RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

RECOMMANDATIONS POUR L'HÉBERGEMENT DANS LE CLOUD DES SYSTÈMES D'INFORMATION SENSIBLES

SOMMAIRE

1 LE CLOUD, UNE OPPORTUNITÉ ET UN DÉFI

Le *cloud computing* est une technologie particulièrement structurante pour nos usages numériques, à laquelle les secteurs privés et publics ont de plus en plus recours. Ce constat s'explique notamment par les opportunités et l'effet levier apportés par cette technologie dans la transformation numérique.

Son recours représente cependant un enjeu de sécurité pour nos données, pour les systèmes d'information en général et en particulier pour les plus sensibles. L'état de la menace démontre en effet que les attaquants ont, depuis plusieurs années, identifié les offreurs de solutions cloud et leurs infrastructures comme des cibles d'intérêt pour la conduite d'attaques informatiques. Les infrastructures sont ciblées en raison de la concentration des données et des traitements qu'elles hébergent, et du fait de l'usage de solutions de virtualisation et d'administration mutualisées. Une menace qui comprend également l'application de lois extraterritoriales, imposant aux hébergeurs, soumis à ces lois, l'obligation de transmettre à leurs autorités les données de leurs clients.

Cette évolution des usages conduit les entités des secteurs public et privé à s'interroger sur la sélection d'offres de cloud adaptées en fonction des spécificités de leurs systèmes d'information.

2 UN OUTIL D'AIDE À LA DÉCISION

Pour répondre à cet enjeu, l'ANSSI a développé des recommandations pour l'hébergement dans le cloud qui précise, en fonction du type de système d'information, de la sensibilité des données et du niveau de la menace associé, les types d'offres cloud à privilégier.

Ces recommandations constituent un outil d'aide à la décision pour les entités qui envisagent un hébergement cloud pour leurs systèmes d'information (SI) de niveau diffusion restreinte, les SI sensibles des opérateurs d'importance vitale et des opérateurs de services essentiels, ainsi que les systèmes d'information d'importance vitale (SIIV). Il est à noter qu'elles ne s'appliquent pas aux systèmes d'information classifiés et que tous les systèmes d'information n'ont pas vocation à recourir aux solutions cloud. Elle s'inscrit, par ailleurs, en cohérence avec la doctrine « **cloud au centre** » de l'État, dont la mise en œuvre est animée par la direction interministérielle du numérique (DINUM).

3 PRÉCAUTIONS D'EMPLOI

L'utilisation de ces recommandations pour l'hébergement dans le cloud suppose qu'un certain nombre de précautions soient prises en compte par les entités dans leur projet de migration.

Étude d'impact et analyse de risques

La décision de migrer des systèmes d'information vers des solutions cloud relève de la plus haute autorité de l'entité. L'ANSSI recommande qu'elle soit éclairée par une étude d'impact, notamment métier et juridique, ainsi qu'une analyse de risques. Cette dernière peut considérer *a minima* :

- le niveau de menace maximal auquel sont exposés les différents systèmes d'information ;
- les risques spécifiques de l'hébergement cloud (exemple : l'exposition des services à internet et la mutualisation des infrastructures avec d'autres clients) ;
- la sensibilité des traitements et des données concernés, en considérant notamment les aspects de confidentialité, d'intégrité et de disponibilité ;
- les risques juridiques liés à la portée extraterritoriale des lois. Certains fournisseurs de cloud peuvent, en effet, être soumis à des législations extraterritoriales imposant le transfert des données à leurs autorités nationales.

Sélection des mécanismes de sécurisation du cloud

L'ANSSI recommande aux entités, quel que soit le type d'offres retenu, de sélectionner des services et licences pertinents afin de disposer des options et mécanismes de sécurité adaptés à leur besoin.

Il est notamment important pour le client de réaliser un certain nombre d'actions qui restent de sa responsabilité, notamment pour configurer les options de sécurité. A titre d'exemple, le déploiement ou la migration d'un système d'information sur une infrastructure cloud nécessitera la configuration les services de filtrage et de contrôle d'accès, pour s'assurer que seule les personnes légitimes accèdent aux interfaces d'administration et de supervision de sa solution.

Il est, par ailleurs, important de prévoir une clause de réversibilité permettant de faciliter la migration d'une technologie cloud vers une autre afin de limiter la dépendance à une seule offre cloud, et à ses évolutions fonctionnelles et de sécurité.

Formation des équipes

Il est enfin recommandé par l'ANSSI que la formation des équipes techniques et de la chefferie de projet à l'usage des technologies cloud dans le cadre d'un projet de migration soit prise en compte. Cette précaution contribuera à assurer la qualité de l'étude de la migration du système d'information vers un hébergement cloud, ainsi que la maîtrise des coûts et les délais. Elle permettra également d'étudier, de manière exhaustive, l'ensemble des aspects techniques et organisationnels de la migration.

4 LES OUTILS NÉCESSAIRES À L'APPLICATION DE CES RECOMMANDATIONS ET LA TERMINOLOGIE ASSOCIÉE

Les recommandations pour l'hébergement dans le cloud de l'ANSSI repose sur trois éléments clés :

- **La typologie des offres cloud ;**
- **L'état de la menace ;**
- **La nature des systèmes d'information.**

En fonction de la nature des systèmes d'information, des données et traitements concernés, la menace pourra différer nécessitant de recourir à un type d'offre cloud plus qu'à un autre. Ces trois éléments, détaillés ci-après, doivent être pris en compte dans toute décision concernant la migration des systèmes d'information vers des solutions cloud.

La typologie des offres cloud

La typologie des offres cloud sur laquelle s'est appuyée l'ANSSI pour ses recommandations comprend deux principales catégories (commerciales et non commerciales), avec des offres répondant chacune à des besoins spécifiques. À noter que le terme « offre cloud » comprend les *Infrastructure as a Service* (*IaaS*), les *Platform as a Service* (*PaaS*), les *Containers as a Service* (*CaaS*), ainsi que les *Software as a Service* (*SaaS*).

TYPOLOGIE DES OFFRES CLOUD		DESCRIPTIF
OFFRES CLOUD COMMERCIALES	**Publique**	Offre cloud mutualisée pour l'ensemble des clients de l'offreur.
	Privée	Offre cloud dont les ressources (processeur, réseau et stockage) sont physiquement dédiées à l'entité souscrivant à l'offre.
	Communautaire	Offre cloud physiquement dédiée à un ensemble d'entités d'intérêt commun qu'elles soient étatiques ou privées.
OFFRES CLOUD NON COMMERCIALES	**Interne**	Offre cloud déployée en interne d'une entité pour ses besoins propres. L'exploitation et la supervision des infrastructures peuvent être assurées par l'entité ou par un sous-traitant.
	Communautaire	Dans certains cas particuliers, des entités d'un même secteur d'activité peuvent constituer avec leurs ressources propres un cloud communautaire. Cette infrastructure pourra alors être considérée comme communautaire et interne. À titre d'exemple, pour l'État, il existe deux offres cloud internes et communautaires : Pi et Nubo

NOTE : L'usage du cloud conduit progressivement à la transformation de l'architecture des systèmes d'information vers leur hybridation. Les entités peuvent, en effet, recourir à différentes offres cloud en fonction de leur besoin et en complément de leurs infrastructures internes classiques.

La typologie des menaces

Le deuxième élément clé des recommandations de l'ANSSI repose sur l'état de la menace. Il est en effet important, en fonction du projet de migration envisagé, d'évaluer le niveau de menace maximal auquel est exposé le système d'information, ainsi que les données et traitements concernés. L'ANSSI met à disposition, ci-après, sa typologie des menaces cyber.

TYPOLOGIE DES MENACES	DESCRIPTIF
MENACE STRATÉGIQUE	Cette menace s'illustre par la conduite d'**attaques informatiques persistantes et ciblées, menées ou financées par un État**. Elle est caractérisée par des **moyens techniques et organisationnels importants**, ainsi qu'un effort de discrétion. Ces attaques peuvent être conduites à des fins d'**espionnage, de pré-positionnement ou de déstabilisation** (exemple : actions de sabotage informatique ou divulgation de données). À noter que le recours par certains États à des **lois extraterritoriales** ou à des législations spécifiques, peut faciliter l'accès à des données hébergées dans le cloud sans nécessiter d'attaque informatique. Les hébergeurs, soumis à ces lois ont, en effet, l'obligation de transmettre à leurs autorités les données de leurs clients, sans voie de recours ou même d'information de ces derniers.
MENACE SYSTÉMIQUE	Les menaces **systémiques** sont susceptibles d'affecter une large proportion d'entités. Elles incluent la **menace cybercriminelle**, caractérisée par la conduite d'**attaques informatiques** majoritairement **opportunistes**. Ces attaques sont généralement conduites à des **fins lucratives** et peuvent se matérialiser par des **rançongiciels** ou des **fraudes**. Ces menaces sont également représentées par la **prolifération d'outils et de services** offensifs disponibles **sur étagère** ou commercialisés par des **entreprises privées**. Ces services peuvent être utilisés dans des actions d'**intelligence économique** ou d'**espionnage industriel**, ou permettre à certains États aux ressources limitées d'accéder à des **capacités offensives**.
MENACE HACKTIVISTE OU ISOLÉE	Cette menace s'illustre par la conduite d'attaques menées par un individu **isolé** ou un **groupe hacktiviste** à des fins de **déstabilisation** (par vengeance, par motif idéologique, etc.). Les moyens mis en œuvre incluent notamment des attaques par déni de service (DDoS) [1] ou des fuites de données. La **menace isolée** comprend également des individus utilisant des outils peu sophistiqués ou bénéficiant d'**accès privilégiés au sein d'une entité**, mais disposant de **peu de moyens**.

1 On parle de « déni de service distribué » (de l'anglais Distributed Denial of Service ou DDoS) lorsqu'une attaque fait intervenir un réseau de machines (souvent compromises) afin d'interrompre le ou les services visés comme un site web.

FOCUS SUR LE RÉFÉRENTIEL ET LA QUALIFICATION SECNUMCLOUD

Élaboré par l'ANSSI, le référentiel SecNumCloud propose un ensemble de règles de sécurité et de bonnes pratiques d'hygiène informatique, garantissant un haut niveau d'exigence tant du point de vue technique, qu'opérationnel ou juridique.

La qualification de sécurité SecNumCloud attribuée par l'ANSSI, basée sur ce référentiel, reconnaît des offres proposées par des opérateurs cloud : services en *PaaS*, *IaaS* ou *Saas*. À noter que la qualification SecNumCloud apporte une confiance sur l'offre cloud, ainsi que sur les pratiques d'exploitation des offreurs qualifiés. Elle ne préjuge en revanche pas du niveau de sécurité des services numériques des clients qui seront portés par ces offres cloud.

Ainsi, l'hébergement d'un site web sur une offre qualifiée n'enlève pas la nécessité de sécuriser le site web en lui-même. Si les mesures de base de sécurisation d'un site web ne sont pas appliquées, le risque de compromission du site restera élevé. A titre d'exemple l'application des correctifs de sécurité sur un site internet face à une vulnérabilité particulièrement exploitée sur les technologies web, comme des injections SQL [2], ne relève pas de l'hébergement qualifié SecNumCloud, mais doit être prise en compte par le client [3].

Ce « Visa de sécurité » permet aux utilisateurs d'identifier des offres cloud qui visent à protéger les données et les traitements sensibles face à la menace cybercriminelle et à l'application de lois extraterritoriales. À noter que la qualification d'une offre permet également de faciliter les processus d'homologation des services numériques des entités clientes qui, dès lors, disposeront d'un certain niveau de garantie sur les infrastructures sous-jacentes. Les offres cloud qualifiées SecNumCloud sont listées sur **le site internet de l'ANSSI**.

---

2 Des injections SQL sont un type de vulnérabilité permettant à un attaquant de manipuler une base de données et accéder à des informations potentiellement importantes.

3 La sécurisation de ces services numériques, la configuration de l'offre et des options de configuration retenues restent à la charge des entités (cf. partie « Précautions d'emploi »).

La nature des systèmes d'information

Enfin, le troisième élément clé des recommandations de l'ANSSI repose sur la nature des systèmes d'information concernés. Les systèmes d'information sensibles de l'État, des opérateurs d'importance vitale et des opérateurs de services essentiels, ainsi que les réseaux de niveau diffusion restreinte sont par nature des cibles d'intérêt pour la conduite d'attaques à des fins d'espionnage ou lucratives. Les systèmes d'information d'importance vitale (SIIV), de par la sensibilité de leurs données et traitements, présentent un intérêt particulier et systématique pour des acteurs offensifs de niveau stratégique. Il est donc nécessaire de prendre en compte la nature du système d'information.

TYPOLOGIE DES SYSTÈMES D'INFORMATION	DESCRIPTIF
Systèmes d'information de niveau **diffusion restreinte** (DR)	Il s'agit des systèmes d'information traitant des données *diffusion restreinte* [4].
Systèmes d'information **sensibles relevant de la** doctrine cloud au centre de l'État	Il s'agit des systèmes d'information, hors SIIV, qui traitent des données sensibles au sens de la circulaire cloud au centre.
Systèmes d'information sensibles des **opérateurs d'importance vitale** (OIV) [5] et des **opérateurs de services essentiels** (OSE) [6]	Il s'agit des systèmes d'information qui ne sont pas réglementés à l'image des SIIV, mais qui restent considérés comme sensibles en raison de la nature des données traitées.
Systèmes d'information **d'importance vitale (SIIV)**	Il s'agit des systèmes d'information pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou pourrait présenter un danger grave pour la population [7].

4 Au sens de l'instruction générale interministérielle (IGI) 1300.
5 Voir la FAQ - Systèmes d'information d'importance vitale | ANSSI (cyber.gouv.fr)
6 Voir la FAQ - opérateurs de services essentiels (OSE) | ANSSI (cyber.gouv.fr)
7 Voir article L. 1332-6-1 du code de la défense.

5 APPLICATION DES RECOMMANDATIONS

En s'appuyant sur son expérience et expertise, l'ANSSI définit pour les quatre systèmes d'information présentés ci-dessus, en fonction de la sensibilité des traitements et données, ainsi que du niveau de la menace associé, les recommandations suivantes.

SI sensible de niveau DR

- L'ANSSI préconise les offres **cloud qualifiées SecNumCloud non commerciales (internes et communautaires) et, commerciales privées** permettant de disposer d'une **infrastructure dédiée** évitant le risque de latéralisation d'un attaquant depuis l'environnement d'un client vers un autre.
- **Les offres cloud qualifiées commerciales qu'elles soient communautaires ou publiques peuvent être toutefois envisagées**, elles supposent cependant une mutualisation des ressources informatiques avec d'autres clients (exemple : les clients stockent leurs données sur une même ressource de stockage physique ou hébergent leur site web sur les mêmes serveurs physiques).

L'externalisation de l'hébergement, reposant sur une offre cloud commerciale qualifiée SecNumCloud, relève de la décision de l'entité pour ce type de système d'information. L'ANSSI recommande d'appuyer cette décision sur une analyse de risques argumentée **démontrant que la solution est protégée au niveau adéquat**.

À noter que dès lors que l'accès à une information est conditionné par la nationalité (exemple : information *Diffusion Restreinte - Spécial France*), une attention particulière doit être portée au lieu d'hébergement et à la nationalité des administrateurs. Une offre cloud non commerciale peut s'avérer plus adaptée pour répondre à cette exigence de l'IGI 1300.

SI sensible relevant de la doctrine cloud au centre de l'État

- Conformément à la « **doctrine cloud au centre** » de l'État, leur hébergement **n'est autorisé que** dans les offres cloud **qualifiées SecNumCloud (internes, privées, communautaires ou publiques)**.

SI sensible d'un opérateur d'importance vitale et SI sensible d'un opérateur de services essentiels (dont les systèmes d'information essentiels)

- L'ANSSI **préconise** tout type d'offres **qualifiées** SecNumCloud.

SI d'importance vitale

En raison de la sensibilité des traitements et des données qu'il traite, le SIIV est un cas particulier qui doit faire l'objet d'une décision motivée relevant du responsable de l'entité concernée.

- Pour les SIIV compatibles avec les technologies cloud, l'ANSSI **préconise** les offres **cloud qualifiées SecNumCloud non commerciales (internes et communautaires) et commerciales privées**, permettant de disposer d'une infrastructure dédiée évitant le risque de latéralisation d'un attaquant depuis l'environnement d'un client vers un autre.
- L'ANSSI ne s'opposera pas à un autre type d'offre cloud commerciale, à condition :
  1. qu'elle soit qualifiée SecNumCloud ;
  2. que le responsable de l'entité appuie sa décision sur une analyse de risques argumentée sur l'externalisation de l'hébergement de son SIIV et que les obligations réglementaires applicables [8] aux SIIV soient respectées.

8 La sécurité des SIIV est encadrée par des mesures réglementaires imposant une maîtrise des risques adaptée à une menace ciblant les intérêts fondamentaux de la Nation.

Version 1.0 – Juillet 2024 – ISSN en cours

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.cyber.gouv.fr — communication@ssi.gouv.fr