HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

Club EBIOS, 11 décembre 2012

Contractualiser la sécurité du cloud computing

Frédéric Connes
<Frederic.Connes@hsc.fr>

Plan

- Contrat
- Envoi des données
- Prérogatives du prestataire
- Obligations du client
- Données à caractère personnel
- Obligation de sécurité
- Audits de sécurité
- Confidentialité
- Effacement des données
- Convention de service attendu
- Réversibilité
- Résiliation
- En conclusion

Contrat

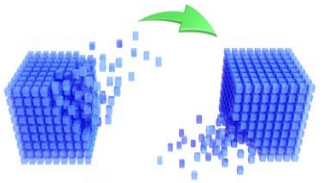
- Normes juridiques : hiérarchie
  - Pas de normes juridiques sur la sécurité du cloud computing
  - Source principale pour le cloud : contrat
- Contrat : en dessous de la hiérarchie des normes
- Code civil, art. 1134
  - Les conventions légalement formées tiennent lieu de loi à ceux qui les ont faites
  - Elles ne peuvent être révoquées que de leur consentement mutuel, ou pour les causes que la loi autorise
  - Elles doivent être exécutées de bonne foi

Contrat

- Obligations réciproques
- En principe résultat d'une négociation
- Code civil, art. 1135
  - Les conventions obligent non seulement à ce qui y est exprimé, mais encore à toutes les suites que l'équité, l'usage ou la loi donnent à l'obligation d'après sa nature
- Code civil, art. 1156
  - On doit dans les conventions rechercher quelle a été la commune intention des parties contractantes, plutôt que de s'arrêter au sens littéral des termes

Envoi des données

- Du client vers le prestataire
- Le prestataire doit garantir la sécurité des données



  - Dès leur acheminement via Internet (canal sécurisé)
  - Dès leur réception dans son système d'information (avant la bascule)
- Moyens techniques
  - A détailler par le prestataire, mais préciser : non limitatifs
  - Exemples : chiffrement, sauvegardes, empreintes, formats de données pour la migration...
- Garantir la continuité avec le système antérieur
  - Responsabilité du prestataire d'être prêt pour éviter toute interruption de service au moment de la bascule

Prérogatives du prestataire

- Intervenir sur les données ou les applications du client
  - En cas d'attaque ou de dysfonctionnement
    - Si le client ne peut pas agir lui-même
      - Urgence : le client ne répond pas
      - Le client n'a pas la compétence technique pour intervenir
  - A l'occasion d'une maintenance
  - A la demande d'un juge

- Selon quelles modalités ?
  - Conditions à remplir pour accéder aux données et applications
  - Indemnisation éventuelle du client en cas de dysfonctionnement consécutif à l'intervention ?

Obligations du client

- Respecter les dispositions légales et réglementaires en vigueur
  - Données personnelles, spam, STAD, ...
  - Propriété intellectuelle, infractions de presse, ...
- Garantir la confidentialité des mots de passe attribués
- Agir promptement en cas de notification de contenus
  - Responsabilité en tant qu'hébergeur si en a la qualité
- Agir promptement en cas d'attaque (intrusion, DoS, ...)
  - Notamment : avertir le prestataire
- Sanctions
  - Suspension, suppression du service, avec ou sans préavis

Données à caractère personnel

- Loi du 6 janvier 1978 « informatique et libertés »
- Qui est responsable de traitement ?
  - CNIL, 25 juin 2012 : le client (le prestataire est sous-traitant)
    - Mais présomption renversable, coresponsabilité possible
  - G29, 1er juillet 2012 : le client est l'unique responsable de traitement
- Déterminer la loi applicable
  - Préciser le lieu d'établissement et la localisation des moyens de traitement
- Prévoir les éventuels transferts de données hors UE
  - Donc : savoir avec précision où vont les données
- Reprendre les obligations du responsable de traitement
  - Formalités préalables, information, droit d'accès, sécurité...

Obligation de sécurité

- Des données personnelles
- A la charge du responsable de traitement
- Obligation de moyens
- Doit être reportée sur le sous-traitant par contrat
- Clauses spécifiques à la sécurité
  - « Mettre tous les moyens en œuvre pour garantir la sécurité »
  - « Apporter tout le soin et la diligence nécessaires à la fourniture d'un service conforme aux usages de la profession et à l'état de l'art »
  - Idéalement, détailler ou renvoyer à une annexe sécurité

Audits de sécurité

- Possibilité pour le client d'en demander
  - Dépend du rapport de force entre le client et le prestataire
  - Risques potentiellement mal évalués si pas d'audit
  - Le prestataire peut convenir de se faire auditer régulièrement à ses frais pour satisfaire tous ses clients
- Périmètre des audits
- Périodicité des audits
- Modalités des audits
  - Techniques
  - Organisationnels
- Processus de certification ?

Confidentialité

- Clause spécifique : possibilité pour le prestataire d'accéder aux données du client
  - Avec ou sans son accord
  - Pratique des clés ssh du prestataire sur les hébergements IaaS
  - Respect du secret professionnel
  - Usage potentiellement fait des données

- Quels contrôles sont réalisés par le prestataire ?
  - Sur l'information des personnels
  - Sur le respect de l'obligation de confidentialité

Effacement des données

- Peut être demandé
  - En cours de contrat
    - A l'expiration d'un délai suivant un événement
    - A tout instant à la demande expresse du client
  - Lors de la résiliation

- Problèmes
  - L'effacement physique est rarement réel et complet
    - Sauf outils spécifiques peu utilisés par les prestataires
  - Il est difficile d'effacer dans
    - Les architectures redondantes (combien de copies ? localisation ?)
    - Les sauvegardes/archives (mutualisées avec d'autres clients ?)
  - Technique des données chiffrées dont on « oublie » la clé

Convention de service attendu

- *Service Level Agreement* (SLA)
- Taux global de disponibilité
  - En comptant les maintenances programmées ?
  - Durée cumulée des indisponibilités
  - Nombre maximum d'indisponibilités
  - Période retenue (jour, semaine, mois, trimestre, année...)
  - GTI, GTR

- Exclusions
  - Force majeure
  - Prévenance
    - Prévoir le délai de prévenance permettant l'exclusion
- Calcul des indemnités et maximum

Réversibilité

- On parle aussi de : portabilité, transférabilité, ...
- Permettre au client de reprendre possession de ses données
  - A tout moment
  - Sans justification

- Délai de prévenance
- Faire des exports réguliers pendant l'exécution du contrat ?
- Formats d'exportation des données : ouverts, standard ?
- Prestataire : « Apporter l'assistance nécessaire pour faciliter le transfert des données et des moyens de sécurité matériels et logiciels vers le client ou tout autre prestataire »
- Finalement, qui est propriétaire des données ?

Résiliation

- Prévoir les motifs
- Manquement grave du prestataire à l'une des obligations de sécurité mises à sa charge par le contrat
  - Disponibilité, confidentialité, intégrité, réversibilité...
  - Liste **non exhaustive** des manquements graves
  - Mise en demeure du client de mettre fin au manquement
    - Prévoir le délai
  - Si le manquement n'est pas réparé dans le délai, le client peut résilier le contrat de plein droit
    - Avec ou sans préavis
  - Prévoir aussi des pénalités

En conclusion

- Le contrat est fondamental pour la sécurité juridique
  - Tant du client que du prestataire
- Ne pas faire confiance aux exemples de clauses que l'on trouve sur Internet
  - Le contrat est nécessairement spécifique
  - Sauf face aux géants qui refusent de négocier
    - « Contrats d'acceptation »

- Réviser périodiquement les clauses sécurité du contrat en fonction
  - De l'évolution de la relation contractuelle et du rapport de force
  - De l'évolution des techniques et de l'état de l'art
  - Des besoins du client et des offres du prestataire

Questions