Partie 4 : lien vers la présentation

https://drive.google.com/file/d/1t6Y9T1AlhIcs4blhMwNQKQ6M0NOAkiQb/view?usp=sharing

Partie 4 : Les aspects juridiques, réglementaires et sécurité

- Aspects juridiques et réglementaires
- La sécurité

Aspects réglementaires et juridiques

- L'abstraction sur la localisation des données proposée par les solutions de cloud public peuvent poser des problèmes juridiques et réglementaires

- Exemples :
  - Dans le cas de l'offre de premier niveau de Google Workspace, le contrat est signé avec une société de droit américain dont le bureau européen est en Irlande, sans savoir où seront stockées les données.

  - Avec les principaux fournisseurs cloud, il est possible de choisir la localisation du datacenter.
    C'est une bonne chose mais …

Aspects réglementaires et juridiques

- Patriot Act : Loi votée par les Etats-Unis à la suite des attentats du 11 septembre 2001, permettant à l'Administration américaine de demander l'ouverture de ses bases de données à toute société ayant son siège aux Etats-Unis, ceci sans en informer le client final.

- Le CLOUD Act (Clarifying Lawful Overseas Use of Data Act)
  - adopté en mars 2018
  - permet aux administrations des États-Unis, disposant d'un mandat et de l'autorisation d'un juge, d'accéder aux données hébergées dans les serveurs informatiques situés dans d'autres pays, au nom de la protection de la sécurité publique aux États-Unis et de la lutte contre les infractions les plus graves dont les crimes et le terrorisme
  - entre en conflit avec le règlement général sur la protection des données (RGPD)

Aspects réglementaires et juridiques

- Quelques résistances au CLOUD Act : Microsoft, Apple avec des refus de donner certains accès à des données personnelles

- Quelques problèmes en Europe révélés par les médias :
  - les données de santé françaises sont hébergées par Microsoft (le gouvernement français envisage de les rapatrier vers un opérateur de services français ou européen)
  - hébergement, sur les serveurs d'AWS, des attestations des prêts garantis par l'État (PGE) aux entreprises pendant la pandémie Covid-19

Aspects réglementaires et juridiques

Tentatives pour créer des clouds "souverains" nationaux ou européens :

- programme européen GAIA-X
  22 entreprises françaises ou allemandes sont membres fondateurs.
  En France : Amadeus, Atos, EDF, Outscale, OVHCloud , Scaleway, Orange, Institut Mines-Télécom, Safran, CISPE (Cloud Infrastructure Services Providers in Europe), Docaposte
  En allemagne : SAP, Siemens, Beckhoff, Bosch, BMW , DE-CIX, Deutsche Telekom, Fraunhofer, German Edge Cloud, IDSA (International Data Spaces Association), PlusServer

- label SecNumcloud : apporte l'assurance aux clients des services cloud certifiés de choisir des solutions dont le niveau de sécurité et de confiance a été vérifié par l'ANSSI (Agence nationale de la sécurité des systèmes d'information).
  Ce label garantit le recours à des solutions, recommandées par l'État français et particulièrement adaptées pour l'administration française et pour les entreprises nationales des secteurs les plus sensibles.

Aspects réglementaires et juridiques

Pour contrer les "initiatives d'indépendance européenne", les géants américains lancent des projets de cloud européen:

- AWS : European Sovereign Cloud
  https://www.lemagit.fr/actualites/366557113/European-Sovereign-Cloud-AWS-lance-lui-aussi-son-cloud-a-leuropeenne

- Microsoft Azure : Cloud for Sovereignty
  https://www.lemagit.fr/actualites/252523002/Microsoft-lance-le-nebuleux-Cloud-for-Sovereignty

- Google Cloud (Sovereign Controls, Supervised Control et Hosted Control)

Aspects réglementaires et juridiques

Quelques normes :

- ISO 27001 : norme reconnue à l'échelle internationale pour l'établissement et la certification d'un système de management de la sécurité de l'information (SMSI).
- ISO 27017 : norme de sécurité développée pour les fournisseurs de services cloud et les utilisateurs afin de créer un environnement cloud plus sûr et de réduire le risque de problèmes de sécurité.
- ISO 27018 : norme qui concerne la protection des données à caractère personnel dans les services cloud.
- RGPD : Règlement Général sur la Protection des Données

Aspects réglementaires et juridiques

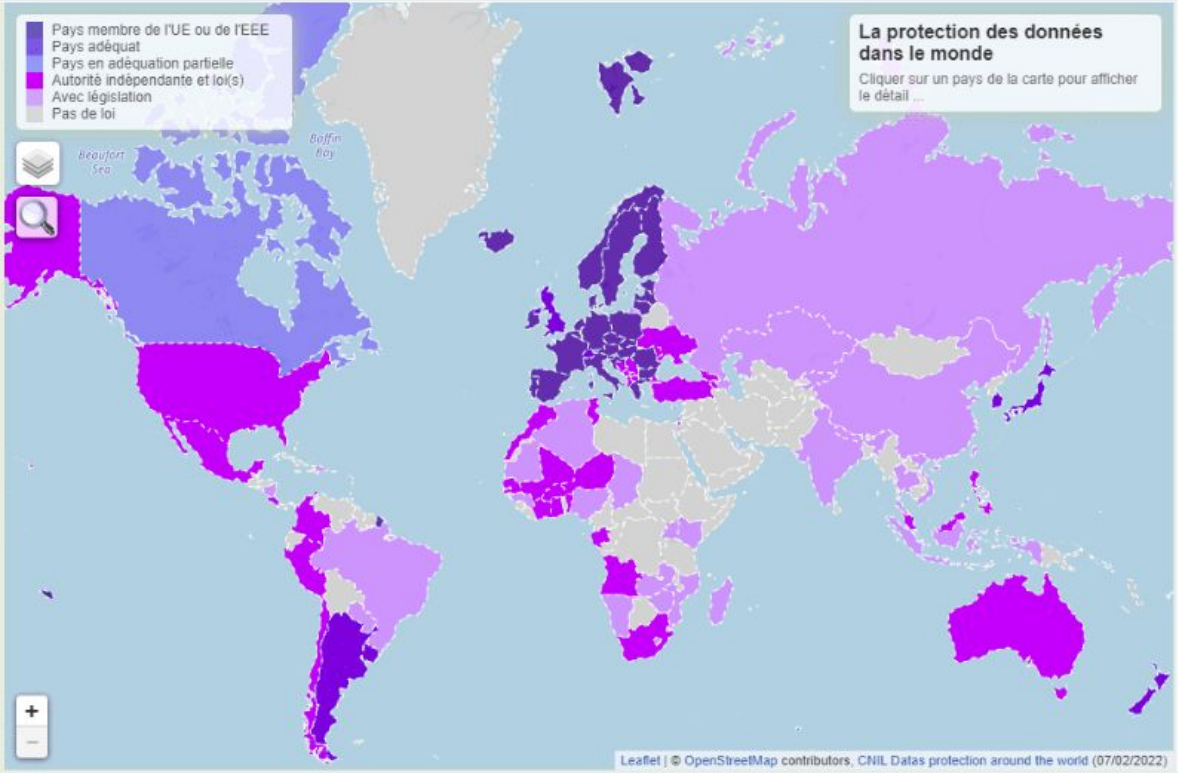
- Rapports SOC (American Institute of Certified Public Accountants - AICPA) :
  - SOC 1 : rapport de contrôle pour les organisations proposant des services et porte sur le contrôle interne des rapports financiers.
  - SOC 2 : rapport qui évalue les systèmes d'information en termes de sécurité, de disponibilité, d'intégrité des traitements et de confidentialité.
  - SOC 3 : rapport général et ne fournit pas d'informations détaillées comme le SOC 1 et le SOC 2. Le rapport SOC 3 est principalement utilisé comme matériel marketing.
- SAS 70 s'applique à toutes les entreprises qui offrent des prestations susceptibles d'affecter la situation financière de leurs clients

Aspects réglementaires et juridiques : focus sur RGPD

- RGPD : Règlement Général sur la Protection des Données
- mai 2018

- Les obligations principales :
  - Recueillir un consentement explicite sur la collecte des données personnelles
  - "Privacy By Design" : ne pas collecter de données sans qu'elles soient nécessaires au service rendu à l'utilisateur
  - Limitation des finalités : en communiquant sur l'usage des données et leur délai de stockage
  - Droit à l'effacement des données sur demande de l'utilisateur
  - Droit à la portabilité (réversibilité) des données sur demande de l'utilisateur
  - Droit au refus du profilage automatique
  - Notification en cas de fuite des données sous 72 heures

Aspects réglementaires et juridiques : focus sur RGPD



Aspects réglementaires et juridiques : focus sur RGPD

Exemples de sanctions pour non-conformités :

- Optical Center : 250.000 € pour ne pas avoir suffisamment sécurisé les données de commandes des clients.
- RATP : 400.000 euros. Plusieurs centres de bus avaient intégré le nombre de jours de grève des agents dans des fichiers d'évaluation qui servaient à préparer les choix de promotion ainsi qu'une durée de conservation excessive des données et des manquements relatifs à la sécurité des données.
- Monsanto : 400.000 euros pour fichage illégal de plus de 200 personnalités et journalistes à des fins de lobbying sur le renouvellement du glyphosate.
- Brico Privé : 500.000 euros pour conservation des données au-delà de ce qui était indiqué dans son registre des traitements (clients n'ayant pas passé commande depuis 5 ans ou personnes ne s'étant pas connectés à leur compte depuis 5 ans), des demandes d'effacement non traitées, absence de demande de mot de passe robuste lors de la création du compte pour les clients ou les salariés, ou encore dépôt des cookies avant le consentement de l'internaute et des messages de prospection, non consentis.

Aspects réglementaires et juridiques : focus sur RGPD

Exemples de sanctions pour non-conformités (suite) :

- AG2R La Mondiale : 1,75 million d'euros, du fait de conservation de données (dont bancaires et santé) au-delà de la limite et un défaut d'information pour les personnes démarchées.
- Google et sa filiale Google Ireland : après 50 Millions en 2019 pour manque de transparence, 150 Millions d'euros concernant les sites web google.fr et youtube.com car la commission a estimé qu'il n'était pas aussi simple de refuser les cookies que de les accepter
- idem pour Facebook Ireland : 60 Millions d'euros, même motif
- Le ministère de l'Intérieur s'est vu infliger deux rappels à la loi, l'un sur les drones de surveillance et l'autre sur le fichier des empreintes digitales :
    - interdiction d'utiliser des drones équipés de caméras pour surveiller le respect des mesures de confinement
    - mauvaise gestion du fichier d'empreintes digitales

Exemple de danger de non-conformité au RGPD

- Cas d'une application de jeu-concours
- Collecte de données personnelles : nom, prénom, numéro de téléphone, email des participants
- Hypothèse : transfert des données à un prestataire chargé d'effectuer le tirage au sort par l'envoi d'un fichier par mail
- Problème : les données risquent de transiter par des serveurs situées hors zone RGPD
- Solution : proposer un espace sécurisé avec une mise à disposition des données

La sécurité

Eléments de l'analyse de risque lié à la sécurité

- authentification des utilisateurs
- confidentialités des données : stockées ou en transit sur le réseau
- intégrité des données : stockées ou en transit sur le réseau
- disponibilité
- traçabilité

La sécurité : cloud et authentification

- Politique d'authentification par défaut : authentification classique par identifiant et mot de passe.
  Pose un problème de sécurité pour le compte Administrateur

- Authentification renforcée, multi facteurs
  Repose sur une combinaison de deux éléments parmi les 3 possibles :
  - la connaissance du mot de passe
  - la reconnaissance biométrique
  - la possession d'un objet d'authentification

  Le plus souvent : mot de passe + objet qui peut être
  - une clef U2F (Universal Second Factor) à connecter en USB ou NFC à son terminal
  - une application sur smartphone qui génère toutes les 30 secondes un code à durée de vie courte. (ex : Google Authenticator)
  - un code envoyé par sms

La sécurité : cloud et authentification

- Fédération d'identité : délégation de l'authentification auprès de l'annuaire de l'entreprise.
  L'utilisateur est redirigé vers le système d'information d'entreprise lors de la phase d'authentification et retourne vers la plateforme cloud une fois authentifié.

La sécurité : cloud et confidentialité

- Confidentialité : certitude qu'une donnée n'a pas été lue par une personne non habilitée.
- La confidentialité des données hébergées chez l'opérateur cloud est un engagement contractuel :
  - contrat entre l'entreprise utilisatrice et l'opérateur
  - certifications obtenues par l'opérateur
- Pour rassurer leurs clients, les opérateurs proposent le principe de "Bring your own key" : la clef de déchiffrement des données reste stockée dans l'entreprise et non dans le cloud.
- Confidentialité des données en transit sur le réseau
  - protocole SSL
  - protocole IPSEC
  - lien dédié entre le datacenter et le SI

La sécurité : cloud et confidentialité

- Gestion classique des accès dans un SI : les cas à prendre en compte :
  - utilisateurs qui accèdent aux applications depuis le siège de l'entreprise
  - utilisateurs qui accèdent aux applications depuis un site secondaire
  - utilisateurs qui accèdent aux applications en situation de nomadisme

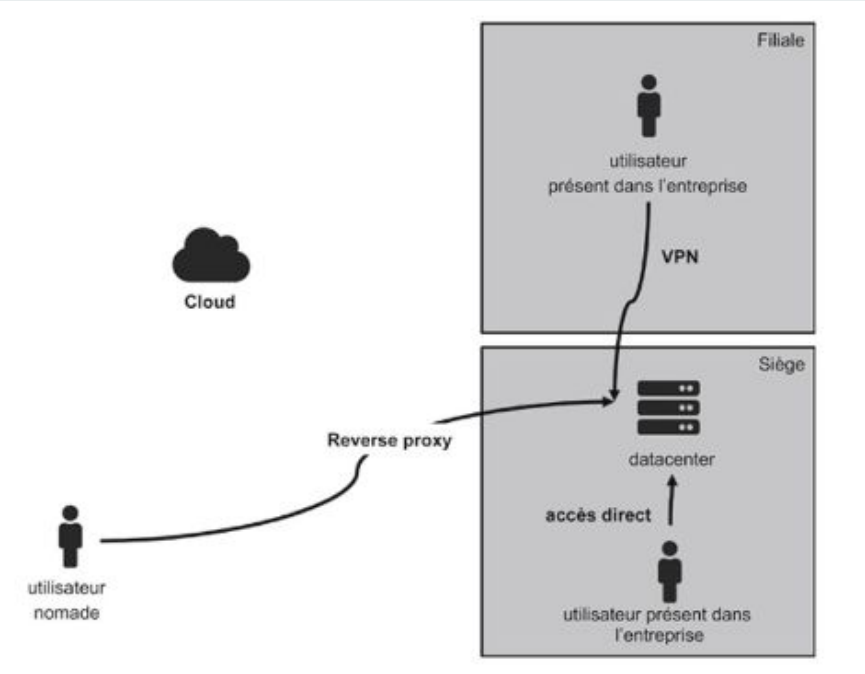
  Implique plusieurs solutions à mettre en place par les administrateurs réseau :
  - accès direct pour les utilisateurs du siège
  - VPN (Virtual Private Network) pour les utilisateurs du site distant
  - Reverse Proxy pour les nomades

  Cette complexité entraîne des coûts et potentiellement des failles de sécurité.

- Nouveau modèle de sécurité : "Zéro Trust" : ce modèle considère que tous les utilisateurs représentent le même danger pour les serveurs à cause de leur infection potentielle par des virus ou des chevaux de Troie

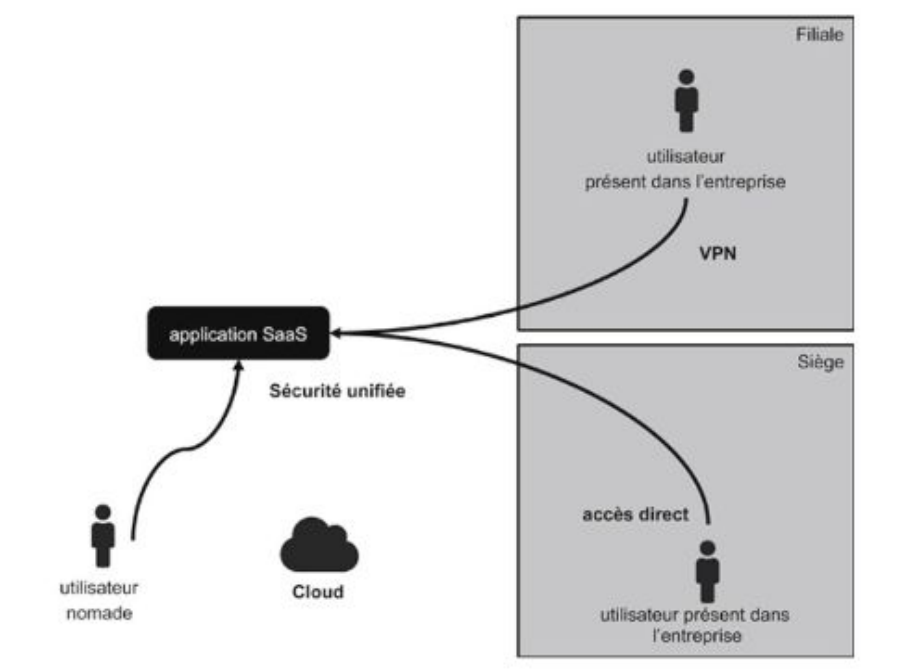
La sécurité : cloud et confidentialité

- Gestion classique des accès dans un SI



La sécurité : cloud et confidentialité

- Gestion simplifiée



La sécurité : cloud et intégrité

- intégrité : certitude qu'une donnée n'a pas été altérée de manière accidentelle ou malintentionnée.

- Plusieurs mesures pour garantir l'intégrité :
  - gestion des accès
  - gestion de la confidentialité
  - sauvegarde et réplication des données

- les opérateurs cloud donne un indice de durabilité
  ex : AWS S3 : 99,999999999 % (11 9).
  Ce niveau de durabilité correspond à une perte moyenne annuelle prévue de 0,000000001 % des objets.
  Par exemple, si vous stockez 10 000 000 d'objets avec Amazon S3, vous pouvez vous attendre à perdre en moyenne un objet unique une fois tous les 10 000 ans.

La sécurité : cloud et disponibilité

- La gestion de haute disponibilité est intégrée nativement dans les architectures mise en place chez les opérateurs cloud.

- différentes offres donnent accès au niveau de disponibilité (exprimé en % : 99,9 %, 99,99 %) requis par l'entreprise utilisatrice.

La sécurité : cloud et traçabilité

- La traçabilité porte sur la gestion des traces (logs) permettant de suivre le comportement des applications en production.
  Elles permettent de comprendre le comportement des utilisateurs et d'optimiser le fonctionnement des applications.

- La gestion de la traçabilité revient plutôt aux équipes de l'entreprise utilisatrice qu'à l'opérateur de cloud.

La sécurité : synthèse des problématiques

Problématiques de sécurité	Réponses des SaaS
Authentification	Possibilité de gérer une politique de mot de passe, une authentification renforcée et de déléguer l'authentification chez certains opérateurs.
Confidentialité	Pas de vrai risque technique. Décision à prendre selon la politique de sécurité et les problèmes juridiques (NSA).
Intégrité	Pas de vrai risque technique. Garantie d'intégrité souvent supérieure à celle du SI.
Traçabilité	Peu de choses disponibles avec SaaS/PaaS. Idem SI pour IaaS.
Disponibilité	Pas de vrai risque technique. Garantie de SLA souvent supérieure à celle du SI.

Gestion du risque de sécurité

Pour une PME :

- Les dirigeants de PME sont souvent ouverts à l'usage du cloud car ils sont intéressés par les garanties sur l'intégrité des données offertes par ce modèle.
- Les moyens en interne ne sont pas suffisants pour atteindre ces garanties.

L'usage du cloud pour une PME est donc un compromis entre des bénéfices d'intégrité et des risques de confidentialité.

Gestion du risque de sécurité

Pour une grande entreprise :

Plusieurs types de risques :

- risque de vol de secret industriel : ce risque existe dans les secteurs très concurrentiels, par exemple, ceux où le dépôt de brevet est critique pour s'assurer de nouveaux marchés.
- risque de vol de données confidentielles sur ses clients : ce risque existe dans des secteurs comme celui de la banque, où la protection des données est critique.
- risque de vol de données de fonctionnement interne : ce risque porte essentiellement sur l'image d'une entreprise connue. Si le public apprenait qu'on lui a volé des données, son image serait salie.

Ces risques sont gérés par la politique de sécurité de l'entreprise, en général, définie et mise en œuvre par le RSSI (Responsable de la Sécurité du Système d'Information).

Gestion du risque de sécurité

Pour une grande entreprise : impacts sur la politique de sécurité si l'entreprise souhaite utiliser les services d'un opérateur cloud

- une mention sur la possibilité d'externaliser vers le cloud au sein de la classification des données
- des règles sur les niveaux d'authentification que doivent offrir les plateformes cloud
- des règles sur les niveaux de sécurisation des flux SI / cloud
- des règles sur la réplication et la sauvegarde des données
- des règles sur le chiffrement des données persistant sur les plateformes cloud
- des règles sur la gestion des traces et logs
- des règles sur les SLA

Gestion du risque de sécurité

Exemple d'analyse de risques :

Type de donnée	Secret industriel	Données confidentielles clients	Données de fonctionnement interne
Classification	Stratégique	Critique	Confidentiel
Risque si externalisation	Très important	Important	Modéré
Externalisation	Impossible	Souvent impossible	Possible

Quelques statistiques "cloud et sécurité"

- Les entreprises considèrent la sécurité du cloud comme leur principale préoccupation

  "Il n'est pas surprenant que 75 % des entreprises considèrent les problèmes de sécurité du cloud comme une préoccupation majeure.
  Parmi celles-ci, 33 % des personnes interrogées sont extrêmement préoccupées, 42 % sont très préoccupées, tandis que seulement 25 % au total sont peu ou moyennement préoccupées."

- Quelles sont les principales préoccupations en matière de sécurité du cloud ?

  "Selon les experts en cybersécurité, les défis les plus pressants en matière de sécurité du cloud sont la mauvaise configuration de l'infrastructure du cloud (68 %), les accès non autorisés (58 %), les API non sécurisées (52 %), le détournement de comptes, de services ou de trafic (50 %) et le partage de données externes (43 %)."

Quelques statistiques "cloud et sécurité"

- Les clouds intrinsèquement sûrs sont une priorité pour les entreprises

  "Étant donné que la sécurité du cloud est si recherchée, il n'est pas étonnant que les entreprises recherchent des services de cloud qui soient sécurisés dès le départ. En fait, un peu plus de la moitié des entreprises (52 %) préfèrent les solutions de cloud computing qui disposent de leurs propres outils de sécurité natifs"

- L'erreur humaine est à l'origine de la majorité des violations de données dans le cloud

  "Dans 88 % des cas, c'est l'erreur humaine qui est à l'origine des violations du cloud, et non les fournisseurs de cloud.
  Avec 34 %, les hommes sont deux fois plus susceptibles de tomber dans le piège du phishing que les femmes (17 %)."

Quelques statistiques "cloud et sécurité"

- La moitié des organisations stockent leurs données confidentielles sur des technologies en cloud

  "Les entreprises semblent accorder une grande confiance à l'informatique en cloud dans l'ensemble, 48 % d'entre elles choisissant de stocker leurs données confidentielles et les plus importantes sur le cloud, qu'il s'agisse de données cryptées ou "normales""

- La plupart des organisations ont mis en place une stratégie multi-cloud

  "Une stratégie multi-cloud consiste à utiliser plusieurs fournisseurs de services en cloud tels que Google Cloud ou AWS. Ainsi, si l'un des services est indisponible pour une raison quelconque, l'entreprise peut basculer sur une sauvegarde fonctionnelle pour la reprise après sinistre. Pour cette raison, 92 % des entreprises ont déjà une stratégie multi-cloud. "

Quiz 8

https://docs.google.com/forms/d/e/1FAIpQLSdH6afmugOBsk448CrBp-m5PIttINMoKAdOMSBv3dkKIfbXUA/viewform?usp=dialog