Telecom Valley / CLUSIR Côte d'Azur

SÉCURITÉ ET CLOUD COMPUTING : OUVREZ VOTRE PARAPLUIE !

02/02/2016

Patrick CHAMBET
RSSI de la Métropole Nice Côte d'Azur / CLUSIR Côte d'Azur / CESIN

Agenda

- Rappels sur le Cloud
- Points juridiques, contrats
- Sécurité réseau / infra
- Authentification, habilitation
- Traçabilité
- Protection des données, chiffrement
- Sécurité applicative
- Recommandations

Un beau nuage... mortel : le « cunimb »

Rappels sur le Cloud

- Le Cloud est-il nécessaire ?
  - Question à se poser à chaque fois, en fonction du service et des données concernées
  - Les données cœur de métier ne sont pas des candidates naturelles pour le Cloud

- Le phénomène du « shadow computing »
  - Hébergement de données ou de ressources dans le Cloud par des Directions métier, sans passer par la DSI (et le RSSI)
    - La nature humaine va vers la facilité ☺
    - Prise de risques par l'entité, sans même le savoir !

Points juridiques, contrats

- Savoir localiser géographiquement ses données
- Pouvoir assurer à ses clients que leurs données sont stockées dans l'UE ou le « G29 » (groupe de l'article 29, pays ayant un équivalent de CNIL)
- Invalidation du mécanisme de « Safe Habor » par la Cour de Justice de l'UE le 06/10/2015
  - Il n'est plus possible de réaliser un transfert de données sur la base du Safe Harbor
  - La CNIL examine actuellement les conséquences juridiques et opérationnelles
- PATRIOT ACT
  - Pour ne pas y être soumis, 3 critères : société européenne, localisée en Europe, avec du personnel européen
- Concurrence économique, voire espionnage
  - Cf un certain Edward Snowden
- Savoir s'assurer de la purge (destruction sécurisée) des données clients, à tous leurs emplacements
- Planifier la récupération d'informations en cas de saisie judiciaire
  - Ex: messagerie hébergée dans le Cloud

Règlement européen sur la protection des données

- Les entreprises seront davantage responsabilisées au travers du principe d' « accountability », imposant de se mettre en conformité et de pouvoir le démontrer
- Selon la nature des données traitées, il conviendra de consulter préalablement l'autorité de protection des données (la CNIL en France) et de mener un DPIA (Data Protection Impact Assessment)
- Mise en œuvre de mécanismes visant à garantir la protection des données par défaut ou dès la conception (notions de Privacy by design et de Privacy by default)
- Un « délégué à la protection des données » devra être désigné dans certains cas
- Les « violations de données à caractère personnel » devront être notifiées à l'autorité de protection des données et selon les cas, aux personnes concernées
- Les sanctions se mesureront en % du CA mondial consolidé
  - Avertissement privé ou public, sanction financière avec un maximum de 1 M€ d'amende ou 4% du chiffre d'affaire mondial consolidé, injonction de cesser le traitement
- Droit à la portabilité, statut du sous-traitant, renforcement du consentement, etc…
- Le règlement est applicable en 2018 (en remplacement de la directive 95/46/CE)

Points juridiques (fin)

- Normes et certifications
  - ISO 27001, PCI-DSS, etc…
  - Ne constituent en aucun cas une protection à toute épreuve !

- Exigences de sécurité dans les contrats
  - Identification du propriétaire des données
  - Responsabilités respectives des partenaires
  - Mises à jour/corrections de sécurité sur les infrastructures du fournisseur
  - Prévoir et organiser la réversibilité ou le changement de fournisseur
    - Quelqu'un l'a-t-il déjà fait en vrai et à grande échelle ? Combien cela a-t-il coûté ? Combien de temps cela a-t-il duré ? Qui a été viré ? ;-)
  - Prévoir la disparition du fournisseur: mon entreprise y survivra-t-elle ?
    - Ce n'est pas une question rétorique
- En cas de litige
  - Quelle est la juridiction applicable ? (cf pays de localisation du Cloud)

Sécurité réseau / infra

- Quels sont les équipements mutualisés ?
  - Routeur externe
  - Firewall (possibilité d'avoir ses propres règles ?)
  - Baie de stockage
  - Equipements anti-DDoS (s'il y en a…)
  - Points d'accès VPN avec l'entreprise

- Quel est mon degré de séparation vis-à-vis des autres clients ?
  - Même VLAN ?
  - Même serveur ?
  - Même hôte de virtualisation ?
  - Localisation du stockage ?

Authentification, habilitation

- Qui accède au service ? Qui a accès à quoi et a le droit de faire quoi ?
  - Comptes, profils d'utilisateurs
- Authentification
  - Authentification nominative des utilisateurs de l'entreprise
  - 3 solutions
    - 2 annuaires distincts (entreprise + Cloud), avec synchronisation éventuelle
    - Délégation d'authentification
    - Fédération d'identités (SAML, WS-Fédération, …)

    } Action nécessaire de la DSI
- Habilitation et contrôle d'accès
  - Mise en place de permissions d'accès fines sur les ressources et les données
  - Interdire les comptes génériques et le partage de comptes

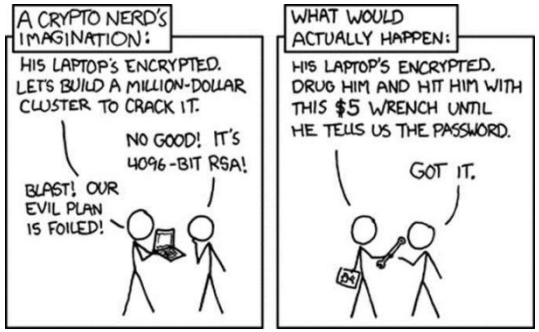
Traçabilité

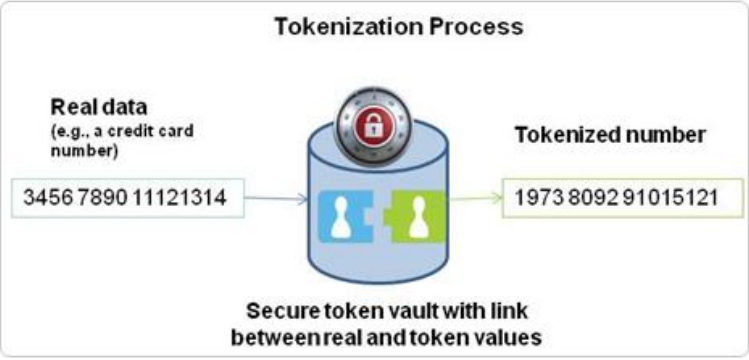
- Qui a fait quoi, quand, sur quelle donnée, depuis où ?
- Deux types de besoins
  - Surveillance des accès aux ressources dans le Cloud
  - Enquête / forensics en cas d'incident

- Recueillir des traces suffisamment complètes (centraliser ou croiser les journaux de logs)
- Protéger l'accès aux traces par le fournisseur de Cloud
- Organiser la consultation ou la récupération des logs
- Prévoir la purge des logs au-delà d'une certaine période

Protection des données

- Objectif: les données sensibles et/ou personnelles ne doivent pas être accessibles au personnel du fournisseur de Cloud ou en cas d'attaque sur l'application
  - Anonymisation dès que possible
  - Chiffrement des données sur le réseau et dans les bases de données
    - On peut effectuer des traitements sur des données chiffrées (stats, …)
  - « Tokenization »
    - Remplacement d'une donnée sensible par un jeton non identifiable avant envoi dans le Cloud
  - Purge dès que possible





Protection des données (suite)

- Chiffrement des données
  - Dans les bases de données et les fichiers
- Chiffrement transparent
  - Chiffrement « à la volée » par l'application ou la base de données
    - Ex: en mode SaaS
  - Les clés de chiffrement sont forcément stockées dans le Cloud
  - Difficile d'interdire l'accès des administrateurs du Cloud aux clés
- Chiffrement de bout en bout
  - Les clés sont détenues par les clients finaux ➔ « BYOK » (BYO Key)
  - Le fournisseur de Cloud ne peut pas déchiffrer les données
  - Mais nécessite soit
    - Un client lourd (ex: Boxcryptor pour stockage sur *Box, *Drive, …)
    - Un proxy/gateway de chiffrement (ex: CipherCloud, Vaultive pour Office 365, …)
    - De la « tokenization as a service » (TaaS) chez un provider tiers

Sécurité applicative

- Le code de l'application louée est-il correctement développé et sécurisé ?
  - Les injections SQL existent depuis 15 ans, pourtant on en produit (et on en trouve) encore !
  - Vérifier que le fournisseur a adopté un cycle de développement sécurisé (cf OWASP, …)

- Des modules de WAF (Web Application Firewall) sont-ils activés pour protéger l'application ?

- Tests d'intrusion nécessaires, périodiques/récurrents
  - Automatisés (scanners de vulnérabilités) ➔ très souvent
  - Manuels, périodiquement

Recommandations (1/2)

- Face à tous ces problèmes, le passage au Cloud est-il opportun ?
  - Oui pour les petites structures, qui peuvent même améliorer leur sécurité actuelle au passage
  - Peut-être pas pour les données cœur de métier d'une grosse structure
  - Analyse de risques: le rapport risques/bénéfices doit être évalué finement au cas par cas par l'entité

- Le passage au Cloud demande une préparation méticuleuse
  - Juridique, organisationnelle, technique
  - Analyse approfondie de l'intégralité des documents juridiques et contractuels (désolé…)
  - Demander (exiger) les architectures techniques détaillées et les logiciels utilisés par le fournisseur, avec leurs versions

Recommandations (2/2)

- Formation des personnels
  - Informaticiens, Directions métiers, juristes, RH, …
- Dédier du personnel à la gestion du Cloud
  - Juridique (évolution des contrats et du service dans le temps ➔ cf Microsoft)
  - Technique (vérification des mises à jour sur l'infrastructure, non dégradation des performances et de la sécurité, audits périodiques, vérification des sauvegardes et restaurations de données, purge des données après les durées négociées, …)
  - Surveillance de la santé du fournisseur
  - Il ne faut pas lâcher le fournisseur !
- La réversibilité doit toujours être envisagée et préparée

QUESTIONS