SECNUMCLOUD

PRÉSENTATION DU RÉFÉRENTIEL

VERSION 3.2

FONDEMENT

- Élaboré en 2016 par l'ANSSI, le référentiel « SecNumCloud » permet la qualification de prestataires de services d'informatique en nuage, plus couramment dénommés « cloud », avec pour objectif de promouvoir, enrichir et améliorer l'offre de prestataires de confiance à destination des entités publiques et privées souhaitant externaliser l'hébergement de leurs données, applications ou systèmes d'information

PRINCIPE

- Appliquer un référentiel de sécurité pour les activités Cloud
- *Obtenir une qualification de l'ANSSI*
- *Plus protecteur face aux lois extra-européennes*
  - ✓ *La version 3.2 de SecNumCloud explicite des critères de protection vis-à-vis des lois extra-européennes. Ces exigences garantissent ainsi que le fournisseur de services cloud et les données qu'il traite ne peuvent être soumis à des lois non européennes.*
  - ✓ *SecNumCloud 3.2 intègre également le retour d'expérience des premières évaluations et précise l'exigence relative à la mise en œuvre de tests d'intrusion tout au long du cycle de vie de la qualification*

STRATÉGIE D'ÉVALUATION

- *Tous les services de Cloud peuvent prétendre à la qualification SecNumCloud. En effet, la qualification est adaptable aux différentes offres : SaaS (Software as a Service), PaaS (Plateform as a Service) et IaaS (Infrastructure as a Service)*
- *Accompagnement de l'ANSSI*

LES LOIS EXTRA-EUROPÉENNE – PATRIOT ACT / CLOUD ACT

- Patriot Act

  Né suite aux attentats du 11 septembre 2001, a pour vocation de détecter et combattre le terrorisme.

  Cette loi octroie des pouvoirs extraordinaires au département de la Justice, à la NSA et à d'autres agences fédérales sur la surveillance intérieure et internationale des communications électroniques.

  Elle élimine les obstacles juridiques qui empêchaient les services de police, de renseignements et de défense de partager leurs informations relatives aux menaces terroristes potentielles et de coordonner leurs efforts pour lutter contre ces menaces.

  La loi comprend 10 catégories, appelées "titres", comprenant :
  Titre I : Renforcer la sécurité intérieure contre le terrorisme
  Titre II : Procédures de surveillance renforcées
  Titre III : Lutte contre le blanchiment d'argent pour prévenir le terrorisme
  Titre IV : Sécurité des frontières
  Titre V : Supprimer les obstacles aux enquêtes sur le terrorisme
  Titre VI : Aide aux victimes et familles de victimes du terrorisme
  Titre VII : Partage accru de l'information pour la protection des infrastructures essentielles
  Titre VIII : Renforcement du droit pénal contre le terrorisme
  Titre IX : Amélioration du renseignement
  Titre X : Divers

  Affaire Snowden 2013

LES LOIS EXTRA-EUROPÉENNE – PATRIOT ACT / CLOUD ACT

- Cloud Act

  La genèse du Cloud Act émanait d'un contentieux entre l'entreprise Microsoft et le gouvernement des États-Unis d'Amérique. Ce dernier sollicitait certaines données numériques hébergées chez la multinationale de Bill Gates.

  Le Cloud Act est un ensemble de lois permettant aux États-Unis la libre exploitation des données digitales de personnes étrangères à travers des entreprises américaines (Facebook, Google, Microsoft, Amazone)

  Le Cloud Act concerne toutes les institutions de droit américain quel que soit son lieu d'implantation. Cela inclut les prestataires d'hébergement basés sur le sol américain ou de nationalité américaine et dans n'importe quel autre pays.

  Un champ d'application plus large que le Patriot Act.

  Un danger pour la souveraineté des entreprises européennes.

LES LOIS EXTRA-EUROPÉENNE – PATRIOT ACT / CLOUD ACT

- Cloud Act + Patriot Act

  Une menace forte pour la souveraineté des entreprises, accentuée par la domination américaine sur le Cloud. Pour se défendre

  RGDP et SECNUMCLOUD

  Ainsi, dans l'article 48 du RGPD, il est énoncé que « Toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre ».

  L'arrêt « Schrems II » de la Cour de justice de l'Union européenne a rappelé l'exigence de garantir une protection équivalente à celle offerte par le règlement général sur la protection des données (RGPD) lorsque des données personnelles de citoyens européens sont transférées hors de l'Union européenne (UE). Par ailleurs, et indépendamment de l'existence de transferts, certaines législations extraterritoriales n'offrant pas un niveau de protection essentiellement équivalent à celui garanti par le RGPD peuvent s'appliquer aux données stockées par les fournisseurs de cloud sur le territoire de l'UE. SecNumCloud 3.2 fournit à cet égard des garanties fortes en matière de protection vis-à-vis des législations non-européennes à portée extraterritoriale. Ces garanties permettront aux clients des offres de cloud qualifiées d'assurer leur conformité aux suites de l'arrêt « Schrems II » tout en écartant le risque d'un accès étranger incompatible avec le RGPD.

SECNUMCLOUD

- Périmètre
  - ✓ Fourniture de Service SaaS

Ce service concerne la mise à disposition par le prestataire d'applications hébergées sur une plateforme d'informatique en nuage. Le commanditaire n'a pas la maitrise de la plateforme en nuage sous-jacente. Le prestataire gère de façon transparente pour le commanditaire l'ensemble des aspects techniques requérant des compétences informatiques. Le commanditaire garde la possibilité d'effectuer quelques paramétrages métier dans l'application.

  - ✓ Fourniture de services PaaS

Ce service concerne la mise à disposition par le prestataire de plateformes d'hébergement d'applications. Le commanditaire n'a pas la maitrise de l'infrastructure technique sous-jacente, gérée et contrôlée par le prestataire (réseau, serveurs, OS, stockage, etc.). Le commanditaire a cependant la maitrise des applications déployées sur cette plateforme.

  - ✓ **Fourniture de services CaaS**

Ce service concerne la mise à disposition d'outils permettant le déploiement et l'orchestration de conteneurs. Le commanditaire n'a pas la maîtrise de l'infrastructure technique sous-jacente (réseau, stockage, serveurs, système d'exploitation), gérée et contrôlée par le prestataire. Le commanditaire a cependant la maîtrise des outils systèmes, bibliothèques, intergiciels, et du code de l'application.

  - ✓ **Fourniture de services IaaS**

Ce service concerne la mise à disposition de ressources informatiques abstraites (puissance CPU, mémoire, stockage etc.). Le modèle IaaS permet au commanditaire de disposer de ressources externalisées, potentiellement virtualisées. Ce dernier garde le contrôle sur le système d'exploitation (OS), le stockage, les applications déployées ainsi que sur certains composants réseau (pare-feu, par exemple).

SECNUMCLOUD

- Niveau de sécurité
  - ✓ Le respect des exigences du référentiel SecNumCloud a pour objectif l'atteinte d'un niveau de sécurité permettant le stockage et le traitement de données pour lesquelles un incident de sécurité aurait une conséquence significative pour le commanditaire. Il assure notamment le respect des bonnes pratiques de sécurité relevant de l'hygiène informatique, telles que décrites dans le guide [HYGIENE] de l'ANSSI.
  - ✓ Le recours, par le commanditaire, à un service qualifié SecNumCloud pour l'hébergement de données soumises à des exigences légales ou règlementaires (telles que les données de niveau Diffusion Restreinte, les données de santé, Les données liées aux OSE, etc.) nécessite le respect d'exigences complémentaires, qui doivent entre déterminées dans le cadre d'une démarche d'homologation comprenant notamment une appréciation des risques

SECNUMCLOUD

- PSI

  Le prestataire doit rédiger une Politique de Sécurité de l'information. La PSI La politique de sécurité de l'information doit notamment couvrir les thèmes abordes aux chapitres 6 à 19 du référentiel.

  Approuvée par la Direction avec engagement et revue annuellement ou lors de chaque changement majeur pouvant affecter le service

SECNUMCLOUD

- **Appréciation des risques**

  Le prestataire doit produire une analyse de risque, intégrant

  - ✓ la gestion d'informations du commanditaire ayant des besoins de sécurité différents ;
  - ✓ les risques ayant des impacts sur les droits et libertés des personnes concernées en cas d'accès non autorisé, de modification non désirée et de disparition de données à caractère personnel ;
  - ✓ les risques de défaillance des mécanismes de cloisonnement des ressources de l'infrastructure technique (mémoire, calcul, stockage, réseau) partagées entre les commanditaires ;
  - ✓ les risques liés à l'effacement incomplet ou non sécurisé des données stockées sur les espaces de mémoire ou de stockage partagés entre commanditaires, en particulier lors des réallocations des espaces de mémoire et de stockage ;
  - ✓ les risques liés à l'exposition des interfaces d'administration sur un réseau public ;
  - ✓ les risques d'atteinte à la confidentialité des données des commanditaires par des tiers impliqués dans la fourniture du service (fournisseurs, sous-traitants, etc.) :
  - ✓ les risques liés aux événements naturels et sinistres physiques ;
  - ✓ les risques liés à la séparation des taches (voir 6.2.a) ;
  - ✓ les risques liés aux environnements de développement (voir 14.4.b).
  - ✓ Intégrer les exigences légales et réglementaires

  Les risques résiduels doivent être validés par la direction

  L'analyse des risques doit être revues annuellement ou lors de tout changement de l'environnement

SECNUMCLOUD

- Le prestataire doit organiser la gouvernance de la sécurité
  - RSSI
  - Documenté
  - Lien RGPD (DPO)
  - Analyse d'impact
  - Assurer la séparation des tâches
  - Assurer la relation avec les autorités, et dans les groupes de sécurité
  - Assurer la sécurité dans les projets

SECNUMCLOUD

- Le prestataire doit

  Assurer la sécurité dans les ressources humaines;

  Mettre en place une gestion des actifs;

  Mettre en place le contrôle d'accès et la gestion des identités

  - ✓ Politique de contrôle d'accès
  - ✓ Enregistrement des désinscription des utilisateurs
  - ✓ Gestion des droits d'accès
  - ✓ Effectuer des revues d'accès
  - ✓ Gérer l'authentification des utilisateurs
  - ✓ Assurer l'accès aux interfaces d'administration notamment par des outils distincts, cloisonné, MFA
  - ✓ Intégrer les différents services SaaS, PaaS, CaaS, IaaS dans la gestion de l'administration
  - ✓ Restreindre l'accès à l'information

SECNUMCLOUD

- Le prestataire doit

  Assurer le chiffrement des données, des flux, le hachage des mots de passe, la non répudiation, la gestion des secrets, s'assurer des racines de confiance;

  Mettre en place la sécurité physique et environnementale;

  Assurer la sécurité liée à l'exploitation

  - ✓ Procédures d'exploitation documentées
  - ✓ Gestion des changements
  - ✓ Séparation des environnements tests, développement et exploitation
  - ✓ Mesures contre les codes malveillants
  - ✓ Sauvegarde de l'information
  - ✓ Journalisation des événements
  - ✓ Protection de l'information journalisée
  - ✓ Synchronisation des horloges
  - ✓ Analyse et corrélation des événements
  - ✓ Gérer les installations de logiciels
  - ✓ Gérer les vulnérabilités techniques
  - ✓ Procédure d'administration
  - ✓ MCO de l'infrastructure
  - ✓ Surveillance des flux E/S de l'infra

SECNUMCLOUD

- Le prestataire doit

Assurer la sécurité des communications

- ✓ Cartographier le système d'information
- ✓ Cloisonnement des réseaux
- ✓ Surveiller les réseaux

Acquisition développement et maintenance des systèmes d'information

- ✓ Politique de développement sécurité
- ✓ Procédure du contrôle de changement du système
- ✓ Revue technique après changement
- ✓ Mettre en place des environnements de développements sécurisés
- ✓ Tester, protéger les données de test

SECNUMCLOUD

- Le prestataire doit

Assurer la sécurité dans la relation avec les tiers

Gérer les incidents liés à la sécurité de l'information

- ✓ Définir les responsabilités et procédures
- ✓ Signaler
- ✓ Apprécier les événements liés à la sécurité de l'information
- ✓ Assurer la réponse aux incidents de sécurité de l'information
- ✓ Tirer les enseignements
- ✓ Assurer le recueil des preuves

Assurer la continuité d'activité

- ✓ Organiser, mettre en œuvre, vérifier revoir, évaluer le PCA
- ✓ Assurer la disponibilité des moyens de traitement de l'information
- ✓ Sauvegarder la configuration de l'infra technique
- ✓ Mettre à disposition un dispositif de sauvegarde des données du commanditaire

SECNUMCLOUD

- Le prestataire doit

Assurer la conformité

- ✓ Identifier les exigences légales et réglementaires
- ✓ Assurer des revues indépendantes de la sécurité de l'information (continue, initiale, lors de changement
- ✓ La conformité des politiques et procédures
- ✓ La conformité des examens techniques

Mettre en place en exigences supplémentaires

- ✓ Des conventions de services (RGDP)
- ✓ La localisation des données
- ✓ La régionalisation
- ✓ La sécurité dans les fins de contrats
- ✓ La protection des données à caractère personnel
- ✓ La protection vis-à-vis du droit extra-européen