CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Rencontre AFCDP CLUSIF

La Synergie CIL – RSSI

Thierry Autret RSSI / Adjoint au CIL
Groupement des Cartes Bancaires CB

Le Groupement des Cartes Bancaires CB

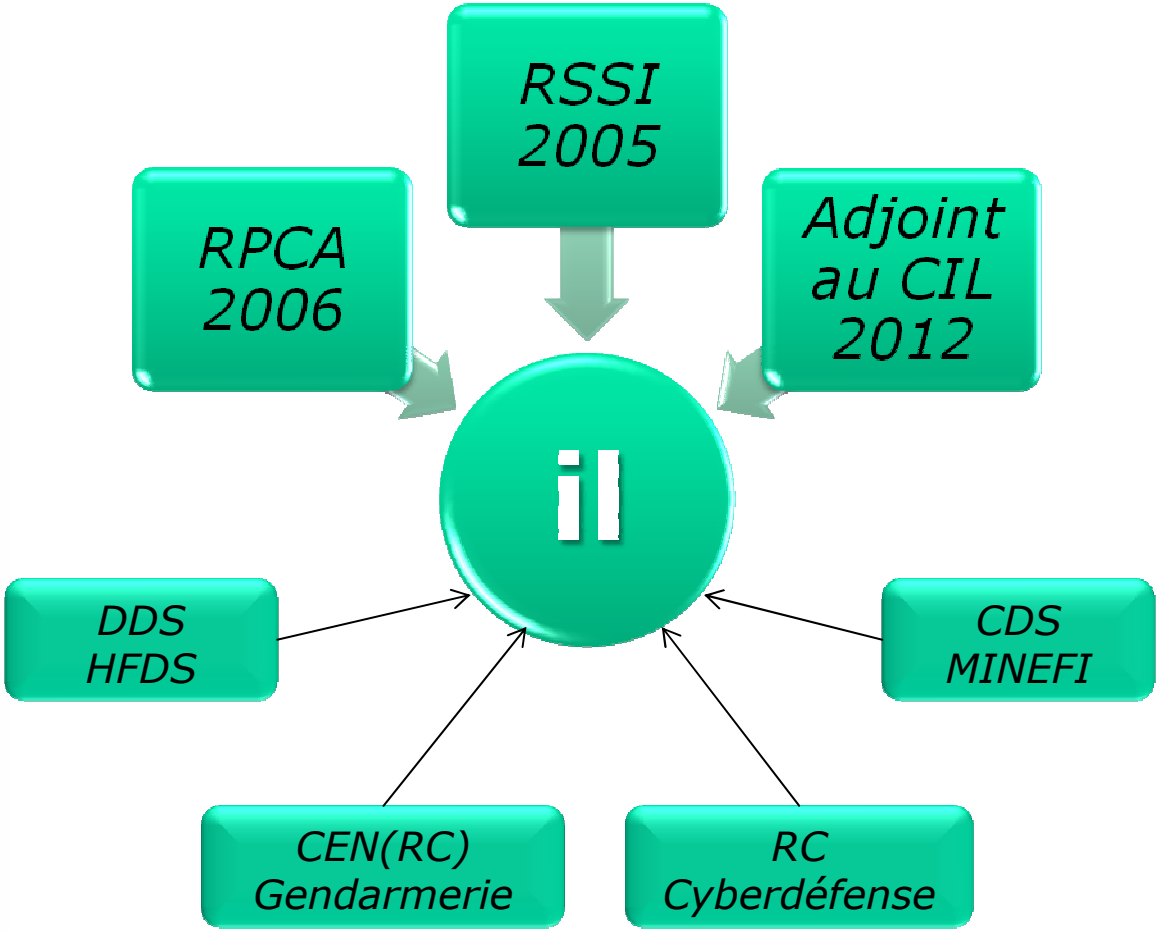
Système de paiement par Cartes Bancaires en France

- Gestion de l'interbancarité en France (134 membres) :
  « *acceptation de toute carte sur tout terminal dans le respect des règles interbancaires* »

- Quelques chiffres au 31 décembre 2011 :
  - Nombre de cartes CB 60 millions
  - Nombres de commerçants 1 million
  - Nombre de DAB 56 000
  - Nombre de transactions (paiements et retraits) 8,5 milliards
  - Montants échangés 482 milliards €

- La société
  - Un peu moins d'une centaine de personnes – taille de PME
  - Visibilité d'importance nationale

Que fait-il ?


RSSI
2005
RPCA
2006
Adjoint
au CIL
2012
il
DDS
HFDS
CDS
MINEFI
CEN(RC)
Gendarmerie
RC
Cyberdéfense

Pourquoi lui ?

36 ans de carrière dont 25 dans la crypto et la SSI

- Compétences SSI ➔ RSSI en 2005

Consultant dans l'offre PCA au cabinet E&Y, puis un des membres fondateurs du ClubCA

- Compétences PCA ➔ RPCA en 2006

Expert à l'International Privacy Championship du cabinet E&Y de 2001 à 2004

- Compétences Privacy ➔ Adjoint au CIL depuis janvier 2012

Pourquoi ce cumul des mandats ?

Les faits

- Le Groupement a une taille de PME (moins de 100p)
  - Difficile de nommer une personne « *à temps plein* » sur chacun des postes
  - Pourtant chacun de ces postes est nécessaire

La recherche d'un barycentre de compétences

- Il n'existe pas forcément
- Mais il peut être un plus qui renforce chacune des fonctions

Il doit être pleinement accepté par le récipiendaire

- Ce n'est pas l'homme à tout faire, ni un mouton à 5 pattes
- Cela requiert une affinité avec les fonctions

Et pleinement officialisé par la Direction et le management

- Fiche de poste à mettre à jour
- Nomination pour les fonctions de CIL ou d'adjoint au CIL

Profil des fonctions : le RSSI

Le profil du RSSI

- Formalisation précise des objectifs de sécurité par des politiques
- Forte sensibilité à la protection des données (classification, chiffrement, intégrité, continuité) – patrimoine informationnel – projet PCI-DSS si concerné
- Aspect relationnel avec la Direction d'une part et le personnel d'autre part (Reporting à la DG, formation, sensibilisation des équipes)
- Relation partenariale avec la DSI
- Connaissance des aspects juridiques liés à la protection du SI et des données (logues, flux, durée de conservation, crypto, etc.)

Profil des fonctions : le RPCA

Le profil du RPCA

- Bonne connaissance des métiers et de leurs besoins
- Connaissance des applications et processus, et donc des données

Profil des fonctions : le CIL

Que dit la loi ?

- La loi Art 22 dit, « *Le correspondant est une personne bénéficiant des qualifications requises pour exercer ses missions* », sans autre indication

Le guide du CIL donne plus d'indications

- Ses compétences doivent porter
  - tant sur **l'informatique** et les **nouvelles technologies**
  - que sur la **réglementation** relative à la protection des données à caractère personnel
  - Elles doivent également avoir trait au **domaine d'activité** dans lequel il exerce ses fonctions. Ainsi, les connaissances du CIL devront aussi concerner **les législations spécifiquement applicables** à l'organisme en matière de commerce électronique, de santé ou de travail, ainsi que les règles particulières de recueil et de traitement de certaines données
  - En **informatique**, une bonne **compréhension du vocabulaire**, des **métiers** et des différents **modes de traitement** des données parait nécessaire.

Qu'est-ce qui est conciliable ?

Compétences juridiques et informatique :

- Elles n'existent pas chez nous sur une seule tête
  - Choix de nommer notre Directrice des Affaires Juridiques et Bancaires comme CIL
  - Choix de nommer le RSSI en tant qu'adjoint au CIL
- Les deux personnes ont été désignées dans leur fonction par la DG via une lettre officielle rappelant les droits et devoirs de la fonction
- Les deux personnes ont été « *introduites* » par courrier
  - À la CNIL
  - Aux filiales
  - Au Comité d'Entreprise
- La CNIL ne reconnait officiellement que le CIL, par exemple l'adjoint au CIL ne reçoit pas d'identifiant pour l'accès à l'intranet

La licéité du cumul de fonction CIL – RSSI

- La loi Art 46 dit : « Les fonctions ou activités exercées concurremment par le correspondant ne doivent pas être susceptibles de provoquer un **conflit d'intérêts** avec l'exercice de sa mission »
- La loi n'en dit pas plus, il est laissé à l'appréciation des entreprises d'en décider

Avantages vs difficultés

Les avantages

- Le RSSI-RPCA une bonne connaissance des applications et des données traitées (encore que !)
- Il connait les métiers
- Il a des relations avec les responsables de traitements
- Il a fait des sensibilisations / formations à la sécurité des données (au sens large)
- La fonction de CIL lui permet de découvrir certaines applications « *dans un coin* »

Les difficultés

- Gérer la double casquette est parfois difficile
- Le RSSI doit connaitre les flux, les applicatifs , il surveille ce que font les postes, il analyse les logues
- Il utilise des outils puissants de scrutation
- Ce n'est pas un réel problème encore faut-il faire la part des choses
- Apprendre à gérer le temps passé à l'une et à l'autre des fonctions