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

L'intérêt de la 27001 pour le CIL

Frédéric Connes
<Frederic.Connes@hsc.fr>

Correspondant informatique et libertés

- Loi du 6 janvier 1978, art. 22, III.
  - Les traitements pour lesquels le responsable a désigné un correspondant à la protection des données à caractère personnel chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi sont **dispensés** des formalités [préalables] (…)
- Désigné à la CNIL
- Indépendant mais pas « protégé »
- Chargé de faire respecter la loi informatique et libertés dans l'organisme
  - Ou plutôt, d'identifier les non-conformités juridiques et leurs conséquences (appréciation des risques juridiques)
  - Le responsable des traitements mettra en balance ces risques avec les autres paramètres

Obligation de sécurité

- Loi du 6 janvier 1978, art. 34
  - Le responsable du traitement est tenu de prendre t**outes précautions utiles**, au regard de la nature des données et des risques présentés par le traitement, pour préserver la **sécurité** des données et, **notamment**, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès
- Obligation de moyens renforcée
- Tous les critères de la sécurité ?
- Sanction pénale : 5 ans, 300 000 euros (226-17 du CP)
- Le CIL peut-il être RSSI ?
  - Conflit d'intérêt ?
  - Le RSSI peut être CIL sans le savoir...
  - Intérêt du cumul des fonctions : art. 34 = levier pour le RSSI

Notification des violations

- Loi du 6 janvier 1978, art. 34 bis
  - (…) on entend par **violation** de données à caractère personnel toute violation de la **sécurité** entraînant **accidentellement** ou de manière **illicite** la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la **fourniture au public** de services de communications électroniques
- Pas de « notamment »
- Uniquement pour les FAI aujourd'hui
  - Mais préfiguration de ce qui attend tout le monde demain
  - Notamment avec le projet de règlement européen

Notification des violations

- Loi du 6 janvier 1978, art. 34 bis
  - En cas de violation de données à caractère personnel, le fournisseur de services de communications électroniques accessibles au public **avertit**, **sans délai**, la CNIL
  - Lorsque cette violation peut porter atteinte aux données à caractère personnel ou à la vie privée d'un abonné ou d'une autre personne physique, le fournisseur **avertit également, sans délai, l'intéressé**
- Inspiré du dispositif américain
- Objectif : inciter à sécuriser pour réduire le risque d'image
- Obligation d'autodénonciation à la CNIL ?
  - Non, car l'article 34 impose une **obligation de moyens** sur la sécurité
  - Il faut donc montrer qu'on a mis en place les moyens

Quels moyens ?

- Contrat avec les sous-traitants
  - Loi du 6 janvier 1978, art. 35
    - Le sous-traitant doit présenter des **garanties suffisantes** pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34
    - Le **contrat** liant le sous-traitant au responsable du traitement comporte l'indication des **obligations** incombant au sous-traitant en matière de protection de la **sécurité** et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que **sur instruction** du responsable du traitement
  - Le responsable des traitements reste responsable de la sécurité

Quels moyens ?

- Mesures de sécurité
  - Se conformer à l'**état de l'art**
  - Mesures proposées par la CNIL lors d'une déclaration
    - Accès physique au traitement protégé (local sécurisé)
    - Authentification des utilisateurs
    - Journalisation des connexions
    - Réseau interne dédié (non relié à Internet)
    - Chiffrement

Quels moyens ?

- Mesures de sécurité
  - 10 conseils de la CNIL (octobre 2009)
    - Politique de mots de passe
    - Procédure de création/suppression des comptes utilisateurs
    - Politique de sécurité du SI
    - Sensibilisation
    - Etc.
  - Guide sécurité de la CNIL (octobre 2010)
    - 48 pages
    - 17 fiches pratiques
    - Questionnaire d'évaluation (14 questions)
    - Pour un public d'informaticiens
    - Informatique mobile, continuité d'activité, sécurité réseau, etc.

Quels moyens ?

- Démarche sécurité
  - Guide sécurité avancé de la CNIL (juillet 2012)
    - Deux documents
    - A destination d'un public technique
    - Approche organisationnelle de la sécurité
    - Document 1 : « Gérer les risques sur les libertés et la vie privée »
      - Proche de la méthode EBIOS
        - Contexte
        - Événements redoutés
        - Menaces
        - Risques
        - Mesures
      - Pourquoi la CNIL soutient-elle EBIOS ?

Quels moyens ?

- Document 2
  - « Mesures pour traiter les risques sur les libertés et la vie privée »
  - Catalogue de bonnes pratiques « informatique et libertés »
    - Agir sur les éléments à protéger
    - Agir sur les impacts
    - Agir sur les sources de risques
    - Agir sur les supports
    - Actions transverses

ISO 27001

- Et ISO 27001 dans tout cela ?
  - Peut-on démontrer l'obligation de moyens en matière de sécurité en implémentant la norme ISO 27001 ?
  - Oui : rien dans les textes juridiques et la jurisprudence n'impose une méthode ou ne favorise une méthode par rapport à une autre
  - Les normes techniques sont d' « application volontaire »
    - Sauf :
      - Si citées explicitement dans un marché public ou un contrat
      - Si rendues obligatoires par un arrêté
        - Dans ce cas, le texte peut conférer une présomption de conformité à la réglementation si respect de la norme technique
        - Mais faible probabilité pour que le respect de l'ISO 27001 vaille un jour présomption de conformité à l'article 34 de la loi informatique et libertés
  - Il faudra donc convaincre la CNIL et le juge pénal de l'efficacité de l'ISO 27001

ISO 27001

- Intérêts fondamentaux de l'ISO 27001
  - Démarche d'amélioration continue (SMSI)
    - Fait progresser la sécurité indépendamment du niveau de départ
  - Certifiable
    - Contrairement à la méthode de la CNIL
    - La CNIL peut labelliser des produits ou procédures (art. 11)
      - Mais pas de label en matière de sécurité
      - Pas avant longtemps
      - Cependant, la procédure d'audit informatique et libertés est labellisable
        - Dans le dossier, la partie audit de sécurité joue un rôle fondamental
          - Empêche d'avoir le label si insuffisante
          - Mais libre choix de la méthode d'audit
          - Un audit ISO 27001 est donc envisageable

ISO 27001

- Intérêts de l'ISO 27001
  - Internationale
    - EBIOS est française (mais c'est peut-être un avantage du point de vue de la CNIL)
  - Adaptée à tous les organismes
    - Notamment aux organismes multinationaux
  - Légère
    - Plus facilement défendable auprès de la direction
  - Formelle
    - Notamment : rôles et responsabilités clairement définis
  - Ne concerne pas spécifiquement les données personnelles
    - Permet de capitaliser la démarche de sécurité sur un périmètre élargi

Pour le CIL

- ISO 27001 est une boîte à outils pour l'action du CIL
  - Plan
    - 5.2.1 c) et A.15.1.1 : identifier et traiter les exigences légales et réglementaires
    - 4.2.1 b) 2) : tenir compte des exigences légales ou réglementaires
    - 4.2.1 c) 1) : identifier une méthodologie d'appréciation des risques adaptée aux exigences légales et réglementaires
    - 4.2.1 g) : sélectionner les objectifs et mesures de sécurité en tenant compte des exigences légales et réglementaires
  - Do
    - A.15.1.4 : protection des données et confidentialité des informations relatives à la vie privée
    - A.13.2.3: collecte de preuves conformément aux dispositions légales à la suite d'un incident lié à la sécurité de l'information

Pour le CIL

- Check
  - 4.3.3 : maîtrise des enregistrements en tenant compte des exigences légales ou réglementaires
  - 4.2.3 d) 6) : réexaminer les appréciations du risque compte tenu des changements apportés à la législation ou à la réglementation
  - 6 a) : conformité à la législation lors des audits internes
  - 7.3 c) 4) : sortie de la revue de direction : modification des exigences légales ou réglementaires

Rôle du CIL

- Plus globalement, quel doit être le rôle du CIL dans la mise en œuvre de l'ISO 27001 ?
  - Aider le RSSI à convaincre la direction et la DSI de l'intérêt de se conformer à la norme, voire de se faire certifier
  - Être maître d'ouvrage de la mise en œuvre de la norme
    - Car la loi fait de lui le garant du respect des obligations légales, et donc de la sécurité des traitements de données personnelles
    - Le RSSI sera alors le maître d'œuvre
  - Conserver les preuves de la prise en compte de l'impératif de sécurité
    - Audits, appréciations des risques, mesures de sécurité prévues et appliquées...
    - Certification le cas échéant
  - Tenir informé le responsable des traitements des non-conformités à l'obligation de sécurité

Contrôles CNIL

- La certification ISO 27001 protège-t-elle d'un contrôle de la CNIL ?
  - Possibilité depuis 2004 : contrôle *a posteriori*, sur place
  - De plus en plus de contrôles sur la sécurité
    - Notamment après des révélations dans la presse
    - La certification peut aider à améliorer la sécurité et donc réduire ce risque
  - Le CIL doit pouvoir produire immédiatement le certificat ISO 27001
  - Mais les agents de la CNIL feront tout de même des investigations techniques
  - Cependant, une bonne partie de l'obligation de moyens sera démontrée par la certification
  - Le risque de sanction, même si les agents de la CNIL identifient des problèmes de sécurité, sera donc largement réduit

Prospective

- La sécurité est-elle l'avenir du CIL ?
  - Le CIL est déjà le garant de la sécurité juridique
  - Le CIL doit posséder des compétences techniques et juridiques
  - Beaucoup de RSSI deviennent CIL
  - Les experts en SSI proposent des formations CIL
  - La sécurité devient la principale préoccupation de la CNIL
- Il doit se former à tous les aspects de la SSI
  - Techniques, organisationnels, juridiques
- Projet de règlement européen : art. 30 à 32
  - Sécurité des traitements et notification des violations

Questions ?