l'erreur.

Oui mais voilà, comme le dit si bien la pub de Krys, ça c'était avant. L'entrée en application du règlement européen sur la protection des données (UE/2016/679) plus connu sous le sigle RGPD a véritablement changé la donne.

Contrairement à la loi I&L de 2004 qui ne mentionnait qu'une seule fois le terme de

sous-traitant dans son article 35 et d'ailleurs juste pour le définir et non pas pour le responsabiliser, le RGPD au contraire implique systématiquement responsable du traitement (data controller) ET sous-traitant (data processor) dans ses exigences. Pour le démontrer, j'ai effectué une petite recherche dans le texte du règlement et j'ai trouvé 171 occurrences de la séquence « le responsable du traitement et/ou le sous-traitant ».

Et oui, la réponse à la question est « Aux deux », c'est-à-dire au client (agissant en tant que responsable du traitement) ET au fournisseur (agissant en tant que sous-traitant). Pourquoi ?

Et bien tout d'abord parce que le responsable du traitement et le sous-traitant ont tout deux une obligation de sécuriser les traitements. L'article 32 du RGPD précise en effet que « le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. »

Alors vous allez me dire, oui mais dans notre cas (faille d'un service SaaS), c'est bien au fournisseur Cloud qu'il incombe de sécuriser le service, le client n'ayant pas la main sur l'infra technique. Oui mais c'est oublier un peu vite l'article 28 (consacré au sous-traitant) qui stipule dès son premier paragraphe que le responsable du traitement doit faire uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées.

En d'autres termes, même s'il parait évident qu'il appartient au fournisseur SaaS de sécuriser son service, s'il ne le fait pas, il faut que le client prouve à l'autorité de contrôle que ce fournisseur présentait pourtant toutes les garanties en matière de sécurité. Et c'est là que les choses se compliquent. Comment faire ? On regardera bien sûr le contrat et les engagements du fournisseur. Le client pourra également s'appuyer sur les garanties annoncées par le fournisseur comme l'adhésion à un code de conduite, un certificat ISO 27001 ou encore la qualification SecNumCloud. Grâce au Cyber Security act, il y aura même prochainement une certification européenne pour attester de la sécurité des fournisseurs Cloud (EUCS – Cloud Services Scheme).

Mais que valent ces garanties aux yeux d'une autorité de contrôle et surtout cela sera-t-il suffisant pour exonérer le client de toute responsabilité ? Rien n'est moins sûr et après investigation, l'autorité de contrôle pourra très bien sanctionner le client ou le sous-traitant ou les deux.

D'autre part, n'oublions pas que le RGPD (article 33) oblige les clients et les fournisseurs à notifier toute violation de données à caractère personnel.
Le client (data controller) doit notifier la violation à l'autorité de contrôle dans

les 72 heures après en avoir pris connaissance. Et bien entendu, s'il ne le fait pas, il encourt une sanction administrative.

Le fournisseur (data processor) doit lui aussi notifier la violation de données mais non pas à l'autorité de contrôle mais au responsable du traitement, c'est-à-dire son client. Et, s'il ne le fait pas, il encourt lui aussi une sanction administrative. Dans le cas du fournisseur, le RGPD n'impose pas un délai maximum de 72h mais précise simplement (article 33 paragraphe 2) « Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance. » On notera qu'il en est de même pour la notification par le responsable du traitement aux personnes physiques concernées par la violation de données. Quelle en est la raison ? Et bien le législateur européen a considéré (à juste titre) que le fait d'obliger le sous-traitant à informer ses clients sous 72h pourrait aggraver la situation en rendant publique une faille non encore totalement corrigée.

Pour conclure, on peut affirmer que dans le cas d'une violation de données à caractère personnel suite à une faille de sécurité d'un service Cloud, la responsabilité incombe à la fois au responsable du traitement (client) et au sous-traitant (fournisseur du service).

Pour les 3 infractions potentielles (insuffisance des clauses contractuelles relatives à la protection des données, violation des règles en matière de sécurité des traitements ou défaut de notification des violations de données), la sanction administrative encourue est de 10 M€ ou de 2% du CA. Pour Microsoft dont le CA worldwide est de 125 Milliards de dollars, cela porte le risque à une amende potentielle de 2,5 milliards de dollars, ce qui serait très largement supérieur à la sanction de 746 M€ infligée à Amazon par la CNPD (l'autorité de contrôle luxembourgeoise) le 16 juillet dernier.