MINISTÈRE
DE L'EUROPE
ET DES AFFAIRES
ÉTRANGÈRES
Liberté
Égalité
Fraternité

DIRECTION GENERALE DE L'ADMINISTRATION
ET DE LA MODERNISATION

DIRECTION DES RESSOURCES HUMAINES

Sous-direction de la Formation, des Concours et des Stages

Bureau des Concours et Examens professionnels
RH4B

CONCOURS EXTERNE ET INTERNE
DE SECRETAIRE DES SYSTEMES D'INFORMATION ET DE COMMUNICATION
AU TITRE DE L'ANNEE 2022

EPREUVES ECRITES D'ADMISSIBILITE

7 - 9 FEVRIER 2022

NOTE DE SYNTHESE

Note de synthèse, établie à partir d'un dossier à caractère scientifique et technique de vingt-cinq pages maximum permettant de vérifier les qualités d'expression, d'analyse et de synthèse du candidat dans les domaines scientifiques et techniques, ainsi que son aptitude à dégager des conclusions et à formuler des propositions.

Durée : 3 heures
Coefficient : 2
Toute note inférieure à 6 sur 20 est éliminatoire.

SUJET

Les technologies d'info-nuage (« Cloud ») font maintenant partie intégrante de la stratégie des directions numériques du secteur public. Maîtrise des coûts, efficacité, performances et évolutivité sont, en général, les gains attendus d'une migration vers ces technologies et offres de services.

Une telle migration induit néanmoins un certain nombre de risques et donc la prise de nécessaires précautions. Le directeur du numérique vous demande de les détailler dans une note à son attention.

Avertissement : La note doit pouvoir être intelligible pour une personne non spécialiste du domaine numérique et se limiter aux éléments du dossier. Vous veillerez également à structurer au mieux votre copie. Enfin, toute recopie, même partielle, des textes du dossier sera sanctionné.

Ce dossier comporte 23 pages (page de garde et sommaire non compris).

SOMMAIRE

Texte 1 - Sécurité dans le cloud : non, le fournisseur ne fait pas tout, l'utilisateur aussi est responsable !
3 pages

Texte 2 - Le partage des responsabilités : clé de voûte pour la sécurité du cloud.
3 pages

Texte 3 - Panique chez les clients d'OVH en défaut de sauvegarde.
3 pages

Texte 4 - Le Cloud pour les administrations.
4 pages

Texte 5 - Extrait du guide de l'ANSSI sur l'externalisation des systèmes d'information.
2 pages

Texte 6 - Prestataires de services d'informatique en nuage (SecNumCloud), référentiel d'exigences.
8 pages

Texte n° 1 :

Sécurité dans le cloud : non, le fournisseur ne fait pas tout, l'utilisateur aussi est responsable !

www.journaldunet.com Le 3 septembre 2021

Tribune co-signée Edouard Camoin, VP Résilience chez 3DS OUTSCALE et Matthieu Bonenfant, Chief Marketing Officer chez Stormshield Alors que la transformation numérique des entreprises s'accélère, poussée notamment par le besoin accru de services en ligne pendant la pandémie, le cloud public reste l'option phare pour digitaliser les opérations.

Or, l'externalisation dans le cloud n'a rien d'une logique « *click and forget* » : le client doit rester sur le pont et assumer plusieurs responsabilités de sécurité, sans quoi il s'expose à de sérieux incidents.

Trois millions de dollars en moyenne portés par les entreprises victimes d'un malware, et 51 % d'entreprises attaquées : le cybercrime se porte bien. Une des raisons vient de la migration massive des entreprises vers le cloud dans le contexte de la crise sanitaire. Ainsi, entre 2019 et 2020 en France, le marché des services de cloud computing a enregistré une hausse de 17 %, et celui du IaaS et du PaaS, prisé pour fournir des solutions en ligne de visioconférence, de collaboration, de e-commerce et de streaming, a augmenté sur la période de 25 %. Mais en déplaçant les données et applications dans le cloud, les entreprises créent aussi une surface d'attaque bien plus vaste pour les malfaiteurs.

C'est pourquoi, à l'heure où la cybersécurité doit garder un train d'avance sur les cybercriminels, la sécurité ne peut pas faire figure de parent pauvre dans la démarche cloud de l'entreprise.

Dans le cloud, la sécurité se joue à tous les étages

Qu'on le veuille ou non, le cloud ne permet pas une externalisation totale de la sécurité des actifs informatiques migrés. Le client aura toujours une part de responsabilité. L'ignorer revient à mettre la sécurité sous le tapis et à s'exposer à de nombreux incidents de sécurité et attaques – vol ou perte de données, non-respect de la confidentialité, interruption des opérations, pour n'en citer que quelques-uns. « Et la confiance que l'on porte à son environnement cloud doit se jouer à tous les niveaux : du fournisseur de service externalisé jusqu'aux applications et solutions de sécurité gérées directement par le client. Les qualifications de l'ANSSI concernant les prestataires de service d'informatique en nuage (SecNumCloud) ou les produits de sécurité permettent de développer cette confiance.» souligne Matthieu Bonenfant.

Il importe en premier lieu de bien cerner que la sécurité dans le cloud exige des protections à tous les niveaux de l'infrastructure :

- Infrastructure physique, sous-jacente au cloud : serveurs, baies de stockage, switchs, systèmes de supervision ;
- Infrastructure virtuelle : instances de calcul, stockage, VPC, réseaux virtuels ;
- Applications et micro services qui vont s'exécuter dans le cloud ;
- Identités des utilisateurs et des administrateurs dont il faut gérer les profils et comptes d'accès pour utiliser applications et données ;

- Données stockées dans l'infrastructure cloud, qu'elles soient non structurées ou structurées en base de données.

Client/fournisseur : qui sécurise quoi dans le cloud ?

Il n'existe pas de réponse unique et applicable à tous les cas de figure. Tout dépend en effet du modèle proposé par le fournisseur de cloud. C'est pourquoi l'entreprise doit bien comprendre ce que son fournisseur prend en charge en matière de sécurité, et ce qu'il lui revient de sécuriser elle-même. À commencer par les grands principes qui suivent :

Dans le cas du IaaS, le fournisseur de cloud est uniquement responsable de l'infrastructure physique sous-jacente au cloud, et de sa sécurité. Le client est donc en charge de la sécurité à tous les autres niveaux. Le PaaS ajoute la sécurité de l'infrastructure virtuelle aux responsabilités du fournisseur, alors que le client se charge des identités et des données. Enfin dans un modèle SaaS, la majorité de la responsabilité de sécurité revient au fournisseur, toutefois, le client doit toujours garder la main sur les identités et ses données.

En synthèse, le client sera toujours responsable de ses données, des comptes utilisateurs et administrateurs et des identités, a minima. Il doit vérifier avec chaque fournisseur quelles autres responsabilités de sécurité lui reviennent selon le contrat. Et d'autant plus si l'entreprise suit une stratégie de cloud hybride et/ou multi-cloud, associée éventuellement à de l'edge-computing, et dans laquelle interviennent plusieurs fournisseurs et types de cloud.

Les bonnes pratiques sécuritaires pour le cloud

Le précepte à garder en tête : le client reste le premier responsable de la sécurité dans les clouds qu'il utilise et doit être proactif en la matière. À tous les niveaux de sécurité du cloud, l'entreprise doit veiller à garder un maximum de visibilité sur ce qui se passe – « Elle doit collecter et exploiter les traces telles que logs d'activité, d'accès, fonctionnement des applicatifs. Avec cette vision holistique, l'entreprise garde le contrôle et assure, le cas échéant, la réversibilité de la sécurité dans le cloud » détaille Edouard Camoin.

Autre bonne pratique : raisonner en mode « Security by design », autrement dit intégrer la sécurité dans le projet cloud dès le départ. Il faut anticiper et s'organiser. Ce qui implique de définir les critères de sécurité pour définir les applications et données éligibles au cloud, décider qui fait quoi en matière de sécurité, à quel moment l'embarquer, anticiper les ressources à allouer, prévoir des sauvegardes, plan de continuité et de reprise intégrant pleinement les caractéristiques de sécurité des clouds utilisés par l'entreprise. De quoi éviter de colmater au prix fort des brèches ultérieures, et surtout d'éviter des crises. Le tout sans oublier la formation et la sensibilisation. En effet, « trop d'opérationnels font encore leur choix de technologie cloud, la négocie en interne et se penchent sur la sécurité à la dernière étape : la pire approche de sécurité dans le cloud ! » regrette Edouard Camoin.

Pour choisir ses fournisseurs de cloud et mettre en place un environnement fiable, l'entreprise doit intégrer la notion de confiance dans ses critères de sélection. Travailler avec des fournisseurs de cloud qualifiés SecNumCloud et des technologies de sécurité qualifiées par l'ANSSI permet d'aller dans ce sens. De plus, l'évaluation des fournisseurs demande une attention particulière au périmètre

de sécurité réellement garanti derrière une certification affichée : l'entreprise doit s'assurer que les engagements de sécurité sont clairement exprimés dans les clauses contractuelles.

Puisque la proactivité du client est essentielle pour la sécurité dans le cloud, l'entreprise doit être prête à prendre les devants pour se couvrir d'un point de vue sécurité, même s'il est pris en charge par le fournisseur. « Par exemple, conserver la clé de chiffrement de ses données, ou même, ne pas laisser le fournisseur se charger des opérations de chiffrement. Et lorsque la sécurité incombe directement au client, il doit utiliser au maximum des technologies de protection tierces, compatibles avec divers environnements cloud, dont il aura la pleine maîtrise », recommande Matthieu Bonenfant. Ce faisant, l'entreprise assure la cohérence des politiques de sécurité sur l'intégralité de son système d'information (y compris en cloud hybride ou multi-cloud) et facilite la réversibilité de la sécurité en cas de changement de fournisseur cloud.

Les entreprises ont une part de responsabilité en matière de sécurité dans le cloud : leurs données et leur souveraineté dans le cloud ne peuvent plus attendre !

Texte n° 2 :

Le partage des responsabilités : clé de voûte pour la sécurité du cloud

www.journaldunet.com Le 24 mars 2020

" D'ici 2025, pas moins de 99 % des incidents de sécurité liés au cloud seront imputables au client. " Gartner tire la sonnette d'alarme quant à l'importance du partage des responsabilités en matière de sécurité cloud. Cet avertissement sous-entend que les organisations elles-mêmes – et non pas les fournisseurs de services cloud – doivent veiller à la pertinence de leur approche en matière de sécurité.

Pour les entreprises, la question de la migration des données vers le cloud divise. Certaines estiment que la sécurité offerte par les services cloud constitue une raison valable en faveur d'une migration. D'autres redoutent au contraire le manque de sécurité inhérent à ces environnements. Les deux parties ont en réalité raison. La sécurité constitue en effet l'aspect le plus important de l'offre d'un fournisseur de services cloud : l'impact lié à un incident de sécurité peut être dramatique, autant pour le fournisseur que pour les souscripteurs.

De par le modèle de sécurité partagée, aucune organisation ne peut assumer à elle seule l'entière responsabilité de la sécurité des données. Organisations, utilisateurs, professionnels de la sécurité informatique et fournisseurs de services cloud ont pour mission commune de s'assurer que toutes les parties impliquées emploient le cloud de façon sûre avec des objectifs de sécurité mesurables et quantifiables. À l'ère de l'économie numérique, la mise en œuvre d'un modèle de responsabilité partagée est synonyme de confiance renforcée, de risques réduits, de réputation améliorée et plus généralement de succès opérationnel pour les entreprises.

Une clarification des rôles indispensable

Une sécurité optimale du cloud requiert plusieurs niveaux de protection, les différents acteurs constituant la « pile des responsabilités » de façon individuelle, tout en interagissant comme une structure unifiée. Sécurité des infrastructures, contrôle du réseau, sécurité des applications, gestion des identités et des accès, protection des terminaux, classification des données, contrôle des usages : la liste est longue et potentiellement effrayante pour tout service informatique, quelle que soit sa taille.

La protection proposée par les fournisseurs de services cloud ne garantit malheureusement pas la sécurité des données en se substituant aux responsabilités de l'ensemble des acteurs. Microsoft, Amazon, Google et autres grands noms précisent à juste titre que la responsabilité ne leur incombe pas entièrement et que les entreprises doivent se faire à l'idée d'une responsabilité partagée. Microsoft a par exemple publié son modèle pour Azure. Amazon applique une approche similaire pour AWS. Dans un cas comme dans l'autre, il est précisé que la sécurité de l'infrastructure repose sur les actions mises en œuvre par le client afin de garantir la sécurité et la conformité de l'écosystème.

Les fournisseurs de services cloud divisent traditionnellement les responsabilités induites de la manière suivante : ils gardent la responsabilité associée à la sécurité d'une partie identifiée de

l'infrastructure et laissent au client le soin de s'occuper du reste. Ce partage peut être source d'incertitudes pour les entreprises clientes. Alors comment déterminer et répartir les aspects relevant de leur responsabilité, quelles certitudes sont données sur les éléments de sécurité incombant au fournisseur de services cloud ? Il est essentiel de clarifier les rôles et les responsabilités de chacun, dans l'entreprise et chez les fournisseurs de services cloud.

Cloud et location de véhicule : la responsabilité partagée de la sécurité comme point commun

Le principe de location d'une voiture illustre parfaitement le partage des responsabilités. Tout d'abord, le constructeur est dans l'obligation d'assurer que le véhicule est en état de rouler à sa sortie de la chaîne de montage. Les freins, roues et airbags doivent fonctionner comme il se doit. Une fois la voiture réceptionnée par l'agence de location, cette dernière ne vérifie pas les airbags, le locataire non plus : tous deux partent du principe que ces équipements fonctionnent correctement. Pendant la durée d'exploitation du véhicule, l'agence doit entretenir celui-ci et garantir qu'il est en état de marche. Le locataire suppose que toutes les vérifications sur les équipements ont été effectuées ; malheureusement, lorsque ce n'est pas le cas, il ne le découvre qu'après avoir rencontré un problème avec le véhicule.

Pour les ceintures de sécurité, le principe est le même. Le constructeur doit les installer, l'agence de location les entretenir, mais c'est au conducteur qu'il revient de l'attacher et de vérifier que tous les passagers ont fait de même.

La location d'un véhicule implique ainsi une répartition des responsabilités clairement définie. Chaque acteur est tenu de jouer son rôle et une défaillance unitaire peut être cause de graves accidents. Ignorer une exigence de sécurité peut donc avoir des conséquences désastreuses.

La responsabilité associée à la gestion des risques incombe à l'entreprise

Microsoft, Amazon et les autres fournisseurs de services cloud s'efforcent d'appliquer systématiquement des modèles de partage des responsabilités, mais les utilisateurs finaux – l'organisation en elle-même, les responsables de la sécurité des données, l'équipe de sécurité informatique, les utilisateurs – doivent assumer davantage de responsabilités. Les dirigeants et responsables informatiques ne peuvent garantir la protection des données dans le cloud que si les fonctionnalités de sécurité sont bien comprises, activées et correctement configurées. C'est ce qu'a récemment démontré une violation de données hautement médiatisée, conséquence d'une mauvaise configuration des règles AWS rendant des serveurs accessibles au public.

De manière générale, les responsables technologiques doivent déterminer à qui incombent la vérification et la gestion des configurations cloud, des flux de données entre différents services cloud, du comportement des utilisateurs, ou encore des contrôles relatifs à la collaboration, aux accès et aux périphériques. En définitive, la responsabilité associée à la gestion des risques incombe à l'entreprise, car c'est avant tout elle qui est chargée de la collecte et de la sécurité des données. Le fournisseur de services cloud joue certes un rôle important, mais contrairement à l'organisation cliente, il n'est pas en contact direct avec le public et n'assume pas le risque associé à la gestion de ces données sensibles. Les membres de l'équipe informatique doivent jouer le rôle de gardiens de la sécurité et de la conformité. Ils doivent travailler de concert avec le RSSI et les autres dirigeants pour comprendre et définir les politiques en matière de contrôle des données, coopérer avec les

différents services pour catégoriser précisément les données, assurer la conformité réglementaire, faciliter les décisions du service des achats, définir les services cloud accessibles aux utilisateurs et garantir l'exhaustivité de la formation des utilisateurs.

En l'absence de processus stricts et de responsabilités clairement définies, une décision opérationnelle comme le déploiement d'un nouveau service de cloud public peut fortement exposer une entreprise à une violation de données ou à des incidents de sécurité connexes. À l'inverse, une démarche de partage des responsabilités permet de veiller à ce que chacun accomplisse son rôle.

Texte n° 3 :

Panique chez les clients d'OVH en défaut de sauvegarde

lemondeinformatique.fr le 17 mars 2021

Collectivités, entreprises, administrations... Petits ou grands, les clients touchés de plein fouet par l'incendie du datcenter d'OVH à Strasbourg ont connu des conséquences notables sur leurs activités en particulier ceux dont le web est un point d'entrée commercial ou de services. La nécessité d'avoir un back-up et un PRA fonctionnel n'a jamais été aussi forte.

Moins d'une semaine après le terrible incendie qui a frappé le datacenter d'OVH à Strasbourg, la tension est vive. Les raisons de l'incident ne sont pas encore pour l'heure établies clairement. L'hypothèse d'un acte malveillant ne peut pas être totalement écartée. Des scellés sont effectués sur les onduleurs, batteries, vidéo surveillance afin de faire avancer l'enquête. « On pense avoir été très transparents et au-dessus des standards de l'industrie, il faut monter ces standards pour que ces types d'incidents n'arrivent plus jamais et que pour des pertes de disques, les données puissent toujours être récupérées », a indiqué dans une dernière vidéo le fondateur d'OVH Octave Klaba. Au-dessus des standards de l'industrie ? Pas vraiment, puisque OVH ne souscrit pas aux onéreuses certifications de l'Uptime Institute. Le groupe qui multiplie depuis quelques mois les annonces (projet d'introduction en bourse, offre d'hébergement de données de santé, acquisition d'OpenIO, conquête du marché des entreprises, partenariat avec Atos pour une offre cloud « de confiance »... a fort à faire avec une concurrence très forte sur le marché de l'hébergement.

En attendant, on peut quand même s'interroger sur les circonstances de cet incident qui ont clairement été mal maitrisées par OVH. Plusieurs points de faiblesse peuvent expliquer la situation. En adoptant un modèle low cost, la société fait sans aucun doute ressortir des lacunes en termes de sécurité incendie mais aussi de certifications. Par rapport à d'autres opérateurs comme Equinix ou Interxion, OVH n'a par exemple pas pris le train de l'Uptime Institute, organisme mondialement reconnu pour ses benchmarks de datacenters, allant même jusqu'à revendiquer s'y conformer sans en être certifié. Le monde à l'envers. De même, toujours afin de comprimer les coûts, de possibles défaillances des maigres systèmes de sécurité incendie [des extincteurs à mains obligatoires], qui se sont révélés incapables de circonscrire le sinistre sur un périmètre restreint, doivent être éclaircies. Le manque de technologies de détection, atténuation ou lutte contre les incendies (brouillard d'eau, sprinkler, gaz, mousse mais aussi détecteur de chaleur, fumée ou flamme...) est un vrai problème dans le datacenter strasbourgeois d'OVH. De conception ancienne (10 ans) et low cost, ce dernier ne bénéficie pas des avancées présentes chez d'autres opérateurs de datacenters.

OVH pris à son propre piège du low cost à tout prix ?

OVH n'a-t-il finalement pas été pris au piège de son propre jeu ? A trop vouloir capitaliser sur les petits clients, le groupe paye-t-il les pots cassés des prix bas ? Toute éventuelle faiblesse ne peut cependant être uniquement à mettre au crédit d'OVH. Les clients eux-mêmes ont aussi certainement leur part de responsabilité. Non dans l'incendie en tant que tel bien entendu, mais dans le manque de clairvoyance en mettant tous leurs oeufs dans le même panier et se satisfaisant d'une prestation à moindre frais. Avec pour principal défaut l'absence cruelle de back-up : une option indispensable pour les entreprises afin de sécuriser leurs activités.

Des impacts hors normes qui font réagir

Les impacts de cet incident hors norme ont fait réagir non seulement les entreprises concernées, mais également des compétiteurs : « Nous sommes très solidaires d'OVH », a indiqué dans un point presse ce matin lors de l'Orange Business Summit Helmut Reisinger, directeur général d'OBS. « C'est la French Tech qui est touchée, avec un incident que l'on pensait impensable ». Même son de cloche du côté d'Atempo : « Ce qui fait mal au coeur c'est qu'il s'agit d'un événement d'une ampleur inimaginable, presque historique. Cela fait de la peine pour notre partenaire qui doit surmonter une telle catastrophe de cette proportion là, on leur souhaite de se remettre dans les meilleurs délais », nous a expliqué Luc d'Urso, directeur général d'Atempo et vice-président d'Hexatrust.

Des clients entre l'étau du désespoir et l'enclume de la négligence

Suite à l'incendie, les entreprises multiplient les témoignages de désarroi et d'excuses. La raison de toute cette agitation ? L'indisponibilité de leurs sites et services web mais aussi l'impossibilité de récupérer leurs données. Selon les clients, les perturbations varient. Chez Cityscoot par exemple, les données d'inscription effectuées depuis au moins le 10 mars n'ont pas été prises en compte, tandis que du côté de l'association toulousaine Parole d'Entreprises ce sont les envois d'emails qui ont été touchés faute de base de données. L'effet domino a également joué à plein : chez le prestataire Intermédia Conseil, ce sont 250 sites clients qui ne peuvent plus créer d'adresses de messagerie. Ennuyeux.

Parmi les clients touchés, on trouve de nombreuses mairies (Artenay, Arras, Saint-Ouen, Cherbourg, Vichy, Vitry-sur-Seine...), des clubs sportifs (AS Cannes, l'US Créteil Handball, l'AS Saint-Priest, club de rugby de Clermont-Ferrand....). Des PME (Nautex International, Duysens Immobilier, Groupe Gorioux, BEG Ingénierie, bureau d'études d'Orléans-La Source, le fabricant de monuments funéraires Stonest...) et éditeurs de services en ligne (Rust, Freshmile Direct, The Artist Academy...). Ou encore des organismes culturels, religieux et touristiques (Frac Bretagne, Centre Pompidou à Paris, Office de tourisme de Colmar et de Saverne, Diocèse de StBrieuc...), des médias (Maddyness, Agro Distribution, L'Essor Isère, La Semaine ...), des services administratifs (datagouv, plateforme de dématérialisation des marchés publics, défenseur des droits...) et de nombreuses associations (CRAIF, CIRSES, Ligue contre l'obésité...), l'aéroport de Strasbourg...

Suite à ce ravage, 3,6 millions de sites web et sous-domaines auraient ainsi été impactés avec des problèmes d'accès de quelques dizaines de minutes ou plusieurs heures pour les plus chanceuses, quand d'autres connaissent l'angoisse d'une indisponibilité totale parfois pour toujours. Tous les profils de clients d'OVH sont touchés : qu'ils soient aussi bien entreprises que collectivités, privé que public, petit ou grand. Mais les plaintes des entreprises qui s'en prennent à OVH sont-elles pour autant justifiées ? Loin de là dès lors que ces dernières ont souscrit un simple service d'hébergement sans prestation de service de back-up associé et n'ont pas non plus pris la peine de souscrire et/ou de mettre en place leur propre plan de reprise d'activité. « Sans parler de négligence de la part de clients qui ont beaucoup souffert, il il faut tirer partie de l'expérience de cet incident. Déléguer un service PaaS ou IaaS ne dispense pas de réfléchir au plan de reprise d'activité », poursuit Luc d'Urso. « La seule chose sur laquelle capitaliser c'est d'avoir une copie de ces données, ce n'est pas à OVH de s'occuper de cela. Il a une sorte de sophisme qui est de dire que le cloud protège les données mais cela n'est absolument pas le cas ». Mise au pied du mur, la société 6Thèmes Info a d'ailleurs expliqué qu'en plus d'un hébergement classique, des serveurs de stockage internalisés seront désormais installés.

Bien sûr, en termes d'hébergement, OVH est tenu d'assurer et de maintenir les services en ligne mais sans souscription d'un service de back-up associé et de PRA, difficile de jeter aussi facilement la pierre à l'hébergeur aussi dure que la réalité puisse être. « Si l'entreprise a souscrit à un PRA elle n'a à ce moment là aucun souci à se faire en termes de récupération de données qui pourront se faire

depuis un des 31 autres datacenters d'OVH en France », estime Luc d'Urso. Quand bien même une prestation de ce type a pu être prise, mieux vaut garder en tête que la meilleure pratique de sauvegarde est de les multiplier, a minima deux, chez deux prestataires différents, dans des régions distinctes, afin de réduire la surface d'exposition au risque de perte de données.

Des pertes qui peuvent être non seulement liées à des événements de type incendie et catastrophes naturelles que cybersécurité. « La montée du cyberhactivisime qui atteint des sommets, les détournements massifs de caméras vidéo, l'explosion des ransomwares... il faut préparer sauvegarde et PRA, c'est le dernier rempart contre des catastrophes », martèle Luc d'Urso. Et si cela la prévention ne suffit pas pourquoi ne pas aller jusqu'à taper du poing sur la table : « Aujourd'hui ne pas avoir de PRA c'est proche de la négligence. On ne peut pas éternellement reposer sur de la sensibilisation, une entreprise qui se prend 4 ransomwares dans l'année devrait être contrainte à se sécuriser ». La cyberassurance c'est bien, la cyber-responsabilité sans doute mieux ?

« La continuité des réseaux optiques est assurée entre Paris et Francfort en passant par Strasbourg. Les premiers routeurs ont été connecté au réseau, on configure de plus en plus de VPN, commutateurs, pour connecter et configurer l'ensemble des switchs qui sont dans la baie », a assuré Octave Klaba. Le fondateur indique par ailleurs travailler avec l'expert de sa société d'assurance pour redémarrer complètement le datacenter sur Strasbourg 1 et 4 sans soucis, sauf les salles 61E et 62E où beaucoup de nettoyage est encore nécessaire en raison de la fumée déposée nécessitant jusqu'à des changements de cartes mères. Sur Strasbourg 3, les 1er, 2e et 3e étages devraient globalement redémarrer mais des soucis au niveau de la salle 5. « On finit de passer les fibres optiques et ramener le network jusqu'à la baie avant de procéder au redémarrage des serveurs », précise Octave Klaba. D'ici samedi ou dimanche la plupart des infrastructures devrait être opérationnelle. 2 500 serveurs vont être livrés en plus cette semaine et 10 000 seront produits d'ici 2 semaines pour un objectif de 15 000 livrés et connectés d'ici mai 2021.

Pertes de données non contractuelles : un geste symbolique de 60€

« On a envoyé aux clients l'état des back-ups internes non contractuels et aussi l'état des services back-up locaux ou à distance, une colonne supplémentaire avec les dates de redémarrage des services seront ajoutées. Si vous êtes impactés par la commande, vous pouvez la passez aujourd'hui, on va vous donner des mois gratuits, dans les cas de coupure de service 3 mois, et 6 mois pour de la perte de data sur les services ». Un geste commercial qui part d'un bon sentiment mais pourrait bien tourner vinaigre pour certains clients dont la société de ventes de bijoux de Mathilde Picouret. Suite au sinistre, cette dernière s'est ainsi vue proposer un avoir de 30€ soit 6 mois d'hébergement, pour un préjudice estimée à 2 000 €. Si dans ce cas une solution de sauvegarde n'a sans doute pas été souscrite, s'agissant d'une « simple » prestation d'hébergement, reste à savoir si le versement d'une somme aussi dérisoire dans un contexte compliqué autant que brutal ne risque pas de provoquer une fronde de la part de clients touchés aussi bien que déçus par cette mesurette. Sur Twitter, certains membres de la FrenchTech, tribu autoproclamée, cherche d'ailleurs à savoir si une action collective contre OVH est envisageable...

Texte n° 4 :

Le Cloud pour les administrations

L'informatique en nuage (Cloud computing) est une formidable opportunité pour accélérer la transformation numérique des administrations. À travers sa doctrine « Cloud au centre », l'État encourage l'ensemble des acteurs publics à se saisir de son potentiel afin de développer une nouvelle génération de services numériques de qualité, tout en protégeant au mieux les données des entreprises et des citoyens français. Au-delà des technologies et des offres de services, c'est un changement de culture qui s'engage, afin que les équipes projets et les développeurs inscrivent les opportunités du cloud dans leurs pratiques professionnelles au quotidien.

Cloud au centre : la doctrine de l'État

Avec l'adoption de la doctrine « Cloud au centre », le Gouvernement fait du Cloud un prérequis pour tout nouveau projet numérique au sein de l'État ou refonte substantielle de l'architecture applicative existante. L'objectif : accélérer la transformation numérique au bénéfice des usagers et dans le strict respect de la cybersécurité et de la protection des données des citoyens et des entreprises.

L'informatique en nuage va au-delà d'un simple socle d'hébergement : elle sous-tend toute une culture, depuis le mode de production des applications (mode produit, DevOps) jusqu'aux principes d'architecture à la base de la conception de ces nouveaux services (architecture nativement cloud).

Accélérer la transformation numérique de l'État

Le Cloud est essentiel pour **accompagner et accélérer l'évolution des pratiques** de développement de produits numériques de l'État. La doctrine Cloud au centre coordonnée par le ministère de la Transformation et de la Fonction publiques permet d'inscrire ce virage durablement dans les directions du numérique des ministères, et plus largement auprès de tous les acteurs de l'État.

L'adoption du Cloud doit permettre de faciliter la maîtrise de la chaîne de production des services numériques et ainsi conduire à équiper les agents de meilleurs outils de travail numériques, plus collaboratifs, et d'améliorer, en continu, les démarches des usagers en ligne, qu'ils soient citoyens ou entreprises.

L'inscription durable du virage vers le Cloud poursuit un objectif principal : répondre aux attentes légitimes des Français d'exemplarité de l'État en matière de **protection de leurs données** ainsi qu'en terme de garantie de la **continuité du service public**, deux prérequis à leur confiance dans le service public numérique.

La doctrine Cloud au centre

Avec cette doctrine, le Cloud devient dorénavant le **mode d'hébergement et de production par défaut des services numériques de l'État**, pour tout nouveau produit numérique et pour les produits connaissant une évolution substantielle. Les recrutements et les programmes de formation continue destinés aux agents publics dans la filière économique comporteront un volet Cloud. La doctrine prévoit également, et c'est une condition nécessaire à sa mise en œuvre opérationnelle, d'être inscrite dans la gouvernance des activités du numérique de chaque administration.

Les services numériques des administrations doivent être hébergés sur **l'un des deux cloud interministériels internes de l'État ou sur les offres de Cloud proposées par les industriels satisfaisant des critères stricts de sécurité**.

Notamment, chaque produit numérique manipulant des **données sensibles**, qu'elles relèvent des données personnelles des citoyens français, des données économiques relatives aux entreprises françaises, ou d'applications métiers relatives aux agents publics de l'État, doit impérativement être hébergé sur le cloud interne de l'État ou **sur un cloud commercial qualifié SecNumCloud par l'ANSSI et protégé contre toute réglementation extracommunautaire**.

Le passage au Cloud est également une occasion de **renforcer la résilience des produits numériques des administrations**, au service de la continuité du service public. Les administrations peuvent donc dès à présent s'appuyer sur une diversité de technologies, de fournisseurs et d'infrastructures pour préparer des **plans de continuité et de reprise d'activité** pouvant être activés en cas d'incident.

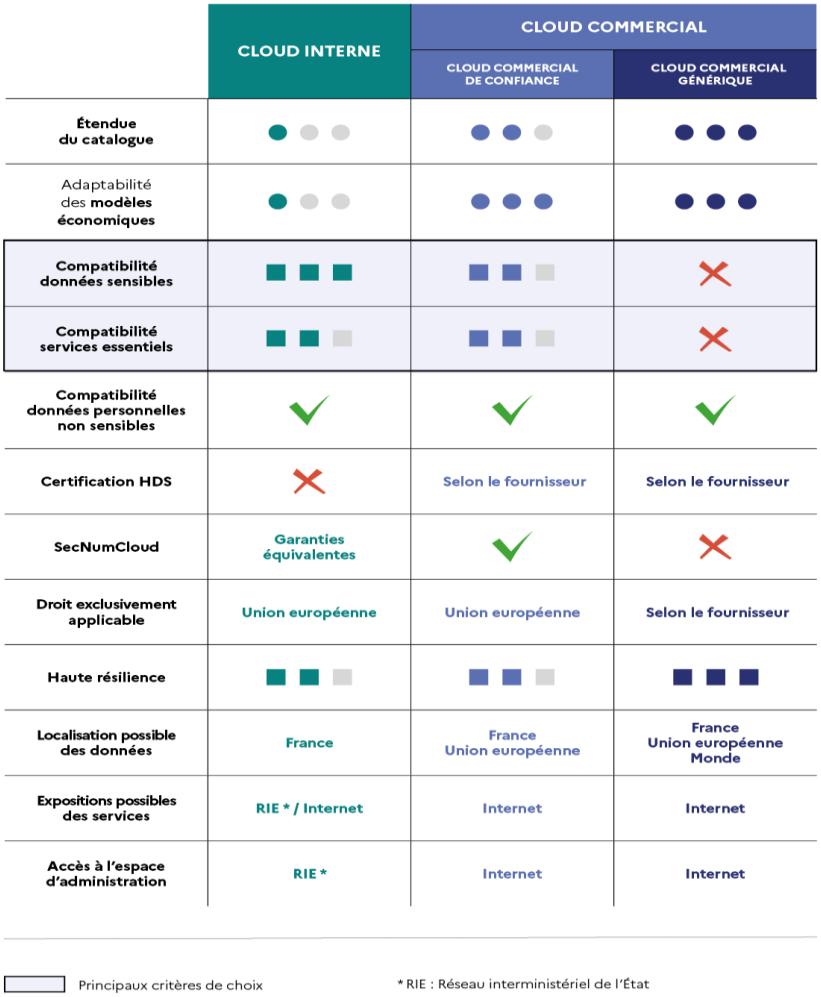
Avec « Cloud au centre », l'État se dote d'une doctrine complète, engageant résolument les administrations sur la voie d'une transformation numérique de qualité tout en renforçant la souveraineté de l'État et la protection des données des Français.

Quelle offre Cloud choisir ?

Quelle offre Cloud correspond le mieux à votre besoin, à votre produit ?

Nous avons résumé dans le tableau ci-dessous les caractéristiques principales de chacune des offres de cloud. Parmi ces critères, la compatibilité avec des données sensibles ou personnelles, et le caractère essentiel du service rendu par le produit sont les facteurs indispensables à prendre en compte.

Caractéristiques des offres Cloud



Détails des caractéristiques des deux offres Cloud

Catalogue de services

Les offres de Cloud commercial, issue des catalogues de services des principaux acteurs des marchés français, européen et mondial, propose une plus grande diversité d'infrastructure, de plateformes et de services innovants que les offres de Cloud interne.

Modèles économiques

Le Cloud offre une grande variété de tarification. Paiement à l'usage, instances à coût marginal, prix réduits en contrepartie d'une longue durée d'engagement : chaque fournisseur a ses propres caractéristiques qu'il convient d'analyser en détail pour optimiser sa facture, le Cloud commercial offrant la plus grande diversité.

Compatibilité données sensibles

À ce jour, seuls le Cloud interne et le Cloud commercial de confiance doivent être utilisés dans le cas d'un produit traitant des données sensibles, c'est-à-dire des données particulièrement confidentielles ou dont l'intégrité est importante, qu'elles relèvent du champ des données personnelles des citoyens français, des données économiques relatives aux entreprises françaises, ou d'applications métiers relatives aux agents publics de l'État.

Compatibilité services essentiels

Les services essentiels de l'État se caractérisent par un fort besoin de disponibilité, quelles que soient les circonstances. Pour la garantie de disponibilité dans des circonstances normales, le choix

peut s'opérer en fonction des niveaux de service constatés des différentes offres des Cloud interne et Cloud commercial ainsi que du niveau de résilience de chacun des services. Par ailleurs, l'État n'ayant que des garanties limitées sur les changements de stratégie des opérateurs du Cloud commercial, les services essentiels qui y seraient hébergés mériteraient de faire l'objet d'une analyse de risques et des possibilités de bascules vers des solutions de repli.

Compatibilité données personnelles
Collecter et traiter des données personnelles au sens du RGPD implique de prendre des mesures pour garantir une utilisation de ces données respectueuses de la vie privée des personnes concernées. En ce sens, l'hébergement des données personnelles sur les deux offres est possible mais relève de la responsabilité de l'administration propriétaire du service et de sa mise en conformité aux règles de protection de données.
Pour les données personnelles dont la confidentialité ou l'intégrité est particulièrement sensible, se référer au critère « compatibilité données sensibles » ci-dessus.

Certification HDS
L'offre de Cloud commercial intègre plusieurs fournisseurs de services Cloud disposant de l'agrément HDS (Hébergeur de Données de Santé).

Qualification SecNumCloud
Le référentiel SecNumCloud, utilisé dans le cadre de la qualification de prestataires de Cloud délivrée par l'ANSSI, décrit le socle minimal de garanties sur les compétences de fournisseur de services Cloud et de son personnel. La conformité du service à ce référentiel permet d'apprécier la qualité de la prestation et la confiance qu'il est possible de lui accorder.
La recherche de conformité au référentiel SecNumCloud n'exclut ni l'application de la législation et de la réglementation nationale, ni l'application des règles générales de sécurité imposées à chaque organisme.

Droit exclusivement applicable
Certains fournisseurs de Cloud commercial sont soumis à une législation d'un pays hors Union Européenne imposant le transfert des données à caractère personnel aux autorités publiques (ex. Cloud Act).

Ce critère permet d'accéder à des fournisseurs non assujettis à ces réglementations.

Haute résilience
Les deux offres Cloud proposent à minima une région d'hébergement comprenant deux zones de disponibilité. En outre, le Cloud commercial offre des services plus résilients et des infrastructures profitant d'une distribution sur un nombre de sites ou de régions plus élevé. De même, l'offre de Cloud interne offre aux ministères une connectivité plus résiliente par leur exposition sur le RIE.

Localisation des données
Le Cloud interne permet d'héberger des données en France métropolitaine, le Cloud commercial de confiance offre des zones d'hébergement en France pouvant s'étendre en Union Européenne, et le Cloud commercial générique dispose d'une plus grande variété de zones d'hébergement permettant d'étendre votre système d'information en France, en Union européenne ou dans le monde. Il est de la responsabilité du bénéficiaire de vérifier que la localisation de ses données est conforme aux contraintes réglementaires applicables.

Expositions possibles
L'offre de Cloud interne est construite sur une double infrastructure comprenant deux zones distinctes : l'une exposée sur le RIE et l'autre sur internet. L'offre de Cloud commercial est exposée uniquement sur internet.

Accès à l'espace d'administration
L'accès à l'espace d'administration des ressources du Cloud interne est possible à travers le réseau interministériel de l'État (RIE). Les ressources du Cloud commercial sont administrables depuis les plateformes des fournisseurs de services Cloud, depuis l'accès internet du RIE ou depuis internet.

Texte n° 5 :

Extrait du guide de l'ANSSI sur l'externalisation des systèmes d'information

L'informatique en nuage ou nébuleuse

➢ Champ d'application

L'informatique en nuage (en anglais cloud computing) est définie par le Journal Officiel du 6 juin 2010 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 ».

Comme le précise également la définition du JO, il s'agit d'une « forme de gérance informatique dans laquelle l'emplacement et le fonctionnement du nuage ne sont pas portés à la connaissance des clients ».

Les architectures de cloud computing mettent généralement en œuvre des technologies de calcul distribué et de virtualisation. Par extension, le cloud computing tend à désigner toutes les offres de services qui s'appuient sur de telles architectures, accessibles via Internet ou un autre réseau, qu'elles soient publiques ou restreintes à une communauté (« nuage communautaire ») ou encore à usage interne de l'entreprise (« nuage privé »).

Les offres proposées dans ce type d'architecture sont de trois types :

- Infrastructure as a Service : fourniture de ressources matérielles abstraites, typiquement des machines virtuelles, permettant d'installer à distance le système d'exploitation et les applications de son choix ;
- Platform as a Service : fourniture de plateformes permettant le développement d'applications à partir d'interfaces de programmation (API) déployées et configurables à distance ;
- Software as a Service : fourniture d'applications directement utilisables à distance.

➢ Les risques de l'informatique en nuage

Compte tenu des principes et des technologies mis en œuvre dans l'informatique en nuage, on retrouve la plupart des risques de l'infogérance « classique ».

Risques liés à la localisation des données :

En Europe, le cadre juridique de protection des données à caractère personnel s'appuie sur le principe suivant : il doit être possible de constater à tout moment la localisation des données (principe de territorialité). Or, le plus souvent dans un nuage public, cette localisation est impossible. En effet, les données peuvent être déplacées très rapidement, d'un État à un autre, en fonction des ressources disponibles au sein des infrastructures du prestataire.

L'impossibilité de localiser les données dans les nuages publics pose le problème de la compétence des juridictions et du droit applicable. L'impossibilité de réaliser des audits, parfois imposés par un cadre réglementaire, ne permet pas de vérifier la mise en œuvre des mesures de sécurité.

En l'absence d'un niveau homogène de protection des données personnelles, et de garantie quant aux mesures de sécurités mises en œuvre, la confidentialité des données est incertaine.

Risques de perte de maîtrise de son SI :

- perte de gouvernance : en utilisant les services d'une infrastructure d'informatique en nuage, le client concède au prestataire un contrôle total, y compris sur la gestion des incidents de sécurité ;
- dépendance technologique : les offres ne garantissent pas toujours la portabilité des données, des applications ou des services. Il paraît difficile dans ces conditions d'envisager un changement de prestataire ou de réinternaliser le système.

Risques liés à la mutualisation des ressources :

- isolation défaillante : les mécanismes de séparation des ressources (stockage, mémoire) peuvent être défaillants et l'intégrité ou la confidentialité des données compromises ;
- effacement incomplet ou non sécurisé : il n'y a aucune garantie que les données soient réellement effacées ou qu'il n'existe pas d'autres copies stockées dans le nuage.

Enfin, il est plus difficile de se prémunir de ces risques que dans l'infogérance classique. En effet, le client souscrit le plus souvent à des offres par validation d'un contrat type, qu'il est souvent impossible de personnaliser en y intégrant des clauses particulières en matière de sécurité.

➢ Recommandations

On portera une attention particulière à l'appréciation des risques, en particulier en ce qui concerne les données dites « sensibles » (données à caractère personnel, médicales, financières, secrets industriels, etc.).

Il faut être conscient des risques que comporte l'externalisation des services d'une messagerie d'entreprise ou d'une suite bureautique auprès d'un prestataire d'informatique en nuage. Les informations échangées ou traitées par ce biais (pièces jointes, agendas des décideurs, etc.) peuvent revêtir un caractère « sensible », et sont susceptibles d'intéresser la concurrence (intelligence économique).

Comme expliqué précédemment, en l'absence de cadre juridique international adapté à l'informatique en nuage, il est préférable de s'assurer que les données à caractère personnel restent localisées sur des serveurs exclusivement situés dans l'Union européenne – voire en France – et de prévoir les moyens de contrôle de cette obligation.

Enfin il est recommandé d'étudier attentivement les conditions des offres, en particulier le régime juridique auquel sont soumises les données et les mesures mises en œuvre pour assurer leur confidentialité.

Texte n° 6 :

Extraits « Prestataires de services d'informatique en nuage (SecNumCloud) référentiel d'exigences Version 3.2.a du 21 septembre 2021»

PM : ANSSI

Sécurité liée à l'exploitation

12.1. Procédures d'exploitation documentées

a) Le prestataire doit documenter les procédures d'exploitation, les tenir à jour et les rendre accessibles au personnel concerné.

12.2. Gestion des changements

a) Le prestataire doit documenter et mettre en œuvre une procédure de gestion des changements apportés aux systèmes et moyens de traitement de l'information.
b) Le prestataire doit documenter et mettre en œuvre une procédure permettant, en cas d'opérations réalisées par le prestataire et pouvant avoir un impact sur la sécurité ou la disponibilité du service, de communiquer au plus tôt à l'ensemble de ses commanditaires les informations suivantes :
- la date et l'heure programmées du début et de la fin des opérations ;
- la nature des opérations ;
- les impacts sur la sécurité ou la disponibilité du service ;
- le contact au sein du prestataire.

c) Dans le cadre d'un service PaaS, le prestataire doit informer au plus tôt le commanditaire de toute modification à venir sur des éléments logiciels sous sa responsabilité dès lors que la compatibilité complète ne peut être assurée.
d) Le prestataire doit informer au plus tôt le commanditaire de toute modification à venir sur les éléments du service dès lors qu'elle est susceptible d'occasionner une perte de fonctionnalité pour le commanditaire.

12.3. Séparation des environnements de développement, de test et d'exploitation

a) Le prestataire doit documenter et mettre en œuvre les mesures permettant de séparer physiquement les environnements liés à la production du service des autres environnements, dont les environnements de développement.

12.4. Mesures contre les codes malveillants

a) Le prestataire doit documenter et mettre en œuvre les mesures de détection, de prévention et de restauration pour se protéger des codes malveillants. Le périmètre d'application de cette exigence sur le système d'information du service doit nécessairement contenir les postes utilisateurs sous la responsabilité du prestataire et les flux entrants sur ce même système d'information.
b) Le prestataire doit documenter et mettre en œuvre une sensibilisation de ses employés aux risques liés aux codes malveillants et aux bonnes pratiques pour réduire l'impact d'une infection.

12.5. Sauvegarde des informations

a) Le prestataire doit documenter et mettre en œuvre une politique de sauvegarde et de restauration des données sous sa responsabilité dans le cadre du service. Cette politique doit prévoir une sauvegarde quotidienne de l'ensemble des données (informations, logiciels, configurations, etc.) sous la responsabilité du prestataire dans le cadre du service.

b) Le prestataire doit documenter et mettre en œuvre des mesures de protection des sauvegardes conformément à la politique de contrôle d'accès. Cette politique doit prévoir une revue mensuelle des traces d'accès aux sauvegardes.
c) Le prestataire doit documenter et mettre en œuvre une procédure permettant de tester régulièrement la restauration des sauvegardes.
d) Le prestataire doit localiser les sauvegardes à une distance suffisante des équipements principaux en cohérence avec les résultats de l'appréciation de risques et permettant de faire face à des sinistres majeurs. Les sauvegardes sont assujetties aux mêmes exigences de localisation que les données opérationnelles. Le ou les sites de sauvegarde sont assujettis aux mêmes exigences de sécurité que le site principal. Les communications entre site principal et site de sauvegarde doivent être protégées par chiffrement.

12.6. Journalisation des événements

a) Le prestataire doit documenter et mettre en œuvre une politique de journalisation incluant au minimum les éléments suivants :
- la liste des sources de collecte ;
- la liste des événements à journaliser par source ;
- l'objet de la journalisation par événement ;
- la fréquence de la collecte et base de temps utilisée ;
- la durée de rétention locale et centralisée ;
- les mesures de protection des journaux (dont chiffrement et duplication) ;
- la localisation des journaux.

b) Le prestataire doit générer et collecter les événements suivants :
- les activités des utilisateurs liées à la sécurité de l'information ;
- la modification des droits d'accès dans le périmètre de sa responsabilité ;
- les événements issus des mécanismes de lutte contre les codes malveillants ;
- les exceptions ;
- les défaillances ;
- tout autre événement lié à la sécurité de l'information.

c) Le prestataire doit conserver les événements issus de la journalisation pendant une durée minimale de six mois sous réserve du respect des exigences légales et réglementaires.
d) Le prestataire doit fournir, sur demande d'un commanditaire, l'ensemble des événements le concernant.
e) Il est recommandé que le système de journalisation mis en place par le prestataire respecte les recommandations de [NT_JOURNAL].

12.7. Protection de l'information journalisée

a) Le prestataire doit protéger les équipements de journalisation et les événements journalisés contre les atteintes à leur disponibilité, intégrité ou confidentialité.
b) Le prestataire doit gérer le dimensionnement de l'espace de stockage de l'ensemble des équipements hébergeant une ou plusieurs sources de collecte afin de permettre la conservation locale des événements journalisés prévue par la politique de journalisation des événements. Cette gestion du dimensionnement doit prendre en compte les évolutions du système d'information.
c) Le prestataire doit transférer les événements journalisés en assurant leur protection en confidentialité et en intégrité, sur un ou plusieurs serveurs centraux dédiés et doit les stocker sur une machine physique distincte de celle qui les a générés.
d) Le prestataire doit mettre en place une sauvegarde des événements collectés suivant une politique adaptée.
e) Le prestataire doit exécuter les processus de journalisation et de collecte des évènements avec des comptes disposant de privilèges nécessaires et suffisants et doit limiter l'accès aux événements journalisés conformément à la politique de contrôle d'accès.

12.8. Synchronisation des horloges

a) Le prestataire doit documenter et mettre en œuvre une synchronisation des horloges de l'ensemble des équipements sur une ou plusieurs sources de temps internes cohérentes entre elles. Ces sources pourront elles-mêmes être synchronisées sur plusieurs sources fiables externes, sauf pour les réseaux isolés.
b) Le prestataire doit mettre en place l'horodatage de chaque événement journalisé.

12.9. Analyse et corrélation des événements

a) Le prestataire doit documenter et mettre en œuvre une infrastructure permettant l'analyse et la corrélation des événements enregistrés par le système de journalisation afin de détecter les événements susceptibles d'affecter la sécurité du système d'information du service, en temps réel ou *a posteriori* pour des événements remontant jusqu'à six mois.
b) Il est recommandé de s'appuyer sur le référentiel d'exigences des prestataires de détection d'incidents de sécurité [PDIS] pour la mise en place et l'exploitation de l'infrastructure d'analyse et de corrélation des événements.
c) Le prestataire doit acquitter les alarmes remontées par l'infrastructure d'analyse et de corrélation des événements au moins quotidiennement.

12.10. Installation de logiciels sur des systèmes en exploitation

a) Le prestataire doit documenter et mettre en œuvre une procédure permettant de contrôler l'installation de logiciels sur les équipements du système d'information du service.
b) Le prestataire doit documenter et mettre en œuvre une procédure de gestion de la configuration des environnements logiciels mis à la disposition du commanditaire, notamment pour leur maintien en condition de sécurité.
c) Le prestataire doit fournir une capacité d'inspection et de suppression, si nécessaire, des entrants (contrôle de l'authenticité et de l'innocuité des mises à jour, contrôle de l'innocuité des outils fournis, etc.) relatifs au périmètre de l'infrastructure technique :
- cette capacité d'inspection et de suppression doit générer des journaux d'activité et doit pouvoir faire l'objet d'un audit de code,
- les entrants doivent être traités sur des dispositifs spécifiques opérés et maintenus par le prestataire et hébergés dans une zone cloisonnée du reste de l'infrastructure.

12.11. Gestion des vulnérabilités techniques

a) Le prestataire doit documenter et mettre en œuvre un processus de veille permettant de gérer les vulnérabilités techniques des logiciels et des systèmes utilisés dans le système d'information du service.
b) Le prestataire doit évaluer son exposition à ces vulnérabilités en les incluant dans l'appréciation des risques et appliquer les mesures de traitement du risque adaptées.

12.12. Administration

a) Le prestataire doit documenter et mettre en œuvre une procédure obligeant les administrateurs sous sa responsabilité à utiliser des terminaux dédiés pour la réalisation exclusive des tâches d'administration, en accord avec le chapitre 4.1 intitulé « poste et réseau d'administration » de [NT_ADMIN]. Il doit les maîtriser et les maintenir à jour.
b) Le prestataire doit mettre en place des mesures de durcissement de la configuration des terminaux utilisés pour les tâches d'administration, notamment celles du chapitre 4.2 intitulé « sécurisation du socle » de [NT_ADMIN].
c) Lorsque le prestataire autorise une situation de mobilité pour les administrateurs sous sa responsabilité, il doit l'encadrer par une politique documentée. La solution mise en œuvre doit assurer que le niveau de sécurité de cette situation de mobilité est au moins équivalent au niveau de sécurité hors situation de mobilité (voir chapitres 9.6 et 9.7). Cette solution doit notamment inclure :

- l’utilisation d’un tunnel chiffré, non débrayable et non contournable, pour l’ensemble des flux;
- le chiffrement intégral du disque.

12.13. Télédiagnostic et télémaintenance des composants de l’infrastructure

a) Dans le cadre du télédiagnostic ou de la télémaintenance de composants de l’infrastructure, considérant les risques d’atteinte à la confidentialité des données des commanditaires, alors le prestataire doit :
- vérifier que la personne à qui l’accès doit être autorisé a satisfait aux vérifications de l’exigence 7.1.a relativement à la sensibilité ou à la spécificité des données du commanditaire ;
- vérifier que la personne à qui l’accès doit être autorisé est localisée au sein de l’Union Européenne ;
- dans le cas d'une intervention réalisée par une personne n’ayant pas satisfait aux vérifications de l’exigence 7.1.a, mettre en œuvre une passerelle sécurisée (poste de rebond) par laquelle la personne devra se connecter et permettant une supervision des actions (autorisation ou interdiction des actions, demande d’explications, etc.) en temps réel, par une personne ayant elle-même satisfait aux vérifications de l’exigence 7.1.a ;
- considérer les actions menées, une fois l’accès autorisé, comme des actions d’administration et les journaliser comme telles.
- supprimer l’autorisation d’accès à l’issue de l’intervention.

12.14. Surveillance des flux sortants de l’infrastructure

a) Le prestataire doit fournir une capacité d'inspection et de suppression des sortants de l’infrastructure technique relatifs au périmètre du service (informations de facturation, les éventuels journaux nécessaires au traitement d'incidents, etc.) :
- les sortants doivent pouvoir être expurgés des données pouvant porter atteinte à la confidentialité des données des commanditaires ;
- cette capacité d'inspection et de suppression doit générer des journaux d'activité et doit pouvoir faire l'objet d'un audit de code ;
- les sortants sont traités sur des dispositifs spécifiques opérés et maintenus par le prestataire, et hébergés dans une zone cloisonnée du reste de l’infrastructure.

13. Sécurité des communications

13.1. Cartographie du système d'information.

a) Le prestataire doit établir et tenir à jour une cartographie du système d’information du service, en lien avec l’inventaire des actifs, comprenant au minimum les éléments suivants :
- la liste des ressources matérielles ou virtualisées ;
- les noms et fonctions des applications, supportant le service ;
- le schéma d’architecture réseau au niveau 3 du modèle OSI sur lequel les points névralgiques sont identifiés :
- les points d’interconnexions, notamment avec les réseaux tiers et publics,
- les réseaux, sous-réseaux, notamment les réseaux d’administration,
- les équipements assurant des fonctions de sécurité (filtrage, authentification, chiffrement, etc.),
- les serveurs hébergeant des données ou assurant des fonctions sensibles ;
- la matrice des flux réseau autorisés en précisant :
- leur description technique (services, protocoles et ports) ;
- la justification métier ou d’infrastructure technique ;
- le cas échéant, lorsque des services, protocoles ou ports réputés non sûrs sont utilisés, les mesures compensatoires mises en place, dans la logique de défense en profondeur.

b) Le prestataire doit réviser au moins annuellement la cartographie.

13.2. Cloisonnement des réseaux

a) Le prestataire doit documenter et mettre en œuvre, pour le système d'information du service, les mesures de cloisonnement (logique, physique ou par chiffrement) pour séparer les flux réseau selon :
- la sensibilité des informations transmises ;
- la nature des flux (production, administration, supervision, etc.) ;
- le domaine d'appartenance des flux (des commanditaires – avec distinction par commanditaire ou ensemble de commanditaires, du prestataire, des tiers, etc.) ;
- le domaine technique (traitement, stockage, etc.).

b) Le prestataire doit cloisonner, physiquement ou par chiffrement, tous les flux de données internes au système d'information du service vis-à-vis de tout autre système d'information. Lorsque ce cloisonnement est réalisé par chiffrement, il est réalisé en accord avec les exigences du chapitre 10.2.

c) Dans le cas où le réseau d'administration de l'infrastructure technique ne fait pas l'objet d'un cloisonnement physique, les flux d'administration doivent transiter dans un tunnel chiffré, en accord avec les exigences du chapitre 10.2.

d) Le prestataire doit mettre en place et configurer un pare-feu applicatif pour protéger les interfaces d'administration destinées à ses commanditaires et exposées sur un réseau public.

e) Le prestataire doit mettre en œuvre sur l'ensemble des interfaces d'administration et de supervision de l'infrastructure technique du service un mécanisme de filtrage n'autorisant que les connexions légitimes identifiées dans la matrice des flux autorisés.

13.3. Surveillance des réseaux

a) Le prestataire doit disposer une ou plusieurs sondes de détection d'incidents de sécurité sur le système d'information du service. Ces sondes doivent notamment permettre la supervision de chacune des interconnexions du système d'information du service avec des systèmes d'information tiers et des réseaux publics. Ces sondes doivent être des sources de collecte pour l'infrastructure d'analyse et de corrélation des événements (voir chapitre 12.9).

14. Acquisition, développement et maintenance des systèmes d'information

14.1. Politique de développement sécurisé

a) Le prestataire doit documenter et mettre en œuvre des règles de développement sécurisé des logiciels et des systèmes, et les appliquer aux développements internes.

b) Le prestataire doit documenter et mettre en œuvre une formation adaptée en développement sécurisé aux employés concernés.

14.2. Procédures de contrôle des changements de système

a) Le prestataire doit documenter et mettre en œuvre une procédure de contrôle des changements apportés au système d'information du service.

b) Le prestataire doit documenter et mettre en œuvre une procédure de validation des changements apportés au système d'information du service sur un environnement de pré-production avant leur mise en production.

c) Le prestataire doit conserver un historique des versions des logiciels et des systèmes (développements internes ou externes, produits commerciaux) mis en œuvre pour permettre de reconstituer, le cas échéant dans un environnement de test, un environnement complet tel qu'il était mis en œuvre à une date donnée. La durée de conservation de cet historique doit être en accord avec celle des sauvegardes (voir chapitre 12.5).

14.3. Revue technique des applications après changement apporté à la plateforme d'exploitation

a) Le prestataire doit documenter et mettre en œuvre une procédure permettant de tester, préalablement à leur mise en production, l'ensemble des applications afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité du service.

14.4. Environnement de développement sécurisé

a) Le prestataire doit mettre en œuvre un environnement sécurisé de développement permettant de gérer l'intégralité du cycle de développement du système d'information du service.
b) Le prestataire doit prendre en compte les environnements de développement dans l'appréciation des risques et en assurer la protection conformément au présent référentiel.

14.5. Développement externalisé

a) Le prestataire doit documenter et mettre en œuvre une procédure permettant de superviser et de contrôler l'activité de développement externalisé des logiciels et des systèmes. Cette procédure doit s'assurer que l'activité de développement externalisé soit conforme à la politique de développement sécurisé du prestataire et permette d'atteindre un niveau de sécurité du développement externe équivalent à celui d'un développement interne (voir exigence 14.1 a).

14.6. Test de la sécurité et conformité du système

a) Le prestataire doit soumettre les systèmes d'information, nouveaux ou mis à jour, à des tests de conformité et de fonctionnalité de sécurité pendant le développement. Il doit documenter et mettre en œuvre une procédure de test qui identifie :
- les tâches à réaliser ;
- les données d'entrée ;
- les résultats attendus en sortie.

14.7. Protection des données de test

a) Le prestataire doit documenter et mettre en œuvre une procédure permettant d'assurer l'intégrité des données de tests utilisés en pré-production.
b) Si le prestataire souhaite utiliser des données du commanditaire issues de la production pour réaliser des tests, le prestataire doit préalablement obtenir l'accord du commanditaire et les anonymiser. Le prestataire doit assurer la confidentialité des données lors de leur anonymisation.

15. Relations avec les tiers

15.1. Identification des tiers

a) Le prestataire doit tenir à jour une liste exhaustive des tiers participant à la mise en œuvre du service (hébergeur, développeur, intégrateur, archiveur, sous-traitant opérant sur site ou à distance, fournisseurs de climatisation, etc.). Cette liste doit préciser la contribution du tiers au service et au traitement des données à caractère personnel. Elle doit tenir compte des cas de sous-traitance à plusieurs niveaux.
b) Le prestataire doit tenir à disposition du commanditaire la liste de l'ensemble des tiers qui peuvent accéder aux données et l'informer de tout changement de sous-traitants au sens de l'article 28 du [RGPD] afin que le commanditaire puisse émettre des objections à cet égard.

15.2. La sécurité dans les accords conclus avec les tiers

a) Le prestataire doit exiger des tiers participant à la mise en œuvre du service, dans leur contribution au service, un niveau de sécurité au moins équivalent à celui qu'il s'engage à maintenir dans sa propre politique de sécurité. Il doit le faire au travers d'exigences, adaptées à chaque tiers et à sa contribution au service, dans les cahiers des charges ou dans les clauses de sécurité des accords de partenariat. Le prestataire doit inclure ces exigences dans les contrats conclus avec les tiers.

b) Le prestataire doit contractualiser, avec chacun des tiers participant à la mise en œuvre du service, des clauses d'audit permettant à un organisme de qualification de vérifier que ces tiers respectent les exigences du présent référentiel.
c) Le prestataire doit définir et attribuer les rôles et les responsabilités relatives à la modification ou à la fin du contrat le liant à un tiers participant à la mise en œuvre du service.

15.3. Surveillance et revue des services des tiers

a) Le prestataire doit documenter et mettre en œuvre une procédure permettant de contrôler régulièrement les mesures mises en place par les tiers participant à la mise en œuvre du service pour respecter les exigences du présent référentiel.

15.4. Gestion des changements apportés dans les services des tiers

a) Le prestataire doit documenter et mettre en œuvre une procédure de suivi des changements apportés par les tiers participant à la mise en œuvre du service susceptibles d'affecter le niveau de sécurité du système d'information du service.
b) Dans la mesure où un changement de tiers participant à la mise en œuvre du service affecte le niveau de sécurité du service, le prestataire doit en informer l'ensemble des commanditaires sans délais et mettre en œuvre les mesures permettant de rétablir le niveau de sécurité précédent.

15.5. Engagements de confidentialité

a) Le prestataire doit documenter et mettre en œuvre une procédure permettant de réviser au moins annuellement les exigences en matière d'engagements de confidentialité ou de non-divulgation vis-à-vis des tiers participant à la mise en œuvre du service.

16. Gestion des incidents liés à la sécurité de l'information

16.1. Responsabilités et procédures

a) Le prestataire doit documenter et mettre en œuvre une procédure permettant d'apporter des réponses rapides et efficaces aux incidents de sécurité. Ces procédures doivent définir les moyens et délais de communication des incidents de sécurité à l'ensemble des commanditaires concernés ainsi que le niveau de confidentialité exigé pour cette communication.
b) Le prestataire doit informer ses employés et l'ensemble des tiers participant à la mise en œuvre du service de cette procédure.
c) Le prestataire doit documenter toute violation de données à caractère personnel et en informer son commanditaire. La violation doit être notifiée à la CNIL1 si elle présente un risque pour les droits et libertés des personnes concernées. Elle doit faire l'objet d'une information auprès des personnes concernées lorsque le risque pour leur vie privée est élevé.

16.2. Signalements liés à la sécurité de l'information

a) Le prestataire doit documenter et mettre en œuvre une procédure exigeant de ses employés et des tiers participant à la mise en œuvre du service qu'ils lui rendent compte de tout incident de sécurité, avéré ou suspecté ainsi que de toute faille de sécurité.
b) Le prestataire doit documenter et mettre en œuvre une procédure permettant à l'ensemble des commanditaires de signaler tout incident de sécurité, avéré ou suspecté et toute faille de sécurité.
c) Le prestataire doit communiquer sans délai aux commanditaires les incidents de sécurité et les préconisations associées pour en limiter les impacts. Il doit permettre au commanditaire de choisir les niveaux de gravité des incidents pour lesquels il souhaite être informé.
d) Le prestataire doit communiquer les incidents de sécurité aux autorités compétentes conformément aux exigences légales et réglementaires en vigueur.

16.3. Appréciation des événements liés à la sécurité de l'information et prise de décision

a) Le prestataire doit apprécier les événements liés à la sécurité de l'information et décider s'il faut les qualifier en incidents de sécurité. Pour l'appréciation, il doit s'appuyer sur une ou plusieurs échelles (estimation, évaluation, etc.) partagées avec le commanditaire.

Note : Les incidents de sécurité incluent les violations de données à caractère personnel.

b) Le prestataire doit utiliser une classification permettant d'identifier clairement les incidents de sécurité touchant des données relatives aux commanditaires, conformément aux résultats de l'appréciation des risques. Cette classification doit inclure les violations de données à caractère personnel.

16.4. Réponse aux incidents liés à la sécurité de l'information

a) Le prestataire doit traiter les incidents de sécurité jusqu'à leur résolution et doit informer les commanditaires conformément aux procédures.

b) Le prestataire doit archiver les documents détaillant les incidents de sécurité.

c) Il est recommandé que le prestataire fasse appel à un prestataire de réponse aux incidents de sécurité [PRIS] qualifié pour traiter les incidents de sécurité nécessitant une expertise supplémentaire.

16.5. Tirer des enseignements des incidents liés à la sécurité de l'information

a) Le prestataire doit documenter et mettre en œuvre un processus d'amélioration continue afin de diminuer l'occurrence et l'impact de types d'incidents de sécurité déjà traités.

16.6. Recueil de preuves

a) Le prestataire doit documenter et mettre en œuvre une procédure permettant d'enregistrer les informations relatives aux incidents de sécurité et pouvant servir d'éléments de preuve.