Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

INGERENCE ECONOMIQUE

Flash n° 35 – Septembre 2017

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.

Vous comprendrez que, 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

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

Flash n°35 Septembre 2017

Les risques liés à l'hébergement des données dans les *data centers* / le *cloud*

L'augmentation constante de la masse des données hébergées à l'aide des techniques d'informatique en nuage[1] représente un enjeu majeur pour la sécurité des informations sensibles des entreprises.

En effet, les données hébergées dans le nuage sont traitées au sein de centres de données[2] dont la maîtrise par le client est limitée et essentiellement d'ordre contractuel. En particulier, la connaissance de la localisation exacte des données est difficile, celles-ci étant réparties entre plusieurs centres géographiquement distincts (pour des questions de résilience notamment) et faisant l'objet de transferts à des fins de rationalisation et d'optimisation des flux de données.

Ces services permettent aux entreprises de bénéficier de solutions d'hébergement ou de traitement de données souples, évolutives, faciles d'emploi et accessibles en tout point du globe.

Cette forme avancée de sous-traitance de la gestion des systèmes d'information **induit en contrepartie d'importants risques pour la sécurité des données des entreprises, françaises en l'espèce.** Ces données sont en effet susceptibles de faire l'objet d'interceptions ou de captations, à tout moment de leur cycle de vie (au cours de leur acheminement sur Internet, durant leur stockage sur des serveurs à distance, lors du transfert au sein d'un autre centre de données, etc.).

Or, les serveurs situés à l'étranger et notamment ceux des centres de données, sont soumis à la réglementation des États qui les hébergent. Les législations de la plupart des pays prévoient ainsi la possibilité, pour les services de police et de sécurité, d'accéder aux données hébergées sur leur territoire. Par ailleurs, certaines autorités peuvent parfois invoquer un motif de sécurité nationale, ou d'autres impératifs d'ordre public, pour justifier l'accès aux données des clients des prestataires. En effet, certains États, grâce à un cadre juridique adapté et à une définition large des enjeux relevant de la sécurité nationale, peuvent enjoindre les prestataires de leur nationalité, même localisés dans un autre pays, de transmettre des données concernant des clients étrangers.

[1] L'information en nuage ou *cloud computing* se définit comme un « *mode de traitement des données d'un client, dont l'exploitation s'effectue par l'Internet, sous la forme de services fournis par un prestataire* », même si des solutions de *cloud* privé, au sein desquels les données ne transitent qu'à travers le réseau d'un opérateur de télécommunication, peuvent être mises en œuvre.

[2] Un centre de données ou *data center* est un centre d'hébergement et de traitement de données à distance pour les entreprises et les administrations, abritant un nombre important de serveurs et d'équipements informatiques tout en fournissant une sécurité physique et une continuité d'activité.

1er exemple

Un prestataire extra-européen d'hébergement de données a refusé de transmettre à son gouvernement des courriels hébergés sur ses serveurs situés à l'étranger. Si une décision de justice lui a donné raison, cette jurisprudence demeure fragile et d'autres prestataires ont pu se voir contraints de transmettre à leurs autorités des emails stockés en dehors de leur territoire national.

Ainsi, certains pays, qui ont fait de l'économie un enjeu majeur pour leur sécurité nationale, utilisent ces instruments légaux pour collecter des informations relevant de cette sphère d'activité.

2ème exemple

Une société française spécialisée dans la pharmaceutique vétérinaire a choisi d'externaliser le stockage de ses données vers une solution de *cloud* gratuite d'un prestataire étranger.

Il a alors été constaté que l'hébergeur de données étranger était soumis à une législation différente, plus souple en matière de collecte de renseignements. Cette entreprise française comptant par ailleurs parmi ses concurrents plusieurs groupes de la nationalité de l'hébergeur, la société tricolore s'expose ainsi à un risque accru d'espionnage économique de ses données stratégiques.

Commentaires

Les risques de l'hébergement de type *cloud* dans des centres de données restent encore **largement sous-estimés.**

Nombreuses sont les sociétés persuadées que les interceptions/captations de données par des puissances étatiques s'inscrivent exclusivement dans le cadre de la lutte contre le terrorisme ou la criminalité organisée. Elles ne se considèrent ainsi pas menacées par le risque de captation de leurs données stratégiques hébergées dans le *cloud*.

Par ailleurs, les solutions de stockage ou de traitement des données à l'étranger sont parfois considérées comme offrant un plus haut niveau de sécurité et des services plus performants que les solutions nationales. Certains prestataires étrangers proposent à cet égard des fonctionnalités avancées, très prisées des entreprises qui se développent à l'international, et à un moindre coût.

En outre, pour rassurer leurs clients face à la **portée extraterritoriale de certaines législations**, et plus largement aux risques d'interception de leurs données par des gouvernements étrangers, certains prestataires extra-européens ont décidé de confier la gestion de leurs centres de données à des groupes européens. Cette solution apparaît toutefois insuffisante pour garantir la protection des données hébergées. En effet, même si les centres de données sont exploités par des opérateurs européens, des entreprises non-européennes conservent régulièrement la maîtrise de l'architecture matérielle et logicielle des installations.

Préconisations de la DGSI

Face au risque d'interception et aux pratiques de certains prestataires, la DGSI émet les préconisations suivantes pour tenter de limiter les risques de captation du patrimoine informationnel des entreprises utilisant les *datas centers* / le *cloud* :

- S'agissant des centres de données localisés sur le territoire national, veiller à accorder une attention particulière aux conditions générales de vente et d'utilisation. Il convient, pour les entreprises, de s'assurer que le contrat ne permet pas le transfert des données hébergées en France vers un pays tiers.

- Préférer des prestataires français, ou à défaut européens, dont les serveurs sont situés dans l'Hexagone ou dans un pays membre de l'Union européenne.

- Bannir l'utilisation des services, gratuits ou non, d'hébergement dans le *cloud*, autorisant l'accès aux données hébergées à des fins publicitaires.

- Distinguer le traitement des données non sensibles, stockables dans le *cloud*, des informations à forte valeur ajoutée économique, stratégique ou financière, à conserver dans des infrastructures internes à l'entreprise.

- Procéder systématiquement au **chiffrement** de l'ensemble des données transférées sur un service d'hébergement à distance. Ce chiffrement doit être effectué par l'entreprise elle-même et non par ses prestataires, ou via les outils de ces derniers.

- Limiter les droits des utilisateurs des services dans le nuage, ne pas utiliser de compte administrateur pour les tâches quotidiennes, surveiller les logs de connexion et assurer une gestion rigoureuse des droits d'accès pour éviter toute usurpation d'identité.

- Procéder à un audit des infrastructures techniques hébergeant les données de l'entreprise et s'assurer du respect des stipulations contractuelles.

- Contacter la DGSI en cas de découverte ou de suspicion d'un cas d'ingérence ou d'interception de données.