A Puteaux le 11 juin 2024

15 critères pour évaluer la confiance numérique d'une solution d'hébergement

Face à l'abondance de solutions, notamment d'hébergement de cloud, qui utilisent indifféremment les termes de confiance numérique et de souveraineté, le Clusif a souhaité clarifier les deux concepts et déterminer 15 critères permettant d'objectiver le niveau de confiance numérique d'une solution d'hébergement.

Contexte : l'adoption massive du cloud

Les entreprises et les administrations, qui hébergent leurs actifs sensibles et d'usage dans leurs propres infrastructures sur site (« *on-premise* ») ou dans des infrastructures hors site (« *off-premise* »), les déplacent progressivement vers des infrastructures de cloud dans le cadre de leur stratégie « priorité au cloud » traduit « *Cloud first* ».

Les données comptent parmi les principaux actifs des organisations en termes de savoir, de savoir-faire bien sûr, mais aussi d'enjeux économiques qui engagent même parfois leur pérennité même.

Dans un tel contexte, les organisations identifient et classifie les données et les services rendus ou utilisés les plus importants et mettent en œuvre les mesures de prévention et de protection associées tant en termes techniques que juridiques.

Un choix qui s'opère dans un flou relatif

Le cloud offre flexibilité et passage à l'échelle aux différentes organisations, mais ce n'est pas sans risques, techniques et juridiques.

Sur le marché du numérique, on parle d'offres dites de « confiance » et « souveraines », sans définition distinctive partagée. Ce flou est particulièrement présent pour les environnements cloud.

Deux concepts clés

Afin d'éclairer le débat, nous proposons de définir la confiance numérique comme un concept qui vise à garantir un niveau de préservation des intérêts des organisations et de leurs utilisateurs en matière de services et de protection des données. Ce concept présente des limites lorsqu'il s'agit de répondre aux impératifs d'indépendance, de résilience et d'immunité face aux menaces institutionnalisées provenant de puissances étrangères. Il ne semble pas donc pas suffisant pour répondre aux besoins de services et d'hébergement de données relevant du domaine régalien (souverain) ou pour les organisations dont les activités

nécessitent un niveau de sécurité accru, notamment en matière de protection de savoir et de savoir-faire, ou des données classifiées comme sensibles par les entreprises (données stratégiques).

Par conséquent, nous définissons la souveraineté numérique comme visant à garantir la préservation des intérêts fondamentaux d'un État ainsi que ceux de ses organisations nationales et de leurs utilisateurs en matière de services et de protection des données. La souveraineté numérique permet de répondre à l'impérieux besoin d'indépendance, d'autonomie stratégique, de résilience et d'immunité face aux menaces institutionnalisées provenant de puissances étrangères. Au niveau des organisations, la souveraineté numérique se traduit par la capacité à être autonome et indépendant de toute contrainte externe. Elle englobe également le contrôle sur les données et les services consommés, garantissant qu'ils ne sont soumis qu'aux lois et règlements géographiques locaux du consommateur et des données. La disponibilité des services doit être maîtrisée dans le temps, même en cas de changement de contexte géopolitique[8]. Le niveau de protection des données peut être considéré comme élevé, à condition de respecter les normes les plus strictes. Ces données sont considérées comme étant non soumises à un autre État que celui du fournisseur du service cloud et/ou via ses technologies en présence, grâce à leur immunité aux cadres légaux extraterritoriaux et à toute forme de dépendance technologique.

La souveraineté numérique vise également à prévenir les fuites de valeur économique pour les acteurs dont cet enjeu est stratégique pour leurs activités.

Le concept de souveraineté numérique est donc particulièrement adapté pour répondre aux besoins de services et d'hébergement de données relevant du domaine régalien. Il s'applique également aux organisations dont les activités nécessitent un niveau de sécurité accru.

Le concept de souveraineté est donc un cadre renforcé et complémentaire à celui de la confiance numérique. Les deux concepts sont imbriqués.

Les risques associés

L'espionnage, la saisie légale, le sabotage et l'indisponibilité des services ou des informations comptent parmi les principaux risques auxquels les organisations sont déjà confrontées en matière de sécurité. Ces risques se retrouvent dans les différentes infrastructures « *on-premise* », « *off-premise* » et cloud.

La transition vers le cloud alimente des risques stratégiques :

- Les transferts de données à caractère personnels non maîtrisés en dehors de la juridiction nationale.
- La captation de données par un organisme étranger par l'usage par un Etat d'une loi extraterritoriale ou l'exploitation de technologies vulnérables ou backdoors.
- La survenance d'incidents ou de défaillances, voire de restrictions de services liées à la dépendance à une technologie ou à un service non national.
- L'absence de prise en compte suffisante de la sécurité dans les offres Cloud
- L'espionnage facilité par l'absence de garanties de maîtrisé des accès aux équipements physiques et serveurs.
- Le manque de réversibilité et de portabilité augmentant la dépendance et freinant l'innovation.

Les solutions qualifiées « SecNumCloud » par l'ANSSI ou équivalent à l'échelle Européenne restent bien entendu à privilégier pour des solutions Cloud.

La souveraineté : un terme qui n’est pas à utiliser à la légère

Comme nous en proposions plus haut la définition, la souveraineté engage la sphère régalienne et répond donc à une série de critères qui ne sont pas forcément accessibles à l’acheteur final. C’est pourquoi le Clusif préconise plutôt de choisir une solution qui réponde aux critères de confiance numérique adaptée à l’activité de l’organisation :

- Localisation physique des Datacenters
- Localisation des données (transit, repos, utilisation)
- Localisation des services et applications tierces
- Localisation des équipes d'admin / exploitation
- Localisation des sous-traitants
- Localisation si chaîne de sous-traitance
- Localisation des personnes à accès à privilèges
- Localisation des supervisions / sauvegardes
- Localisation du siège de la société
- Nationalité des services ou produits utilisés
- Nationalité du ou des hébergeurs
- Nationalité des personnels à accès techniques
- Nationalité des fonds de capitaux
- Montage juridique de la société / entité
- Certifications pour l'hébergeur

L’heure du choix d’une solution

Définir plus précisément le niveau de confiance d’une solution d’hébergement est un préalable méthodologique important mais il ne couvre pas l’intégralité du besoin des organisations. A l’heure du choix d’une solution, plusieurs critères se conjuguent voire s’affrontent.

Pour aider à la décision, le Clusif a donc travaillé sur une **grille d’évaluation** des besoins des organisations en matière d’hébergement de leurs données et publie un guide complet sur le sujet. Ce guide sera d’abord réservé aux adhérents de l’association puis sera rendu disponible en accès libre sur notre site.

Campus Cyber
Tour Eria – 5 rue Bellini – 92821 Puteaux cedex
France
✆ +33 1 53 25 08 80
clusif@clusif.fr

clusif.fr