POINTS DE VIGILANCE SUR LES CONTRATS DE PRESTATIONS CLOUD SOUS L'ANGLE CYBER

11 MARS 2025

alerion AVOCATS

OSSIR

Intervenant

Corinne THIERACHE, Avocate Associée, Cabinet ALERION

- **Responsable des Départements IP/IT/Protection des données Personnelles (Innovation)**
- **Membre de Cyberlex (Président, Vice-Président et membre du conseil d'administration de 2005 - 2017)**
- **Membre du CyAn (CyberSecurity Advisors Network)**
- **Membre de SecureSphere by EPITA**
- **Membre de l'AILCC (Association Internationale de lutte contre la cybercriminalité)**
- **Membre du Geste (Groupement des éditeurs de contenus et de services en ligne), coresponsable de la commission « Enjeux réglementaires » et préside et anime le Groupe des DPO des membres du Geste**
- **Membre de l'AFCDP (Association Française des Correspondants à la protection des Données à caractère Personnel)**
- **Expert auprès du Conseil de l'Europe et de la Commission Européenne (lutte contre la cybercriminalité)**
- **Membre du Comité d'éthique de vidéoprotection de la ville de Paris depuis 2017 et du Comité d'évaluation de l'expérimentation de traitements algorithmiques d'images légalement collectées au moyen de systèmes de vidéoprotection en 2024**

alerion
AVOCATS

Introduction

- **Contextualisation** : le cloud computing permet de mettre à la disposition du client des services, des plateformes ou des logiciels en ligne sans qu'il ait besoin de le télécharger ou de l'installer sur ses propres serveurs (≠modèles *on-premise*)
- **Avantages** :
  - Plus facile à installer et mettre à jour
  - Moins coûteux (achat des serveurs, sauvegarde)
  - Multiples accès à distance grâce à internet à haut débit
- **Inconvénients** :
  - Risques cyber
  - Dépendance des clients par rapport à leurs prestataires
- **Clauses classiques à prendre en compte comme pour tous contrats :**
  - Loi applicable & juridiction compétente
  - Propriété intellectuelle
  - Mais pas que… avec une acuité plus grande pour la confidentialité et le partage des responsabilités (gestion des données et des identités)

© Dessin de Fix C.

Plan

➢ I. Identification des risques cyber en présence

➢ Risques cyber liés à une défaillance technique

L'exemple de Microsoft (panne liée au logiciel de cybersécurité Falcon)

➢ Risques cyber liés à des cyberattaques

➢ A. Risque augmenté à cause de l'IA

➢ B. Multiplication des vulnérabilités *Supply Chain Attacks*

➢II. Mitigation des risques cyber à prendre en compte dans les contrats Cloud

➢ A. Solutions contractuelles

1. Clauses relatives à la sécurité des données
2. Sous-traitance et accord de traitement des données (*Data Processing Agreement – DPA*)
3. Clause d'audit et de contrôle
4. Clause de niveau de service (*Service Level Agreement – SLA*)
5. Réversibilité et portabilité
6. Interopérabilité
7. Clause de responsabilité (obligations de moyen et de résultat)

➢ B. Solutions techniques

1. Différents niveaux de sécurité à mettre en place
2. Blockchain

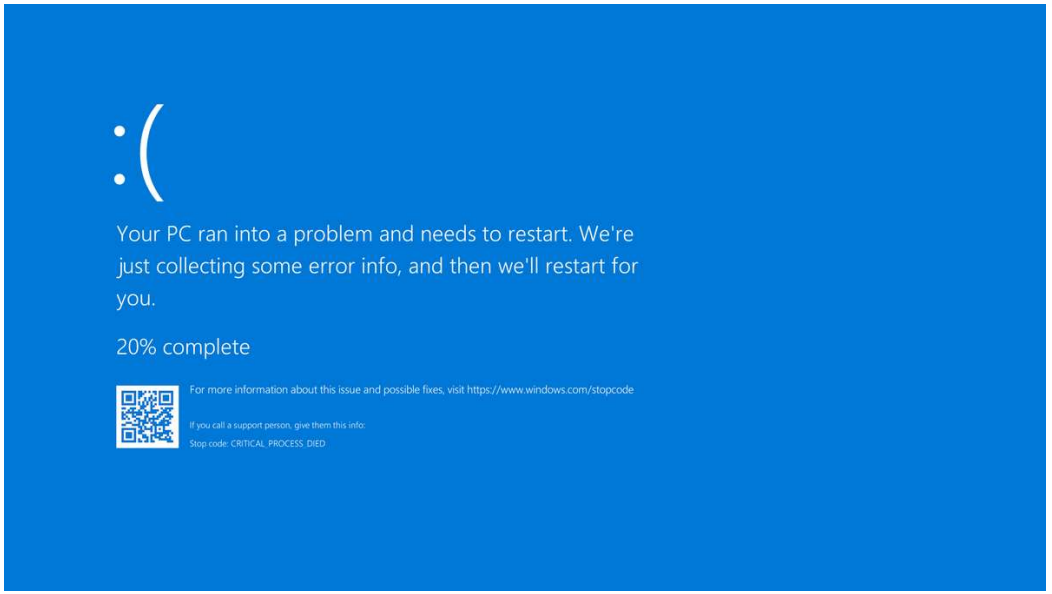
alerion
AVOCATS

I. Identification des risques cyber en présence

Risques cyber liés à une défaillance technique

- **Incident du 19 juillet 2024 - Panne de Falcon de Crowdstrike :**

- Le 19 juillet 2024, une panne liée au logiciel de cybersécurité Falcon a empêché le démarrage de Windows sur de nombreux ordinateurs. Falcon, un outil EDR (Endpoint Detection and Response), surveille les systèmes en temps réel pour prévenir les pannes et cyberattaques.
- Le bug, causé par une mise à jour, a affecté des centaines d'entreprises, y compris des **aéroports, hôpitaux, compagnies aériennes, chaînes de télévision ainsi que la Bourse de Londres**. Bien que cet incident n'ait pas été une cyberattaque, il a révélé la vulnérabilité des systèmes numériques mondiaux.
- Selon Chris Beauchamp, chef analyste marchés du courtier IG « *l'incident a mis en évidence l'interconnexion de l'infrastructure numérique mondiale et les conséquences considérables des défaillances techniques* »



Risques cyber liés à des cyberattaques

A. Risque augmenté à cause de l'IA

- Usage de plus en plus important de l'intelligence artificielle pour les cyberattaques : identification des vulnérabilités, déploiement des campagnes d'attaque, établissement de portes dérobées dans le SI, exfiltration ou altération des données, interférence avec les opérations du système

- **Points communs des cyberattaques aidées de l'IA :**

- **Automatisation des attaques**
- **Collecte efficace des données**
- **Personnalisation des attaques**
- **Apprentissage par renforcement**
- **Ciblage des employés**

alerion
AVOCATS

B. Multiplication des vulnérabilités dans le cloud avec les Supply Chain Attacks

- **Développement des Supply Chain Attacks :** Attaque indirecte via la chaîne logistique, ciblant un prestataire Cloud plutôt que directement l'entreprise visée.
- **Méthode** : L'attaquant pénètre dans le SI d'un fournisseur (souvent dans le Cloud) pour atteindre plusieurs clients sans effort supplémentaire.
- **Secteurs ciblés** : Principalement les fournisseurs de logiciels et fabricants de matériel technologique.
- **Objectifs** :
  - Injecter du code malveillant via des pratiques non sécurisées dans la chaîne de développement.
  - Exploiter des produits utilisés par de nombreuses entreprises pour exfiltrer des données sans détection.
- **Risques** :
  - L'attaque peut toucher en une seule attaque des milliers de clients, incluant des entreprises technologiques, gouvernements, et prestataires de services de sécurité.

alerion
AVOCATS

II. Mitigation des risques cyber à prendre en compte dans les contrats Cloud

A. Solutions contractuelles

1. Clauses relatives à la sécurité des données

a. Clause de sécurité en lien en annexe avec un Plan d'assurance sécurité

- Document technique et juridique expliquant comment le prestataire de service respecte les exigences de cybersécurité au sein du SI du client (mesures techniques et organisationnelles pour la sécurité physique et logique + l'intégrité des données) dont risque de perte, de fuite, de corruption ou détournement de finalité
- Notification de failles au responsable de traitement avec procédures d'alerte et mesures de lutte contre les intrusions frauduleuses

b. Clause d'hébergement des données

- Exigences de sécurité pour l'hébergeur de données afin de garantir la disponibilité des données et d'assurer la redondance des systèmes et une sauvegarde assez régulière sur plusieurs serveurs

c. Clause de localisation des données

- Localisation géographique des serveurs
- Nécessaire pour s'assurer du traitement des données sur le territoire national, ou au moins dans l'UE ou dans un pays offrant un niveau de protection adéquat (RGPD)
  Quid USA ? résurgence des CCT

d. Clause de confidentialité

- Impose un niveau de confidentialité des données traitées suffisant au prestataire, à ses salariés avec des clauses de porte-fort pour les freelances et autres sous-traitants

e. Gestion des incidents de sécurité (Data Breach Process)

- Dispositif essentiel définissant les procédures d'escalade permettant de réagir à un incident de sécurité ou une menace (plans d'action et remèdes pour limiter les impacts des incidents de sécurité)

alerion AVOCATS

A. Solutions contractuelles

2. Sous-traitance et accord de traitement des données (*Data Processing Agreement – DPA)*

- Le RGPD impose d'annexer un *Data Processing Agreement* (DPA) au contrat Cloud pour définir les rôles et obligations des parties. Ce DPA inclut une clause sur les sous-traitants ultérieurs, permettant au responsable de traitement de contrôler la chaîne de sous-traitance et d'imposer un veto si nécessaire. Il est essentiel de vérifier régulièrement la liste des sous-traitants et de privilégier ceux situés dans l'UE.

3. Clause d'audit et de contrôle

- Une clause d'audit permet de vérifier le respect des obligations contractuelles du prestataire Cloud avec obligation de coopération du prestataire. Bien que coûteux, un audit est crucial si les données ou l'activité confiée sont vitales pour l'entreprise. Il permet aussi de s'assurer de la conformité du prestataire aux **normes de cybersécurité** comme ISO.

4. Clause de niveau de service (*Service Level Agreement – SLA*)

- Un SLA définit les attentes entre un client et son prestataire en précisant les niveaux de service, taux de disponibilité, délais de réponse et critères de performance. Il garantit des engagements de qualité, notamment en matière de disponibilité pour les services Cloud. Un SLA bien rédigé inclut les responsabilités, pénalités et modalités de suivi, assurant une réaction rapide en cas d'incident.

alerion
AVOCATS

A. Solutions contractuelles

5. Clause de réversibilité et de portabilité des données

- Une clause de réversibilité doit prévoir la restitution des données en fin de contrat. Elle définit quelles données sont restituées, sous quel format pour faciliter la restitution, à qui et dans quels délais. Le RGPD impose aussi de garantir une récupération / exportation rapide des données si le prestataire ne respecte plus les exigences de sécurité. Le cas échéant, prévoir un certificat de suppression des données sur les serveurs du prestataire.

6. Importance de l'interopérabilité

- L'interopérabilité est cruciale pour intégrer un nouveau prestataire dans l'écosystème existant. Certains fournisseurs limitent cette compatibilité pour **verrouiller** leurs clients et les rendre dépendants. Cela complique et rend coûteux tout changement de prestataire.

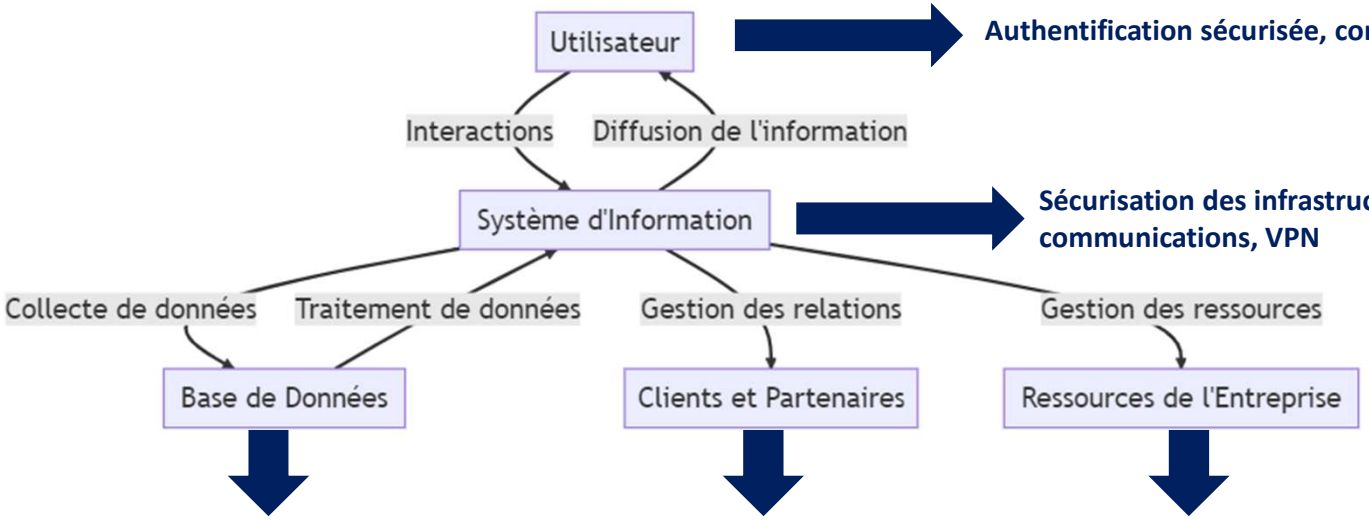
7. Clause de responsabilité (obligations de moyen ou de résultat)

- Une clause de responsabilité encadre les cas d'engagement de responsabilité entre les parties pour en limiter les risques financiers. Elle inclut des limitations pour le prestataire tout en évitant un déséquilibre contractuel, surtout avec des acteurs majeurs (attention aux clauses limitatives de responsabilité qui en réalité privent de sa substance l'obligation du prestataire). Elle doit aussi prévoir des conséquences en cas de violation de cybersécurité, comme des pénalités, un plafond de responsabilité ou une résiliation.

alerion
AVOCATS

B. Solutions techniques

1. Différents niveaux de sécurité à mettre en place



Authentification sécurisée, contrôle des accès, formation et sensibilisation

Sécurisation des infrastructures, pare-feu, chiffrement des communications, VPN

Chiffrement des données
Intégrité des données
Sécurisation des API
Isolation des environnements

Sécurisation des plateformes d'échange
Vérification des partenaires

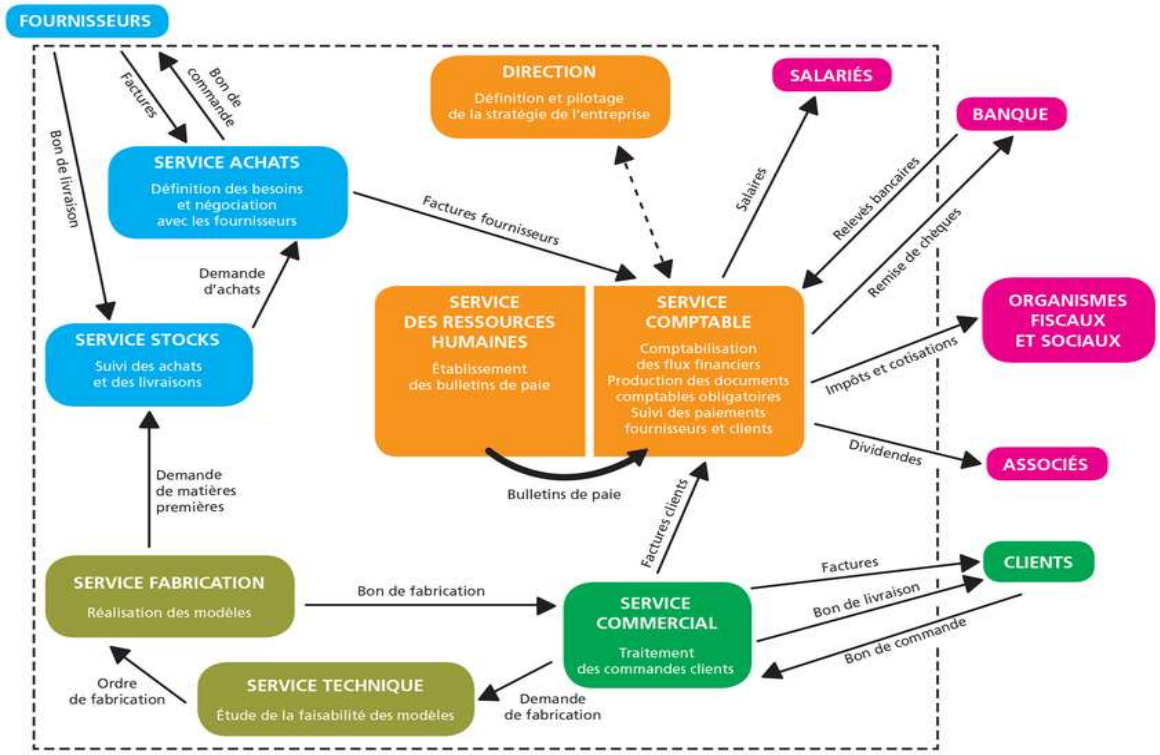
Sécurisation des accès aux ressources (*Identity Access Management)*
Protection physique des infrastructures

Schéma de Foxeet en date du 14 novembre 2023, annoté par nos soins (https://fr.linkedin.com/pulse/comprendre-le-syst%C3%A8me-dinformation-si-d%C3%A9finition-et-exemples-foxeet-h1s6e)

B. Solutions techniques

1. Différents niveaux de sécurité à mettre en place

La réalité des SI est souvent bien plus complexe (hybridation)



alerion
AVOCATS

Schéma du système d'information réalisé par A. Lam (https://www.i-manuel.fr/PRCG_P1CTC/PRCG_P1CTCpart1dos1UD2doc2.htm)

B. Solutions techniques

2. Blockchain

- La **blockchain**, développée en 2008, est une technologie de stockage et de transmission d'informations **décentralisée**, garantissant **sécurité et immutabilité** des données grâce à la cryptographie
- **Avantages pour la cybersécurité Cloud :**
  - **Décentralisation** : Pas de point unique de défaillance, réduisant les attaques ciblées.
  - **Immutabilité** : Données inaltérables, assurant authenticité et traçabilité.
  - **Sécurisation cryptographique** : Protection par hachage et clés publiques/privées.
  - **Transparence** : Auditabilité des transactions et détection rapide des anomalies.
  - **Résistance aux attaques DDoS** : Pas de serveur central à saturer.

- **Limites** : Coût énergétique élevé (Proof of Work) et vulnérabilité de certains nœuds.
- **Conclusion** : Aucun système n'est invulnérable, mais la blockchain renforce la sécurité Cloud face aux cybermenaces.

alerion
AVOCATS

Conclusion

Cybersécurité et Cloud : Un Enjeu Stratégique

- **Cyberattaques en hausse** : Rançongiciels, espionnage, sabotage – la prévention est essentielle.
- **Shadow IT** : Utilisation d'applications non contrôlées = porte d'entrée pour les attaques.
- **Responsabilité des prestataires Cloud** : Possibilité d'indemnisation mais impact immédiat sur la réputation et la gestion de crise → ne pas oublier la responsabilité des clients dans la gestion des données, des comptes et des identités, l'élaboration des plans de continuité (PCA) et de reprise d'activité (PRA) (cf. *Rapport de l'ANSSI « Cloud computing : Etat de la menace informatique », 19 février 2025*)

Souveraineté Numérique & Sécurité

- **Indépendance face aux fournisseurs étrangers** : Protection des données sensibles contre la surveillance et les lois extraterritoriales (ex: Cloud Act).
- **Renforcement des infrastructures critiques** : Cloud souverain, cybersécurité locale et réglementation stricte pour limiter les risques (NIS 2….)
- **Alliances stratégiques & confiance numérique** : Garantir la protection des données et la fiabilité des technologies dans un monde interconnecté.
- **Objectif 2030** : Avec **30 milliards d'objets connectés**, la cybersécurité devient une priorité absolue pour assurer un avenir numérique sûr et résilient en maintenant la confiance dans le numérique.

alerion
AVOCATS

MERCI !

Corinne Thiérache
cthierache@alerionavocats.com
Tél : 01 58 56 97 00

Inès Benhassine
ibenhassine@alerionavocats.com