




La Sécurité



Introduction

Pour aborder la notion de protection des données dans le Cloud, il est important de la relier d'abord aux enjeux des Métiers. Cette réflexion sur l'analyse du risque encouru peut ainsi se structurer à partir de la question « **quel Cloud pour quel usage ?** ». Il s'agit donc de déterminer le niveau de protection nécessaire aux données hébergées, quelle que soit leur localisation, et de choisir l'offre la plus adaptée à l'usage souhaité.



Par ailleurs, force est de constater que cette nouvelle offre de Cloud, pour s'imposer sur un marché de masse, a centré sa communication sur la mise en valeur d'avantages incontestables en matière d'agilité, de capacité de réponse rapide à un besoin opérationnel, de réduction importante des coûts de déploiement et d'usage, et d'élasticité de l'offre, c'est-à-dire la capacité de s'ajuster au plus près de la croissance ou décroissance du besoin. Ainsi, l'aspect de la protection des données est, dans les faits, passé au second plan chez les fournisseurs de Cloud.

Par ailleurs, le retour d'expérience des entreprises montre que les offres actuelles de Cloud n'apportent pas un niveau de garantie satisfaisant en matière de protection des données confidentielles ou à caractère personnel.




Typologie des données

Pour protéger les données de façon adéquate, il est fondamental qu'elles soient inventoriées et qualifiées selon une typologie distinguant les données **sensibles** des autres données utilisées et traitées par le système d'information.

Pour qualifier les données, il existe de nombreuses méthodes, souvent lourdes à mettre en œuvre. Néanmoins, une méthode simple pour qualifier une donnée est d'évaluer quel serait l'impact pour l'entreprise si la donnée :

- était rendue indisponible,
- était utilisée ou modifiée par une personne non autorisée (interne ou externe),
- devenait publique ou largement diffusée.



et qu'il n'existait pas de surveillance efficace permettant de détecter cette perte de confidentialité, d'intégrité et de disponibilité, et d'en déterminer la cause et l'origine.

Ainsi, les données de l'entreprise peuvent être réparties selon les trois catégories suivantes :

- les données sensibles à caractère personnel (cf. CNIL),
- les données stratégiques pour l'entreprise,
- les autres données utilisées dans les applications métiers.



Nous définissons les données stratégiques de l'entreprise comme un ensemble d'informations qui, si elles étaient détenues ou mises en corrélation par des tiers, pourraient permettre de prendre de vitesse ou neutraliser une prise de position envisagée par l'entreprise et dont l'impact serait d'une telle ampleur, que la stratégie de l'entreprise serait fortement ou durablement impactée.

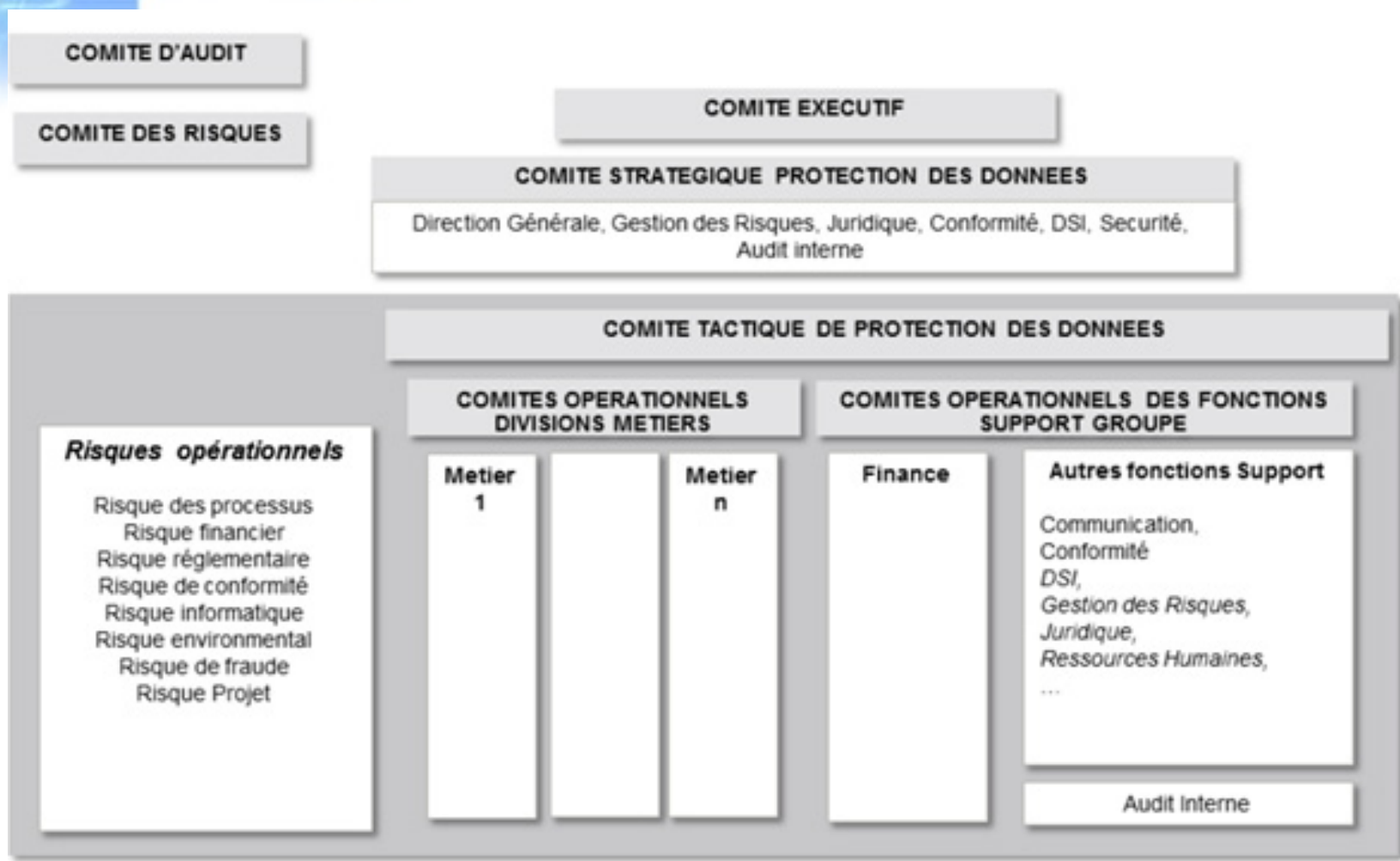
Par ailleurs, le caractère stratégique d'une donnée est lié à la durée de validité de l'axe stratégique de l'entreprise (fusion, appel d'offres...) qu'elle concerne.

Une donnée stratégique peut alors être confidentielle ou sensible pendant un temps déterminé, et perdre cette caractéristique ultérieurement.

Gouvernance de la protection des données



La protection des données n'est pas spécifiquement liée à l'émergence du Cloud. C'est une problématique ancienne et indispensable à la gestion de ces actifs informationnels et à la mise en conformité de l'entreprise avec le cadre législatif relatif à la protection des données. Néanmoins, la mise en œuvre d'une solution de Cloud Computing doit être l'occasion de mettre en place ou d'actualiser sa gouvernance de la protection des données. Avant de se lancer dans un projet Cloud, les entreprises doivent être préalablement sensibilisées à la protection des données et avoir mis en place un programme d'entreprise sur ce sujet. La DSI est un acteur incontournable de cette bonne gouvernance, mais il n'est pas le seul. En effet, elle implique de nombreux acteurs à tous les niveaux, comme le montre l'exemple ci-dessous, que l'on pourra adapter en fonction des spécificités de l'entreprise.



Exemple d'organigramme d'un programme de protection des données (Source Groupe de travail AFAI-CIGREF-IFACI 2013)



Comme tout dispositif de maîtrise des risques, la protection des données requiert :

- des objectifs clairs,
- le support du management,
- l'implication de toutes les parties prenantes (métiers et fonctions support groupe),
- une gouvernance (comités, rôles et responsabilités) appropriée,
- un plan d'action détaillé spécifiant les ressources et budget,
- un suivi du plan d'action.



Une implication responsable des propriétaires des traitements et des données

est indispensable en matière :

- d'identification et d'évaluation des risques,
- de qualification des données,
- de gestion des autorisations d'accès aux applications,
- de conception, de mise en œuvre, de test et de suivi de l'efficacité des contrôles associés.



La DSI est, quant à elle, impliquée dans la sécurisation :

- des applications,
- des bases de données et des systèmes,
- du réseau,
- des infrastructures,
- de la conception, de la mise en œuvre et du suivi de l'efficacité des contrôles.

L'audit interne contribue à la maîtrise de l'usage du Cloud en évaluant notamment :

- le processus de sélection,
- le référentiel de contrôle du prestataire,
- la gouvernance de la prestation, y compris par l'exécution de la clause contractuelle d'audit.




Questions à se poser avant de souscrire une offre Cloud

Avant de mettre en place une solution Cloud dans l'entreprise, il est nécessaire de répondre aux questions suivantes.

□ **Quels sont les traitements et les données susceptibles de migrer vers le Cloud ?**

La première question à se poser avant de souscrire une offre concerne l'identification des données qui seront hébergées dans le Cloud et de leur traitement. Certains types de données sont en effet soumis à des exigences réglementaires ou Métiers particulières, qu'il faut alors identifier avant de valider leur transfert dans le Cloud.



Il est important de ne pas faire de choix ponctuel, dicté uniquement par des considérations informatiques. Le choix doit être effectué à partir des services que l'on veut offrir aux utilisateurs :

- décrire au préalable le processus Métier de bout en bout, pour s'assurer de la continuité opérationnelle, vue par les utilisateurs,
- identifier les interfaces entre les SI internes et les futurs SI hébergés sur le Cloud, le chemin critique, les éventuelles ruptures de charge dans le flux des données,
- vérifier la cohérence de fonctionnement entre les SI internes et ceux qui seront hébergés sur le Cloud (temps de cycle, points de reprises en cas d'anomalies, gestion des changements, gestion des incidents...).

Quelles sont les opportunités du Cloud par rapport à une informatique « traditionnelle » ?

Pour une entreprise, les opportunités potentielles du Cloud, par rapport à une informatique plus traditionnelle, sont entre autres :

- une meilleure flexibilité et évolutivité, par la mise à disposition réactive des services et l'adaptation en continu, au niveau des besoins ;
- un accès rapide aux dernières technologies et sans nécessité d'investir en moyens et en compétences supplémentaires ;

Quelles sont les opportunités du Cloud par rapport à une informatique « traditionnelle » ?

- une baisse des coûts, à confirmer néanmoins de manière spécifique et systématique, issue de la mutualisation des infrastructures, la standardisation et la banalisation des applications : les dépenses d'investissements sont réduites et remplacées par un coût à l'usage, au juste nécessaire (selon une enquête réalisée en 2011 par la Commission européenne ¹, le Cloud permettrait à 80% des entreprises de réduire leurs coûts de 10% à 20%) ; pour des projets mal préparés ou mal suivis, le coût pourra être supérieur à d'autres solutions classiques.



Quels sont les risques à maîtriser ?

Les principaux risques inhérents à la mise en œuvre d'une solution Cloud dans le SI de l'entreprise sont 2 :

- Perte de maîtrise des traitements :
 - perte de maîtrise des normes et technologies mises en œuvre par le fournisseur ;
 - difficultés d'intégration entre services disponibles en interne et ceux qui sont sur le Cloud, ou entre diverses briques Cloud de fournisseurs différents ;
- Dépendance technologique et fonctionnelle vis-à-vis du fournisseur de Cloud et difficulté pour exercer la réversibilité du fait d'une perte de compétences SI et fonctionnelles en interne ;



- Faille dans la sécurité des données :

- disponibilité : perte de maîtrise du système d'information et manque de visibilité sur les dysfonctionnements ;

- intégrité : risque de perte de données, de destruction, d'altération par erreur ou malveillance ;

- confidentialité : risque d'intrusion, d'usurpation ou de non étanchéité entre les différents utilisateurs ;

- traçabilité difficile ou impossible des données et des accès ;

- problème de gestion des droits d'accès...

- Non maîtrise de la localisation des données et des intervenants ;

- Incapacité pour le client de répondre en temps et en heure aux requêtes judiciaires ;



- Réquisitions judiciaires imposées aux prestataires selon les juridictions compétentes entraînant une perte de confidentialité et/ou de disponibilité des données pour le client ;
- Non-conformité réglementaire, notamment sur les transferts internationaux ;
- Destruction ineffective ou non sécurisée des données, ou durée de conservation trop longue, au-delà des délais légaux de conservation (sauvegardes, archives...) ;
- Sauvegarde ineffective ;
- Incapacité du client à modifier l'application en cas d'évolution de ses besoins fonctionnels ;



- Faille dans la chaîne de sous-traitance impactant le niveau de service ;
- Indisponibilité du service du prestataire ;
- Difficulté à tester et à mettre en œuvre un Plan de Continuité d'Activité métier
(BCP) cohérent avec le DRP (Disaster Recovery Plan) du fournisseur ;
- Cessation d'activité du prestataire ou acquisition du prestataire par un tiers.



Une analyse de risques permet d'identifier les mesures de sécurité complémentaires à mettre en place dans l'entreprise au moment de la souscription de l'offre Cloud.

Ces mesures peuvent concerner l'entreprise comme le prestataire choisi

Quel Cloud pour quel traitement ?

Toutes les solutions de Cloud Computing ne sont pas adaptées à tous les types de données et de traitements dans l'entreprise.

Le choix du modèle privé ou public, voire partagé, interconnectant environnements externes et internes à l'entreprise doit prendre en compte, selon Gartner, plusieurs paramètres :

- Le calcul des coûts d'exploitation à court et moyen terme,
- Le niveau de flexibilité recherché,
- Les besoins de consacrer les ressources internes sur des activités à forte valeur ajoutée, favorable à l'innovation,



- Les contraintes des charges de travail,
- La sécurité,
- La qualité de services et la souplesse contractuelle vis-à-vis des fournisseurs
- La performance et la disponibilité,




Comment choisir le prestataire ?

La plupart des offres Cloud proposées sur le marché sont « standard ».


L'entreprise doit donc évaluer si les offres envisagées répondent aux exigences de sécurité préalablement définies en interne :

- Si l'entreprise dispose d'un cadre de contrôle interne relatif à la protection de données, elle doit le communiquer au prestataire,
- En l'absence d'un tel référentiel, elle peut s'appuyer sur des questionnaires d'évaluation fournis par des organismes de normalisation reconnus .



Evaluer le niveau de protection que le prestataire assure aux données traitées (confidentialité, intégrité, disponibilité, traçabilité) :

- par une exploitation sécurisée et efficace : sécurisation physique des locaux, sécurisation de l'infrastructure technique, gestion des incidents, gestion des changements, gestion et sauvegarde de la configuration, tests de sécurité, chiffrement des communications, journaux, redondance des moyens, gestion des identités, gestion des accès distants, procédures de surveillance et d'audit...
- par une confirmation de la localisation des données,
- par un personnel formé et expérimenté (politique d'embauche, de formation, encadrement des accès privilégiés, recours à des sous-traitants ou à des tiers...),



Le prestataire doit être capable d'apporter des garanties suffisantes notamment sur les mesures de sécurité et de confidentialité appropriées. Il doit également être transparent par rapport aux moyens employés.

Lors du choix du prestataire, il est primordial de :

- Déterminer la qualification juridique de la prestation, sachant que le prestataire peut être conjointement responsable du traitement en s'interrogeant sur :
 - la juridiction de référence,
 - la collecte des données,
 - l'usage des données
- S'assurer de la localisation des données



- par une définition explicite des niveaux de service (SLA, pilotage, support et assistance, escalade...),
- par l'assurance de la localisation des opérateurs.

Il faut également vérifier la possibilité d'exporter ses données (avec effacement total) afin de ne pas se retrouver ensuite dépendant de ce fournisseur.

L'établissement d'un Plan d'Assurance Sécurité 1 (PAS) approprié pourra être requis en fonction de la criticité des données, telle que définie dans l'analyse de risques.

Quel impact sur la politique de sécurité interne

?

Les problèmes de sécurité générés par le Cloud sont ceux déjà rencontrés dans l'utilisation quotidienne d'Internet par les entreprises, en particulier le problème de la confidentialité des échanges. Le passage au Cloud computing met en évidence,

voire amplifie, les failles de sécurité préexistantes en local.

Avant tout déploiement de SI basé sur le Cloud, le client doit disposer d'une infrastructure saine et fonctionnelle : vérifier et optimiser la sécurisation de ses données, de son infrastructure et de son réseau avant de passer au Cloud (antivirus, antispywares, monitoring réseau...). Il faut également faire évoluer les procédures,


Recommandations contractuelles relatives

à la protection des données

L'entreprise doit définir des critères de choix du prestataire à partir de l'analyse de risques : « quel niveau de service pour quelles données ? ».

Idéalement, le projet ne doit démarrer qu'une fois le contrat signé. Dans la pratique,

la finalisation contractuelle, qui est souvent une opération longue, peut s'achever après le démarrage du projet.



Dans ce cas, il est important d'intégrer dès la lettre d'intention une clause suspensive si les critères de protection des données requis ne sont pas atteints.

Au-delà des critères techniques mis en place par le fournisseur de service Cloud, il est primordial d'intégrer dans les clauses contractuelles des obligations fortes en matière de disponibilité, d'intégrité, de confidentialité, d'audit et de conformité exigées par l'entreprise, ses clients et les régulateurs.

Le cadre contractuel doit être validé par le département juridique, éventuellement assisté d'experts juridiques en matière de protection des données, afin d'engager la responsabilité du fournisseur, qui en cas de non-respect doit être soumis à des pénalités financières.

Le fournisseur devra pouvoir démontrer qu'il a mis en œuvre les mesures de sécurité adéquates par rapport au référentiel de contrôle du client.



Disponibilités des données ?

Pour se prémunir contre le risque de perte de données, il est préconisé de répliquer celles-ci sur un autre site distant et d'exiger un engagement de résultat de restauration des données dans des délais contractuels définis.

En cas de perte de données, le client doit être alerté et pouvoir enquêter.

Intégrité et confidentialité des données ?

Les clauses de responsabilité du contrat doivent être clairement définies, tout particulièrement en matière de respect de la confidentialité des données (accès non autorisés, voire frauduleux), et d'atteinte à leur intégrité. Dans certains cas,

comme par exemple, dans le domaine médical ou de la défense nationale, le client

pourra exiger que :

- ces données restent localisées sur des serveurs exclusivement situés dans l'UE,
- le prestataire soit français et/ou agréé par l'Etat,
- les moyens de contrôle de cette obligation lui soient fournis par son prestataire.



Avec un stockage et un accès aux données personnelles à l'intérieur de l'UE, le client s'exonérera ainsi d'un ensemble de formalités CNIL liées au transfert de données en dehors de l'UE.

Dans le domaine médical, le prestataire doit se conformer à un cahier des charges

strict qui donne lieu à des audits réguliers et à un agrément par le Ministère de la

Santé, valide pendant 3 ans.

Dans le cadre d'un service Cloud qui héberge des données à caractère personnel, géré par des opérateurs offshore (hors UE), il est nécessaire de s'assurer que l'on est en conformité avec les règlements relatifs aux transferts internationaux de données. Ceci est notamment vrai même si les données restent physiquement en Europe, mais que le personnel qui y accède se trouve en dehors de l'Europe.



Pour ce faire, le client et son prestataire peuvent recourir à l'un des mécanismes

ci-dessous :

- déclaration de transferts internationaux entre le contrôleur (propriétaire de données) et le processeur (fournisseur de service),
- Binding Corporate Rules 1 ,
- clauses contractuelles européennes (Standard Clauses 2).

Il est à noter que certains pays sont exemptés de tels dispositifs :



Il est à noter que certains pays sont exemptés de tels dispositifs :

- les États membres de l'UE : l'Allemagne, l'Autriche, la Belgique, la Bulgarie,

Chypre, le Danemark, l'Espagne, l'Estonie, la Finlande, la France, la Grèce, la Hongrie, l'Irlande, l'Italie, la Lettonie, la Lituanie, le Luxembourg, Malte,

les Pays-Bas, la Pologne, le Portugal, la République tchèque, la Roumanie, le

Royaume-Uni, la Slovaquie, la Slovénie et la Suède,

- les États membres de l'EEA : l'Islande, le Liechtenstein et la Norvège,

- les autres pays exemptés : Andorre, Argentine, Australie, Canada, Guernesey,

Ile de Man, Iles Féroé, Israël, Monaco, Suisse.



Convention de niveau de services - SLA (Service Level Agreement)

Une convention de niveau de service de sécurité doit être contractuellement définie avec le prestataire en fonction du niveau de protection requis pour la catégorie de données concernée et traiter notamment les incidents, la confidentialité, l'intégrité, la disponibilité, la traçabilité, les performances, les vulnérabilités.

La rédaction de cette convention de niveau de services peut s'inspirer du document de l'ANSSI : « Maîtriser les risques d'infogérance » - Chapitre 4 : Le plan d'assurance sécurité.



Convention de niveau de services - SLA (Service Level Agreement)

Le prestataire doit disposer d'outils de mesure, d'indicateurs du niveau de « service sécurité » et rendre compte de ces mesures au client. Un système de malus ou de pénalités pourrait être appliqué en cas de non-respect de la convention.

Dans le cas d'un service Cloud nécessitant un niveau de protection élevé, cette convention est une condition sine qua non.



Clause d'audit

Le prestataire de services de Cloud Computing doit intégrer dans son offre, un audit annuel par une société indépendante et/ou autoriser le client à organiser lui-même des audits ; le prestataire doit s'engager à traiter les déficiences observées. Attention, l'absence de clause d'audit dans le contrat peut rendre toute mission commanditée par le client non recevable.



Plan de réversibilité

Pour assurer une pérennité des services de Cloud, il s'avère primordial de contractualiser un plan de réversibilité permettant de transférer les services à d'autres prestataires ou de les réintégrer dans l'entreprise. Ce plan prévoira notamment les facteurs déclencheurs de cette réversibilité (carence du prestataire, libre choix du client à échéance du contrat après un certain nombre d'années...), les conditions de cette réversibilité (simple discontinuité du service, arrêt total du service...) et le coût de celle-ci pour l'entreprise.

La mise en œuvre de la réversibilité devra inclure la suppression des données par le prestataire sur ses moyens propres.

Mise en œuvre et pilotage de la protection des données

Pour assurer le respect des engagements contractuels, le client doit disposer de moyens de pilotage et de suivi opérationnel.

Le prestataire de services Cloud doit être en mesure de fournir des éléments de preuve suffisants à son client, à travers un dispositif de contrôle efficace et testé par des auditeurs indépendants. Le prestataire doit pouvoir communiquer ces éléments aux acteurs concernés (la direction, les auditeurs internes, les clients ou les régulateurs) et démontrer ainsi que le niveau de protection des données est satisfaisant.

Cette démonstration peut se concrétiser par la publication de « Rapports d'assurance » de type ISAE 3402

Structurer la gouvernance de la prestation

Dans la phase de mise en œuvre, il est nécessaire de déployer une gouvernance avec des responsabilités clairement définies et suivies lors de réunions du comité de pilotage. Les questions relatives à la protection des données doivent être plus spécifiquement suivies par un comité de sécurité.

Un comité de sécurité régulier doit être mis en place entre le client et le prestataire, et animé par les correspondants sécurité des deux parties pour traiter des sujets suivants :

- la conformité des services de sécurité (patchs sécurité, anti-virus...),
- la gestion du risque opérationnel (identification, évaluation, remédiation) et le suivi des actions de remédiation des vulnérabilités critiques identifiées,
- les incidents, les intrusions et leur traitement,
- la gestion des contrôles, des audits et des rapports d'assurance (planification, périmètre, certification).

Définir et mettre en place les mesures de protection exigées

- Périmètre des contrôles par rapport aux services fournis

Le client doit vérifier que le périmètre de contrôle du prestataire couvre bien le service demandé. Il est possible, par exemple, que le prestataire n'ait mis en œuvre qu'un sous-ensemble des activités de contrôle attendues.

A titre d'exemple, un prestataire peut avoir mis en œuvre des activités de contrôle en matière de sécurité physique et environnementale, ainsi qu'en matière de sécurité réseau mais très peu en matière de sécurité logique, parce que le prestataire avait historiquement un métier d'hébergeur (IaaS) et a peu de maturité en matière de service logiciel (SaaS). Dans ce cas, le prestataire disposera d'un rapport, qui est un gage de sécurité physique, mais qui ne couvre pas les activités de contrôle liées aux accès logiques.

Définir et mettre en place les mesures de protection exigées

Objectifs et activités de contrôle

En matière de protection de données, on peut distinguer cinq familles d'objectifs de contrôle :

1. **les données sensibles** : le prestataire doit mettre en œuvre, de façon cohérente, les processus en matière de sécurité, gestion du personnel, inventaire, qualification et traçabilité des données,
2. **les datacenters** : le prestataire doit disposer d'une gestion sécurisée des accès physiques aux datacenters,
3. **la sécurité des accès logiques** : le prestataire doit disposer de contrôles d'accès logiques assurant la protection des données,

Définir et mettre en place les mesures de protection exigées

4. **la sécurité des systèmes** : le prestataire doit disposer de systèmes correctement configurés et protégés des failles de sécurité, en particulier pour

les environnements hébergeant les données,

5. **la sécurité du réseau** : le prestataire doit disposer d'un réseau sécurisé avec un isolement approprié des autres clients.



Assurer le suivi de la prestation

Le suivi de la prestation implique que le client :

- suive et contrôle les indicateurs de niveau de service de sécurité transmis par le prestataire à l'occasion de chaque réunion du comité sécurité,
- analyse les rapports d'assurance du prestataire,
- active la clause d'audit (notamment la capacité du client à réaliser des tests d'intrusion permettant de mesurer la robustesse effective de la sécurité de la prestation) et l'organiser en coordination avec le prestataire.



Données

Le prestataire assure que :

- la localisation des données sensibles du client est connue et conforme aux exigences du client (datacenter et serveur),
- les systèmes de sauvegardes et plans de secours informatiques associés sont mis en œuvre,
- il dispose d'un code d'éthique appliqué par son personnel et il n'exerce pas des activités pouvant entraîner un risque de conflits d'intérêt,
- son personnel suit régulièrement des formations de sensibilisation à la sécurité,
- il dispose de moyens de traçabilité centralisés permettant de détecter des violations de privilèges ou des comportements malveillants,
- il dispose d'une gestion des incidents de sécurité incluant la détection, l'alerte, le traitement jusqu'à la résolution, l'identification des causes et la communication au client.

Sécurité des accès physiques

Le prestataire assure que :

- il dispose de systèmes d'accès physique sécurisés, de détection d'intrusion et de vidéo surveillance,
- les accès aux datacenters sont autorisés aux seules personnes habilitées en suivant un circuit d'approbation approprié, ils sont tracés et revus régulièrement,
- tout sous-traitant de maintenance amené à utiliser ou réparer des équipements contenant des données sensibles est soumis à des clauses contractuelles de confidentialité,
- tout media de stockage de données contenant des données sensibles et destiné à être mis au rebus ou recyclé fait l'objet d'un effacement physique préalable de ces données.

Sécurité des accès logiques

Le prestataire assure que :

- il applique les règles d'autorisation d'accès aux données en fonction des éléments communiqués par le client (création, modification et suppression) ; il fournit la liste des accès au client,
- les accès des utilisateurs et administrateurs aux systèmes contenant des données sensibles s'appuient sur des mécanismes assurant la confidentialité et la traçabilité (pistes d'audit sur les accès aux données et traitement de la problématique des comptes génériques),
- il applique une politique d'authentification et de mot de passe conforme à celle du client.

Sécurité des systèmes

Le prestataire assure que :

- les données sauvegardées quel que soit le support sont chiffrées,
- il gère les vulnérabilités des systèmes et organise au moins annuellement des tests d'intrusion ; les vulnérabilités critiques identifiées sont corrigées immédiatement,
- les serveurs hébergeant des données sensibles sont configurés avec un niveau de sécurité renforcé ; les patches de sécurité sont gérés de façon centralisée et appliqués dans des délais inférieurs à un mois,
- les anti-virus sont installés sur les serveurs, mis à jour et supervisés,
- l'usage des clés USB ou autres media de stockage mobile est contrôlé et interdit sur tous les systèmes contenant des données sensibles.



Sécurité des accès au réseau

Le prestataire assure que :

- les points d'entrée au réseau sont limités, sécurisés et filtrés,
- les tâches d'administration des systèmes sont opérées depuis un réseau d'administration dédié et isolé en se connectant avec des mécanismes d'authentification forte,
- les changements d'équipement réseau sont tracés, documentés et approuvés,
- dans le cas d'un Cloud partagé :
 - l'accès au réseau est autorisé uniquement à des terminaux de confiance,
 - le réseau sur lequel sont connectés les systèmes hébergeant les données sensibles est isolé du réseau des autres clients.

Les analystes de Gartner ont identifié sept défis de sécurité empêchant les entreprises adoptent le modèle Cloud Computing, énumérés ci-dessous :

a. accès utilisateurs privilégiés. Les informations transmises par le client par le biais d'Internet posent un certain degré de risque, en raison de problèmes de propriété des données; les entreprises doivent passer du temps pour connaître leurs fournisseurs et leurs règlements, autant que possible avant d'attribuer certaines applications triviales.




b. **conformité à la réglementation.** S'assurer que le vendeur est d'accord pour avoir des

audits externes ainsi que des certifications de sécurité.

c. **localisation des données.** Savoir si le fournisseur offre un contrôle sur la localisation des données.

d. **ségrégation des données.** S'assurer que le chiffrement est possible à tous les niveaux et que les schémas de chiffrement aient été testés et approuvés.

e. **récupération.** Chaque fournisseur doit avoir un protocole de récupération de données pour protéger les données des utilisateurs.



f. soutien aux enquêtes. Si un client soupçonne une activité défectueuse du fournisseur, il peut ne pas y avoir beaucoup de moyens juridiques pour poursuivre une enquête.

g. viabilité à long terme. Se réfère à la capacité de rétracter un contrat et toutes les données si le fournisseur actuel est racheté par une autre entreprise.



Mesures de sécurité dans le Cloud Computing:

Diverses mesures de sécurité ont été proposées pour résoudre les problèmes de sécurité et contrer les menaces dans un environnement de Cloud Computing. Ces mesures sont classées

de façon générale en :

- virtualisation. Chaque locataire peut bénéficier d'un environnement isolé complètement virtuel pour son exécution ;
- virtual Private Network (VPN). L'échange de données entre le fournisseur de Cloud et l'utilisateur peut être assuré par l'utilisation de VPN ;




-identité fédérée (Federated Identity). C'est la capacité de transporter des données à travers des domaines de sécurité utilisant des allégations et affirmations à partir d'un fournisseur d'identité signé numériquement. Les utilisateurs qui ont déjà été authentifiés dans le réseau de l'organisation devraient être autorisés à utiliser les services en cours d'exécution sur le Cloud. Cela est assuré par un service d'identité fédérée, qui relie ensemble la gestion des identités de l'organisation et le fournisseur de services Cloud ;

-gestion de politique. Définit des politiques permettant de décider quel fournisseur choisir en se basant sur des facteurs tels que la fiabilité, la sécurité, etc... ;



la virtualisation:

La virtualisation est le point clé définissant un environnement de Cloud Computing. Dans un environnement multi-locataire, il est nécessaire d'avoir un isolement entre les processus des différentes organisations. Un bug dans l'application ou dans le système d'exploitation peut conduire à un problème. La solution est soit d'allouer des machines physiques distinctes, soit des machines virtuelles distinctes. Bien sûr, la virtualisation dans cette situation devient une solution plus rentable. En plus de la séparation des processus la virtualisation offre d'autres avantages, tels qu'une rapide élasticité, où les ressources peuvent être ajoutées ou retirées en fonction de la demande



de l'organisation. Un autre avantage de la virtualisation est la portabilité : il est facile de déplacer des machines virtuelles d'une machine physique à une autre. Les organisations peuvent aussi déployer des solutions de sécurité sur leur espace virtuelle augmentant encore plus le niveau de sécurité. Des solutions comme le pare-feu, la détection et la prévention d'intrusion, la surveillance de l'intégrité, l'inspection des logs, la confiance, etc...



Pare-feu:

Un pare-feu est un système conçu pour empêcher l'accès non autorisé à ou à partir d'un réseau privé. Il peut aider en diminuant le domaine d'attaque des serveurs virtuels d'un environnement de Cloud Computing.

Le déploiement de pare-feu sur des machines virtuelles (VM) utilisant des politiques correspondant aux besoins de l'organisation permet l'isolement de la machine virtuelle, le filtrage des données, la ségrégation des données couvrant l'ensemble des protocoles basés sur IP, les types de trames, etc... Les attaques telles que les dénis de service (DoS) peuvent être évitées. Les pare-feu permettent également l'établissement de différentes politiques sur différentes interfaces réseau.



Détection et prévention des intrusions (IDS / IPS):

IDS et IPS protègent des vulnérabilités dans les systèmes d'exploitation et les applications jusqu'à ce qu'ils puissent être corrigés et mis-à-jour, pour assurer une protection rapide contre les attaques connues.

Un IDS et IPS peuvent détecter les nouvelles vulnérabilités découvertes dans les applications et le système d'exploitation dans la VM, ce qui fournit une protection contre les tentatives pour compromettre les machines virtuelles. Il existe des IDS et IPS basés sur des techniques d'intelligence artificielle, permettant la découverte de nouvelles vulnérabilités dynamiquement.



Surveillance de l'intégrité:

Les fichiers système critiques (fichiers, répertoires, clés de registre et les valeurs, etc...)


peuvent être surveillés pour détecter les modifications malveillantes et inattendues qui pourraient signaler un compromis des ressources. Le logiciel de surveillance de l'intégrité doit être appliqué au niveau de la machine virtuelle. Une solution de surveillance de l'intégrité devrait permettre:

- une détection à la demande ou programmée ;
- un contrôle complet de propriété de fichier, y compris les attributs ;
- une surveillance au niveau de l'annuaire ;
- une surveillance flexible et pratique par le biais d'inclusion/exclusion ;
- des rapports d'audit.



Inspection des journaux:

L'inspection de journaux recueille et analyse les journaux de log du système d'exploitation et des applications pour une analyse de sécurité. Des règles sont définies dans l'inspection des logs permettant l'extraction efficace d'événements liés à la sécurité. Ces journaux peuvent être envoyés à un système de sécurité autonome ou à un système d'information de sécurité et de gestion d'événement (SIEM 11) ou à un serveur de journalisation centralisée pour l'analyse. Le logiciel d'inspection de logs sur les ressources Cloud permet de détecter tout comportement suspect.



Dans le cadre du paradigme du Cloud Computing, une organisation renonce à un contrôle direct sur de nombreux aspects de la sécurité et, ce faisant, confère un niveau sans précédent de confiance au fournisseur de services. Divers défis se rapportant à la confiance peuvent être considérés :


- Accès interne. La menace pour la sécurité interne est un problème bien connu pour la plupart des organisations et s'applique aussi aux services de Cloud Computing sous- traitant.

Le déplacement de données et d'applications dans un environnement de Cloud Computing externe élargit le risque pour la sécurité interne, non seulement au personnel du prestataire de services mais aussi potentiellement aux autres clients utilisant le service.




Services de composites. Les services Cloud peuvent être composés par d'autres services. Les fournisseurs de services qui sous-traitent certains services à partir d'un tiers fournisseur peuvent rencontrer certaines difficultés comme la portée du contrôle sur la tierce partie, les responsabilités en cause et les remèdes et recours disponibles en l'accord.

cas de problème. La confiance est souvent non transitive, exigeant que les arrangements d'un tiers soient divulgués avant de parvenir à un accord avec le prestataire de services et que les modalités de ces ententes soient maintenues tout au long de



Visibilité. L'utilisation de services Cloud laisse le contrôle au fournisseur pour sécuriser les systèmes sur lesquels les données et les applications fonctionnent. Pour éviter de créer des lacunes dans la sécurité, des contrôles de gestion, de procédures et de techniques doivent être appliqués proportionnellement à celles qui sont utilisés pour les systèmes internes de l'organisation. C'est une tâche colossale, puisque les mesures pour comparer la sécurité de deux systèmes informatiques demeurent un domaine de recherche continu. En outre, le suivi du réseau et du système par l'utilisateur est généralement en dehors du champ d'application de la plupart des services, ce qui limite la visibilité et les moyens de vérification des opérations directement.



gestion des risques. Avec les services Cloud, certains sous-systèmes ou composants de sous-système sont en dehors du contrôle direct de l'organisation qui détient l'information et autorise l'utilisation du système. Certains se sentent plus à l'aise quand ils ont plus de contrôle sur les processus et les équipements concernés. Au minimum, un degré élevé de contrôle offre la possibilité de considérer d'autres solutions, établir des priorités et agir de façon décisive dans l'intérêt de l'organisation lorsqu'ils sont confrontés à un incident. Lors du choix entre une solution en interne et une mise en œuvre dans le Cloud, les risques associés doivent être évalués en détail. Évaluer et gérer les risques dans les systèmes qui utilisent les services de Cloud peut être un défi.

Menaces, vulnérabilités et attaques dans le cloud

Le cloud computing est particulièrement exposé à des menaces et vulnérabilités pouvant être de natures variées. Nous présentons les principales caractéristiques des attaquants, menaces et vulnérabilités présentes dans le cloud.



Nature des attaquants


Pour comprendre qui peuvent être les attaquants dans le cloud, nous partons du principe que tout acteur du cloud est un attaquant potentiel. Un acteur est une personne pouvant remplir un ou plusieurs rôles. Il existe de nombreux rôles possibles dans le cloud. Celui-ci étant aussi un modèle économique, certains rôles sont des fonctions à tendance plus économique (liée aux notions de service, client et fournisseur). Par ailleurs, les infrastructures cloud impliquant de nombreux composants technologiques,



d'autres rôles sont à tendance plus technologique (liée aux contrôles sur les composants). Le Tableau 1.2 reprend les différents rôles tels que cités dans la littérature, selon qu'ils sont d'une orientation économique ou technologique. Dans la suite de ce document, nous nous focaliserons sur les rôles économiques de client et fournisseur de services.

Auteurs	Rôles économiques	Rôles technologiques
NIST [112]	Consommateur de services cloud Fournisseur de services cloud Développeur de services cloud Distributeur de services cloud	
Bauer et Adams [48]	Vendeurs Fournisseur de services Consommateurs du cloud Utilisateurs finaux	
Vaquero <i>et al.</i> [142]	Fournisseur de services Utilisateur de services Fournisseur d'infrastructure	
Leimeister <i>et al.</i> [92]	Client Fournisseur de services Fournisseur d'infrastructure Agrégateur de fournisseurs de services Fournisseur de plateforme Consultant	
Eucalyptus [73]	Manager Manager de services cloud Utilisateur de cloud Architecte des données cloud Administrateur de stockage cloud	Administrateur système Opérateur d'ordinateur Administrateur réseau Administrateur de stockage Administrateur de base de données Utilisateur final Architecte de cloud Développeur de code Administrateur de cloud Opérateur de cloud Architecte d'application cloud Développeur cloud

Tableau 1.2 – Rôles dans le cloud



administrateur employé de l'organisation cliente, même si ceci n'est pas fréquent dans le cloud car l'administrateur est généralement employé par le fournisseur de cloud. Un employé qui veut nuire à son employeur (le fournisseur de cloud) pourrait faire des dégâts à une organisation cliente pour desservir la réputation du fournisseur de cloud.

Les quatre niveaux d'administrateurs considérés ici sont :

1. Administrateurs d'applications.
2. Administrateurs système.
3. Administrateurs des machines virtuelles.
4. Administrateurs de l'hébergement.



Un administrateur a les privilèges des administrateurs de tous les niveaux qui lui sont inférieurs (par exemple, un administrateur système a également les privilèges de l'administrateur d'applications). Le second type d'attaquant interne est celui qui cherche (potentiellement dirigé par une source externe) à obtenir un accès non autorisé aux données de son organisation qui utilise le cloud. un troisième type d'attaquant interne est même proposé, proche du précédent, mais à la différence que



l'employé de l'organisation utilise des services cloud pour mener une attaque sur son propre employeur, mais pas forcément sur des données localisées dans le cloud. En résumé, la classification des attaquants internes du cloud sépare donc les administrateurs du fournisseur de cloud (avec différents niveaux ciblant son employeur ou une organisation cliente) et employé de l'organisation cliente (ciblant son employeur à travers le cloud).
les attaquants internes sont différenciés selon :



fournisseur

de services, employé du fournisseur de services et employé (avec des privilèges d'accès autorisés) dans l'organisation de l'utilisateur du cloud. Toujours d'après , un attaquant externe correspond simplement à un utilisateur n'appartenant pas à l'organisation de sa victime. Son rayon d'action est relativement vaste, pouvant agir depuis Internet et pouvant généralement facilement s'introduire dans le périmètre cloud en souscrivant à un abonnement par exemple.

Classes d'attaques, incidents, et menaces


La littérature offre différentes manières de classer des attaques informatiques, en fonction de différents critères : type d'attaquant, objectif de l'attaque, vecteur d'attaque, cible de l'attaque, résultat de l'attaque, etc. Etant donné la complexité des rôles parmi les acteurs du cloud, la diversité des cibles et des objectifs potentiels, il est plus pertinent d'utiliser le vecteur d'attaque pour obtenir une classification ordonnée et facilement compréhensible. Par conséquent, pour présenter les grandes familles d'attaques informatiques, nous avons retenu une classification reposant sur le vecteur d'attaque comme critère. Un vecteur d'attaque est le moyen pour une attaque d'atteindre sa cible.



Le Tableau 1.3 présente une classification des attaques informatiques par vecteur d'attaque. Elle permet de donner une vue d'ensemble des catégories d'attaques informatiques principales, mais n'a pas pour but de lister toutes les attaques existantes. Nous y avons répertorié les principales attaques retrouvées dans les environnements cloud. Ces attaques incluent des vulnérabilités connues et traditionnellement retrouvées dans les infrastructures physiques. Cependant, leur exploitation et leur visibilité sont facilitées par la concentration actuelle de capacités importantes de calculs et de stockage, Par ailleurs, on retrouve aussi de nouvelles formes d'attaque spécifiques aux environnements virtuels comme les attaques par reconnaissance et canaux auxiliaires .

	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
Malware		Virus			
		Verus			
		Chevaux de Troie			
Défis de service	Hôte	X-DoS		XML Parser DoS	
				XML Attribute Blowup	
				XML Entity DoS	
			B-DoS		
			ReDoS		
		Public Key DoS			
		Ping of Death			
	Réseau	Flooding		TCP flooding	
				UDP flooding	
				ICMP flooding	
			SIP flooding		
			XML flooding		
	Smurfing		STP BPDU flooding		
Attaques applicatives	Débordements de tampon	File			
	Débordements d'entier	Tim			
	Chaînes de format				
Attaques réseau	Spoofing	ARP Spoofing		Attaques par Gratuitous ARP	
				Attaques par réponse ARP	
				Attaques par requête ARP forgée	
			IP Spoofing		
			STP BPDU Spoofing		
	Vol de sessions	Interceptions SSL/SSH			
	Attaques sur les réseaux sans-fil				
	Attaques applicatives Web	Injections		Injections XML	Injections de référence d'entité
				Injections SQL	Injections par échappement de caractères
				Injections XPath	
		XSS			
		CSRF			
		Violations de gestion d'authentification et de session		SOAPAction Spoofing	
		Attaques SOAP		WS-Addressing Spoofing	
			XML Signature Element Wrapping		
		Redirections de référence			
		Attaque SOAP Array			
Attaques sur les VLAN	VLAN Hopping	Switch Spoofing			
Attaques sur les VXLAN	VXLAN Spoofing	Double tagging			
Attaques DMA					
Attaques physiques	Van Eck phreaking				
Attaques sur les mots de passe	Estimations		Attaques par force brute		
			Attaques par dictionnaire		
Attaques d'écoute et reconnaissance	Sniffing	Canal auxiliaire		Etude des traces	
				Etude des accès	
				Etude temporelle	
	Mapping	Vérifications de co-résidence		Vérifications par temps de réponse réseau	
				Vérifications par adressage IP	
				Vérifications par passerelle réseau	
Scanning	Scan de ports		Scan TCP		
			Scan UDP		
			Scan ICMP		

Tableau 1.3 – Classification d'attaques par vecteur d'attaque



attaques applicatives Web constituent une proportion prédominante des incidents du cloud, ces derniers sont de plus en plus proches que ceux historiquement rencontrés dans les infrastructures traditionnelles.

Classe d'incident	Définition
Attaques applicatives	Tentatives d'exploit sur des applications ou services ne s'exécutant pas sur le protocole HTTP.
Attaques par force brute	Tentatives d'exploit comptant un grand nombre de combinaisons pour trouver une faille.
Activité de malware/botnet	Activité malveillante d'un logiciel installé sur un hôte et pouvant communiquer à l'aide d'un canal de commande et contrôle.
Attaque de reconnaissance	Activité centrée sur les balayages et la cartographie de réseaux, applications ou services.
Scan de vulnérabilité	Découverte automatique de vulnérabilités.
Attaques applicatives Web	Attaques ciblant l'interface, la logique ou la base de données d'une application Web.

Tableau 1.4 – Classes d'incidents dans le cloud



De son côté, la Cloud Security Alliance (CSA) a défini sept grandes classes de menaces pour le cloud :

- Abus et usage néfaste du cloud.
- APIs et interfaces non sécurisées.
- Malveillance interne.
- Problèmes liés aux technologies de partage.
- Perte ou fuite de données.
- Détournement de compte ou de service.
- Profil de risque inconnu.

Ces efforts de classification témoignent de la prise de conscience des dangers liés aux menaces dans le cloud et de l'importance actuelle de sécuriser ces environnements.

Mécanismes de sécurité réseau dans le cloud

Les mécanismes de sécurité réseau ont pour but d'assurer la sécurité des hôtes et applications des réseaux auxquels ils appartiennent. Nous nous intéressons particulièrement à deux mécanismes de sécurité réseau :

- Le contrôle des accès réseau, réalisé par les pare-feu ou firewall.
- La détection d'intrusion, réalisée par les systèmes de détection d'intrusion ou Intrusion Detection Systems (IDS).

Ces mécanismes ont pour but d'appliquer la politique de sécurité au sein des réseaux qu'ils protègent.

Pare-feu virtuels

Un pare-feu est un outil permettant de contrôler le trafic circulant entre l'intérieur et l'extérieur d'un périmètre de sécurité . Le périmètre de sécurité constitue la limite entre le réseau que l'on considère comme sûr ou que l'on désire protéger et le reste de l'Internet . Les pare-feu peuvent offrir différents services, mais nous nous

Pare-feu virtuels

intéressons au service de base, à savoir le contrôle d'accès au niveau réseau. La fonction principale du contrôle d'accès réseau est le filtrage de paquets, opéré par des règles de filtrage permettant d'interdire ou autoriser certains types de trafic. Ces règles sont établies en fonction des paramètres des en-têtes protocolaires situés dans les paquets. Elles sont appliquées sur chaque paquet transitant par le pare-feu, en respectant un certain ordre de priorité dans l'application des règles. La plupart des pare-feu sont

Pare-feu virtuels

il existe les deux types de pare-feu virtuels suivants, illustrés par la Figure 1.5 :

– Pare-feu en mode pont : machine virtuelle déployée comme passerelle des réseaux virtuels, capable de router, filtrer et traduire les adresses du trafic entrant et sortant.

Ces pare-feu sont généralement contrôlés par les clients.

– Pare-feu en mode hyperviseur : composant logiciel embarqué dans l'hyperviseur qui filtre le trafic envoyé ou reçu par les machines virtuelles sans prendre en compte la topologie réseau. Il est généralement contrôlé par le fournisseur de services, mais certaines règles peuvent être appliquées par les clients seulement sur certains réseaux virtuels, ce qui implique de donner un contrôle partiel aux clients sur ce type de pare-feu.

Pare-feu virtuels

généralement à suivi d'état ou plus simplement à états (stateful en anglais), c'est-à-dire qu'ils vérifient en plus l'appartenance des paquets à une connexion en cours (comme une connexion TCP) avant de les autoriser. Ils vérifient ainsi que chaque paquet autorisé par les règles initie une nouvelle connexion ou fait bien partie d'une connexion déjà existante. En outre, différents niveaux d'inspection peuvent être réalisés sur les paquets. Le niveau le plus courant est le Deep Packet Inspection (DPI) qui s'attache à regarder le contenu d'un paquet en profondeur pour autoriser l'accès ou non. Les pare-feu applicatifs Web ou Web Application Firewall (WAF), dédiés à la protection des serveurs Web, sont également de plus en plus répandus.

Mécanismes de sécurité réseau dans le cloud

Pare-feu virtuels

La complexité des architectures cloud, couplée à la complexité des applications actuelles, rend les exigences en contrôle d'accès réseau plus importantes. Le travail des pare-feu, en charge de ces contrôles d'accès, est de ce fait rendu plus compliqué. Le périmètre de sécurité est plus complexe à dessiner que dans un environnement traditionnel, du fait de la multiplicité des organisations présentes dans le cloud. Ainsi, le positionnement des pare-feu et leur comportement sont des aspects stratégiques. Pour maintenir une défense en profondeur dans les infrastructures virtuelles,

Systemes de détection d'intrusion

la détection d'intrusion concerne l'ensemble des pratiques et mécanismes utilisés pour la détection d'erreurs pouvant conduire à une défaillance de sécurité, et/ou pour la détection d'attaques, un IDS est l'implémentation des pratiques et mécanismes de détection d'intrusion. Les IDS ont donc pour rôle de détecter et/ou bloquer (on parle dans ce cas d'Intrusion Prevention System) des attaques survenant au sein d'un système ou d'un réseau. Ils peuvent être déployés sur l'hôte surveillé, on parle alors de Host-Based Intrusion Detection System (HIDS) ;
ou bien sur le réseau surveillé, on parle alors de Network-Based Intrusion Detection

Systemes de détection d'intrusion

System (NIDS).

Comme le montre la Figure 1.6, il existe deux techniques principales de détection :

par signatures (signature-based detection ou misuse detection en anglais) ou par comportements (anomaly detection en anglais). L'approche par signatures consiste à détecter des attaques en vérifiant si les observations correspondent à des attaques connues, tandis que l'approche par comportements (ou par détection d'anomalies) consiste à détecter une attaque en vérifiant que les observations ne correspondent pas à des comportements légitimes de référence. Certains IDS combinent les deux approches afin d'obtenir de meilleurs résultats.

Systemes de détection d'intrusion

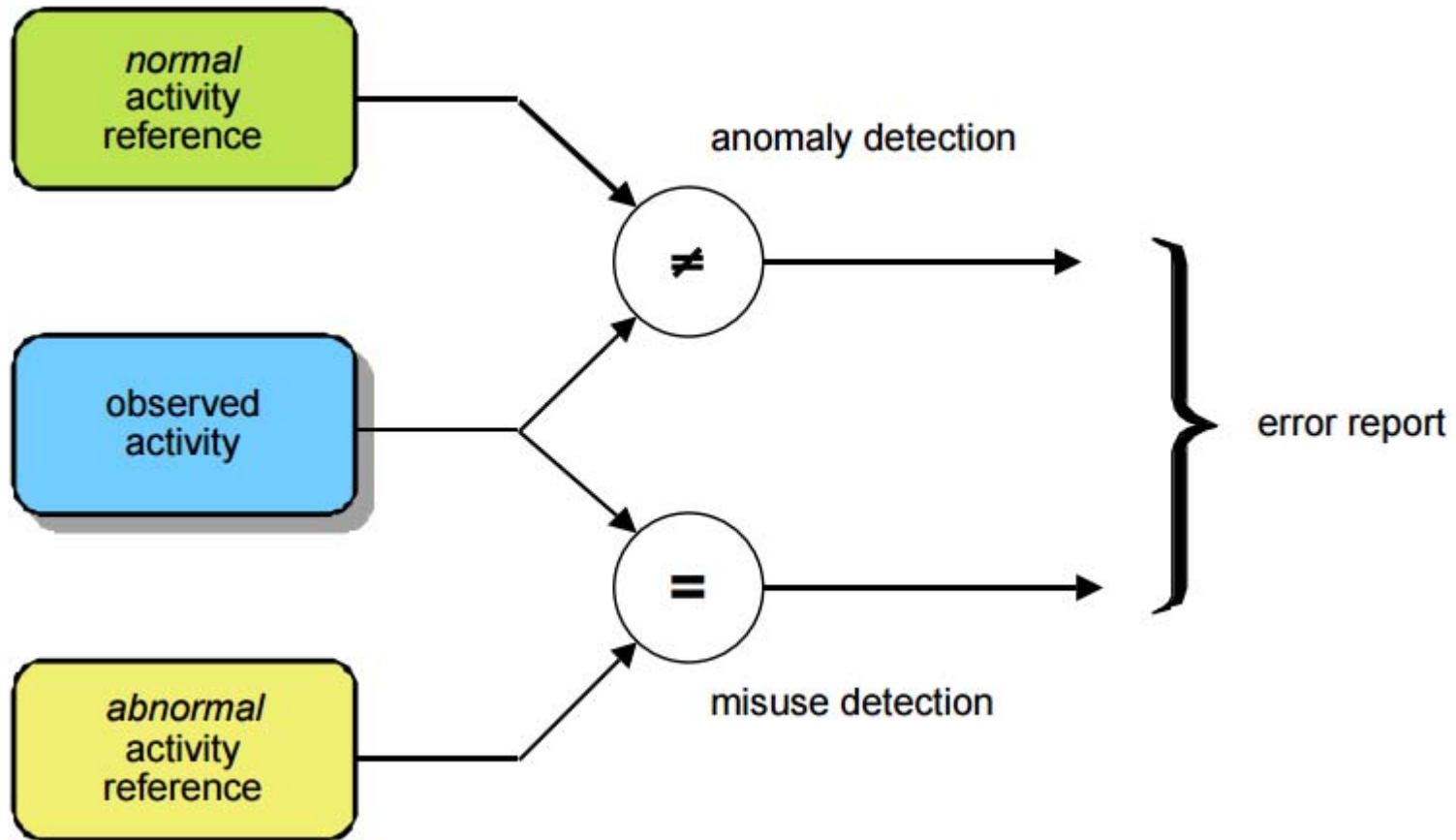


Figure 1.6 – Techniques de détection d'intrusion (extrait de [120])

Niveaux de déploiement des sondes dans le cloud

Dans une infrastructure physique traditionnelle, les sondes de détection sont généralement placées en entrée des réseaux à surveiller, ou dans les systèmes d'exploitation à surveiller. Dans le cloud, la multitude d'organisations partageant l'infrastructure et l'ajout de la virtualisation rend la stratégie de positionnement des sondes plus délicate à établir. La Cloud Security Alliance (CSA) a décrit plusieurs niveaux de déploiement possibles de sondes IDS/IPS dans le cloud :

1. Virtuel interne : la sonde est déployée sur un équipement virtuel qui relie les commutateurs virtuels par un pont et est reliée à une interface réseau physique de l'hôte.

Niveaux de déploiement des sondes dans le cloud

2. Physique externe : la sonde est déployée sur un équipement physique dédié relié à l'hôte physique qui redirige le trafic depuis ses commutateurs virtuels grâce à la mise en miroir du trafic ou port mirroring an anglais, ou transmet directement le trafic à la sonde qui l'intercepte.

Mécanismes de sécurité réseau dans le cloud

Niveaux de déploiement des sondes dans le cloud

3. **VMM** : la sonde est déployée au sein du gestionnaire de machines virtuelles en utilisant les APIs offertes.
4. **Systeme invité** : la sonde est déployée au sein du système d'exploitation des machines virtuelles.
5. **Applicatif** : la sonde est déployée au sein même du code de l'application surveillée.
6. **Hybride** : la sonde est déployée au sein du VMM pour intercepter le trafic et l'envoyer vers une sonde virtuelle interne ou physique externe.

Authentification et identification

L'authentification consiste à s'assurer qu'une entité (personnes, périphériques) est bien celle dont nous parlons et que nous définissons comme telle

- De manière générale, des serveurs authentifient les entités pour leur accorder des autorisations (liste de contrôles d'accès) et offre ainsi une certaine forme d'imputabilité (journaux d'évènements). Ce type de service est communément appelé « AAA » c'est-à-dire Authentication, Authorization f§ Accounting.

Les serveurs authentifient les entités en se fondant sur trois types de facteurs d'authentification élémentaires :


1. Ce qu'est cette entité : une empreinte biométrique, un numéro identifiant unique, etc.;
2. Ce que possède cette entité : une clé, un badge, une puce RFID, etc.;
3. Ce que connaît cette entité : un mot de passe, NIP UQAM, etc.




L'authentification forte reconnaît une entité par l'utilisation d'au moins deux des facteurs cités précédemment (au-delà, l'utilisateur se heurte à la frontière utilisabilité versus sécurité).

Au dire des usagers, un mot de passe est contraignant pour plusieurs raisons.

Microsoft offre un système d'exploitation Windows Server qui propose notamment la mise en place de GPO (Global Policies Object) via un Active Directory :1. Ces stratégies conduisent à la création d'une politique de gestion vis-à-vis des ordinateurs et des utilisateurs. Tous les quarante jours une modification du mot de passe est nécessaire ainsi qu'une utilisation de mots de passe forts.



L'utilisateur doit retenir un nouveau mot de passe à chaque renouvellement de période; par expérience, il fera confiance à son post-it qui ne colle plus ou son papier brouillon qu'il ne retrouve plus. Par ailleurs, de nouveaux mots de passe à mémoriser affluent dans les services d'une entreprise ou sur les sites internet. Ces derniers suggèrent l'authentification unique pour la connexion (par ex. se connecter avec Google, se connecter avec Twitter, etc.). La mémoire de l'utilisateur n'est pas mise à rude épreuve puisqu'elle n'a qu'un seul mot de passe à retenir. Cependant, la sécurité des informations confiées par chaque individu sur ces différents sites et services n'est assurée que par un unique mot de passe (celui du compte Twitter ou Google). Une personne mal intentionnée mais habile peut s'emparer de ce mot de passe et accéder aux sites et services associés à ce compte.



Afin d'éviter toute confusion, nous sommes amenés à bien mesurer la différence entre une authentification et une identification. Cette dernière, comme son nom l'indique, identifie une entité, l'authentification suit le même cheminement en incluant des mécanismes supplémentaires de garantie. Ce rôle peut être assumé par un certificat électronique, qui a pour rôle d'identifier un objet (personne, périphérique). Il représente une carte d'identité numérique, contenant une clé publique, une signature et des informations d'identification sur l'objet en question

La confidentialité des données offre la garantie qu'aucune information dite sensible ne peut être divulguée à autrui, à un service ou un matériel non autorisé. Dans un contexte d'informatique décentralisé, les enjeux de la confidentialité sont bien plus importants puisque le datacenter qui héberge les données n'appartient pas nécessairement à l'entreprise cliente. Celle-ci doit pouvoir certifier que le cloud provider fait appel aux mécanismes d'authentification et d'autorisation adéquats car ces deux facteurs représentent l'assurance d'un certain degré de confidentialité. La pratique de la cryptographie offre des solutions pour assurer une bonne confidentialité des données. Étudions les deux grandes approches cryptographiques.



La première, nommée **chiffrement**

symétrique, consiste à crypter une donnée à l'aide d'un algorithme de **chiffrement** {par bloc ou par flux) et d'une clé. Le message crypté peut être recouvert par

l'utilisation d'un algorithme de déchiffrage et de la même clé. La seconde approche, nommée **chiffrement asymétrique**,

prévoit deux clés : l'une publique, l'autre privée. Le sujet A qui envisage d'envoyer un message

crypté au sujet B, doit au préalable obtenir la clé publique de B

1

pour crypter le message. Le

sujet B reçoit le cryptogramme et le déchiffre au moyen de sa clé privée.



Le chiffrement des données présente des inconvénients pratiques : nous serions amenés à gérer autant de clés que de fichiers ou de hiérarchies de fichiers existants. Par ailleurs, la puissance computationnelle requise pour de tels chiffrements est considérable et le management de données cryptées bien plus complexe que le management de données en clair : il est nécessaire de gérer et d'utiliser ces clés en suivant de bonnes pratiques de sécurité .



Un cloud provider qui reçoit l'approbation d'une entreprise pour héberger cette clé, peut déchiffrer le contenu des données puisqu'il détient un accès physique aux salles hébergeant les serveurs. De plus, la divulgation d'informations dans un contexte de saisie juridique

~ légal », offrirait à un gouvernement l'accès aux données en clair (via cette clé). La véracité de nos propos se confirme suite à la parution d'un article publié

par le quotidien Lemonde.fr qui soutient que le FBI et la NSA auraient accès aux serveurs de Google, Facebook, Microsoft, Yahoo !, etc. 6 .



L'intervention du Président

Obama à ce sujet est surprenante, il affirme

~

que le monitoring ne concerne pas les

citoyens américains ». Logiquement, ces accès se rapporteraient au reste de la planète,

et dans le cheminement de notre logique, puisque les entreprises étrangères

(dans le sens où elles ne sont pas implantées sur le sol US) externalisent leurs

données économiques dans les datacenters US, le gouvernement des États-Unis

d'Amérique s'arroge un droit d'accès aux données du reste du monde!



Un client qui possède la clé, doit pour la protéger, se doter d'une infrastructure informatique adaptée; la conception du cloud pourtant n'abonde pas dans ce sens puisqu'elle préconise le déport de l'infrastructure informatique dans le nuage (donc transitivement, des données).

5. Voir: Elaine Barker

Les différents moyens d'encryption, qu'ils soient commerciaux, open-source ou intégrés, augmentent le niveau de complexité puisque la gestion des divers systèmes de cryptographie nécessite une bonne cohésion. TI est donc primordial d'assurer le stockage et l'accès aux données sur le long terme car par un effet boomerang une clé perdue ou corrompue conduit à la perte de toutes les données.



Le chiffrement des données présente un réel intérêt dans le cadre de leur transfert (de bout en bout), le déport s'effectue du client vers le datacenter et vice-versa. Par la création d'un tunnel virtuel privé (VPN) entre les deux protagonistes, la protection des informations est garantie. La suite de protocoles IPSec par exemple autorise la création d'un tunnel sécurisé qui atteste l'intégrité, la confidentialité et l'authentification des données.

Considérations légales

Localisation des données et lois

Connaître la localisation des données confiées est un droit légitime pour tout utilisateur d'un service informatique en nuage. Les sièges sociaux des plus grands acteurs du cloud (par ex. Amazon, Google, Salesforce, Microsoft, etc.) se situent aux USA. Les centres de données de ces différents protagonistes sont implantés aux USA, en Europe et au Canada. Chaque pays possède sa propre législation en matière de données ; les entreprises doivent se soumettre aux lois de l'état dans lequel leurs données résident. Le seul fait qu'un utilisateur ne sache pas systématiquement où se trouvent ses informations (dans un modèle de type cloud public ou cloud privé externe) constitue une atteinte à la confidentialité. Nous présentons ci-dessous quelques lois importantes en vigueur aux USA et nous poursuivrons par les directives européennes.







