MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

FLASH DGSI #69

novembre 2020

INGÉRENCE ÉCONOMIQUE

LES RISQUES LIÉS A L'HÉBERGEMENT DE DONNÉES DANS LE *CLOUD*

Ce « flash » évoque des actions d'ingérence économique dont des sociétés françaises sont régulièrement victimes. Ayant vocation à illustrer la diversité des situations auxquelles les entreprises sont susceptibles d'être confrontées, il est mis à votre disposition pour vous accompagner dans la diffusion d'une culture de sécurité interne.

Par mesure de discrétion, le récit ne comporte aucune mention permettant d'identifier les entreprises visées.

Pour toute question relative à ce « flash » ou si vous souhaitez nous contacter, merci de vous adresser à : securite-economique@interieur.gouv.fr

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

FLASH DGSI #69
NOVEMBRE 2020

INGÉRENCE ÉCONOMIQUE

LES RISQUES LIÉS À L'HÉBERGEMENT DE DONNÉES DANS LE *CLOUD*

La pratique du *cloud computing*, traduit en français par l'*informatique en nuage*, se caractérise par l'externalisation de services informatiques tels que le stockage, la gestion, la sauvegarde et le partage d'informations et de données. Ces services sont effectués par un prestataire dédié à travers l'utilisation de serveurs informatiques. La question de la protection des données hébergées dans le *cloud* est alors essentielle.

Le *cloud computing* permet aux structures utilisant ce service (entreprises, administrations, etc.) de réaliser d'importantes économies, en réduisant les coûts, notamment ceux liés à l'acquisition de matériels informatiques, de rendre leur fonctionnement plus flexible grâce aux différentes offres de *cloud* qui s'adaptent à leurs besoins, et d'améliorer sensiblement l'accessibilité des outils et des données.

Si le marché du *cloud* est en croissance continue depuis plusieurs années, son emploi s'est fortement intensifié dans le contexte de la crise sanitaire liée à la lutte contre la Covid-19, obligeant de nombreuses entreprises et administrations à s'adapter. Ces entités ont ainsi adopté des solutions de télétravail ou développé les mesures déjà en place afin d'assurer une continuité d'activité. Ces situations ont eu pour conséquence un partage massif de données en ligne.

Bien que nécessaire, l'externalisation de ces services, tels que le stockage de données dans le *cloud,* peut exposer les entreprises et les administrations à :

- des risques de fragilisation en cas de paralysie de leurs activités à la suite d'une défaillance technique ;
- des menaces liées à des cyberattaques ;
- des menaces d'espionnage économique au profit d'un concurrent ou d'une puissance étrangère à travers la captation d'informations stratégiques ou sensibles.

PREMIER EXEMPLE

Au cours du printemps 2020, pendant la période du confinement lié à la crise sanitaire, plusieurs entreprises françaises ont eu recours à une solution gratuite de *cloud* afin de mettre en place une base de données destinée à faciliter la collaboration entre les différents acteurs de leur filière d'activité. Les contributeurs pouvaient notamment y indiquer les coordonnées d'un représentant de leur entreprise

et renseigner de nombreux champs, fournissant ainsi de précieuses informations sur leur société (état des stocks, matériaux et machines utilisés, capacité de production, etc.).

Libre d'accès et téléchargeable gratuitement, notamment en raison d'une mauvaise configuration des options de l'offre *cloud* choisie, ce fichier rassemblait des données stratégiques sur l'activité et la santé économique de nombreuses entités françaises, voire sur l'ensemble de l'écosystème français de ce domaine sensible. En dépit de la bonne intention de départ, cette fuite d'informations, organisée par les entreprises malgré elles, a potentiellement permis à des sociétés concurrentes de récupérer données stratégiques, tout en offrant la possibilité à des entités étrangères de dresser un panorama des capacités françaises dans ce secteur.

DEUXIÈME EXEMPLE

En 2018, préférant voir ses données encadrées et protégées par la législation française, une entité française, qui s'était tournée vers une entreprise étrangère pour héberger ses données dans un *cloud*, a demandé à son prestataire de service de transférer les informations de la société sur des serveurs exclusivement implantés en France. En effet, stockées dans plusieurs pays étrangers, ces données sont soumises à plusieurs législations étrangères et sont ainsi exposées à des risques de captation, notamment dans le cadre de mesures juridiques à portée extraterritoriale. Si le prestataire de service a accepté cette demande, il a toutefois imposé un délai de deux ans pour effectuer la migration de la totalité des données en France.

La crise sanitaire liée à l'épidémie de la Covid-19 a poussé l'entreprise française à privilégier le télétravail pour maintenir son activité. En conséquence, alors que le transfert en France des données n'était toujours pas achevé, la société, afin de maintenir l'activité à distance de ses collaborateurs, a été contrainte d'ajouter de nombreuses données stratégiques et sensibles dans le *cloud* de son prestataire étranger.

Par ailleurs, après avoir relancé son prestataire étranger, l'entité française s'est vue finalement imposer un nouveau délai de deux ans.

TROISIÈME EXEMPLE

Un prestataire de *cloud* a été victime d'une attaque informatique de type *ransomware* chiffrant une partie des données qu'il hébergeait pour ses clients. L'auteur de l'attaque informatique a profité de l'obsolescence de certains systèmes d'exploitation et logiciels utilisés par les clients du prestataire pour accéder aux différents serveurs de ce dernier et ainsi s'attaquer aux données hébergées sur le *cloud*.

Si les offres de sociétés spécialisées présentent des garanties de sécurité, le recours à un prestataire extérieur n'exclut pas les risques d'atteintes à l'intégrité des données des entreprises contractantes.

COMMENTAIRES

En recherche d'économies, d'efficacité et de flexibilité dans la gestion de leurs données, les entreprises françaises privilégient de plus en plus l'utilisation des services de *cloud computing*,

s'exposant ainsi à des risques de captation de leurs données stratégiques dont la divulgation pourrait porter atteinte à leurs intérêts économiques.

Par ailleurs, la prédominance des prestataires étrangers sur le marché du *cloud*, proposant l'hébergement des données sur des serveurs localisés à l'étranger, engendre des risques juridiques pour les entreprises françaises alors soumises à des réglementations étrangères, notamment dans le cadre de lois extraterritoriales.

Dépendant d'un prestataire extérieur, une entreprise peut être momentanément déstabilisée par l'indisponibilité du service informatique et par des failles techniques l'empêchant d'accéder à ses données. Un tel incident peut également entacher son image et susciter la méfiance de ses partenaires d'affaire.

Un bon usage de ces solutions en ligne nécessite donc la mise en œuvre d'une politique de sécurité informatique, de règles comportementales et d'une attention particulière portée au contrat passé avec le prestataire, afin de se prémunir des principaux risques de captations ou d'indisponibilités des données.

PRÉCONISATIONS DE LA DGSI

RECOMMANDATIONS FACE AUX RISQUES INDUITS PAR L'HÉBERGEMENT DES DONNÉES DES ENTREPRISES DANS UN *CLOUD* :

- **Classer ses données en fonction de leur niveau de sensibilité afin d'assurer un meilleur suivi et une meilleure sécurisation de ses informations.** Il convient de différencier les données non sensibles, stockables dans le *cloud,* des informations stratégiques (données financières, listes de clients et de fournisseurs, etc.) à conserver dans des infrastructures internes à l'entreprise.
- **Procéder en interne au chiffrement de l'ensemble des données stockées,** en évitant de recourir à un prestataire extérieur ou au même prestataire que celui chargé du stockage.
- **Favoriser des prestataires français ou européens dont les serveurs sont situés en France ou en Europe.** L'ANSSI fournit sur son site internet la liste des prestataires informatiques français qualifiés.
- **Accorder une attention particulière aux conditions générales de vente et d'utilisation.** Il convient de s'assurer que le contrat ne permet pas le transfert de données hébergées en France vers un pays tiers et de s'assurer que le prestataire met en place les moyens nécessaires à la sécurisation des données qui lui sont confiées.
- **Ne pas avoir recours aux services gratuits d'hébergement de données** et autorisant l'accès aux données hébergées à des fins publicitaires.

- **Limiter les droits des utilisateurs des services *cloud*.** Ne pas utiliser de compte administrateur pour des tâches quotidiennes, surveiller les logs de connexion et assurer une gestion rigoureuse des droits d'accès pour éviter toute usurpation d'identité.
- **Effectuer un audit de sécurité informatique en privilégiant un prestataire de service français ou européen afin d'établir les vulnérabilités des systèmes d'informations de l'entreprise.**
- **Prévoir un Plan de continuité d'activité (PCA) et un Plan de reprise d'activité (PRA)** établissant l'ensemble des procédures qui permettront de relancer l'activité de l'entreprise en cas de faille technique ou en cas de cyberattaque provoquant l'indisponibilité des serveurs informatiques de l'entreprise. Le PCA et le PRA doivent prendre en compte les spécificités du prestataire et ses éventuelles défaillances.
- **Envisager, et si besoin souscrire, une assurance spécifique.**
- **Signaler tout incident à sa hiérarchie et au service informatique compétent.**