CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles

Feedback FIC 2017

Plan

1. Constats et volontés de la CNIL
2. Qui sont-ils ?
3. Quelles sont leurs interrogations ?
4. Réponses et pistes de réflexions.

Présence de la CNIL

- Présence au FIC en 2016 et 2017
  - Nombre de personnes vues (progression)
- Objectifs
  - Identifier les attentes des responsables de traitement
  - Identifier les problèmes clés de sécurité
  - Se positionner comme un acteur à part entière de la prise en compte des enjeux de sécurité
- Proposer
  - Une prise en compte en amont du respect de la vie privée et de la sécurité
  - Rapprocher les enjeux de sécurité et de protection de la vie privée
  - Mettre en œuvre une démarche orientée risques

Qui

Organisations

- Organismes publics (santé, police, justice, collectivités territoriales)
- Cabinets de conseil
- Cabinet d'avocats
- Editeurs de solutions et SSI
- Entreprises diverses

Services

- Juridique
  - Notamment le service I&L / DPO
- DSI et/ou Risque
  - Notamment le service RSSI
- RH
- Marketing et commercial

Personnes

- Consultants
- Juristes et avocats
- CIL
- Chefs d'entreprise
- DSI
- RSSI
- Responsables sureté
- Ingénieur informatique (sécurité, développement, projet, risque)
- MOA et AMOA

Sujets

Trois axes majeurs pour les visiteurs du stand de la CNIL :

I - le **règlement européen sur la protection des données** (GDPR)

II - les **solutions de sécurité**, leur évolution et la posture en rapport avec la **Loi Informatique et Libertés**

III - les sujets propres à la **protection des libertés individuelles** (notamment sphère police, justice et renseignement dans un contexte géopolitique compliqué)

GDPR

Je suis responsable sécurité en charge des risques et j'ai peur que le juridique reprenne la main sur le PIA via son rôle I&L (et inversement)

- Compréhension du **règlement** (de nombreuses parties restent floues)
- Le **PIA (Privacy Impact Assessment)**
  - quand (rétroactivité sur applicatifs déployés) ?
  - pour qui ?
  - comment ?
- **Notification** de violation de données à caractère personnel
  - Question autour du lien entre notification et contrôle pour la CNIL
  - Modèle de déclaration et évolution
- Différence entre **CIL** et **DPO/DPD** (G29)
- Quid de la possibilité d'entrer dans une démarche d'échange et de conseil
  - Quid de l'évolution de la CNIL pour prendre en compte la capacité **d'accompagnement** auprès des organismes (ressources) ?
  - Quid de la possibilité d'assister aux **ateliers CIL** (MOOC) ?

Sécurité

- De la sécurité périmétrique à la détection
  - Blocage des adresses IP et problèmes des **listes noires** (Notamment solution de protection contre le **DDOS** + problème géographique des solutions)
  - Désencapsulation des flux **HTTPS** / Loi **Godfrain**
  - Solutions de **détection** et **analyse comportementale** de l'individu
  - **Mode de déclaration** des sociétés d'audit te de test d'intrusion (Prestataire d'audit de la sécurité des systèmes d'information (PASSI) de l'ANSSI)
  - Solutions de **bug-bounty** et accès aux données à caractère personnel
  - Gestion des **logs** de sécurité et Loi I&L
  - Outils de gestion de la **fraude** et de détection des actions malveillantes

Libertés individuelles

- De nombreux échanges ont également concernés :

  - Chiffrement et portes dérobées
  - Vidéosurveillance et vidéoprotection
  - Fichier TES (Titres électroniques sécurisés)
  - Privacy shield et sa viabilité
  - Rôle de la CNIL autour des enjeux éthiques des algorithmes
  - Liens entre la CNIL et l'ANSSI
  - Evolution de la Loi I&L
  - La notification des violations de données à caractère personnel (un individu peut-il notifier à la CNIL ?)

Réponses et pistes de réflexions

- Mise à disposition d'un **outil PIA**
- Participation à des **groupes de travail** (ISO/Normes, Forum des compétences, Groupe de Berlin,)
- **Sensibilisation** (conférences, salons, etc.)
- Evolution des **formulaires de notification** + Mise en œuvre de processus de gestion internes
- Clarification des éléments du règlement via les **guidelines G29**
- Accompagnement des entreprises et organismes publics :
  - GDPR
  - protection des données à caractère personnel
  - prise en compte des enjeux de sécurité

CNIL.

On parle des problèmes de sécurité rencontrés avec les métiers

On construit des équipes pluridisciplinaires

On ne connecte pas le WiFi client au réseau bureautique de l'entreprise

On verrouille son poste de travail

On chiffre les données transmises

Pas de base de données de production en test

MERCI DE VOTRE ATTENTION