LISE BRETEAU
Avocat au Barreau de Paris

lb@breteau-legal.fr

GS Days
LES JOURNÉES FRANCOPHONES DE LA SÉCURITÉ

La lutte défensive, pour répondre à quels risques légaux et réglementaires?

GS DAYS #8 – Paris – 07 Avril 2016

« Lutte défensive : de la détection à la réponse à incident, quelle réalité ? »

La lutte défensive, pour répondre à quels risques légaux et réglementaires?

- Contexte
- Historique et évolutions à anticiper
- Enjeux
  1. Répondre aux nouvelles obligations légales de notification
  2. Répondre au renforcement des obligations de gestion de la sécurité
  3. Gérer la banalisation de risques forts
  4. Couvrir les risques de responsabilité liés aux traitements d'informations

Contexte

- Des attaques de toutes sortes
  - Outils d'attaques des plus simples aux plus complexes, voire inconnus/invisibles
  - Objectif de collecte de données ou de modification/suppression de données ou de systèmes
- Enjeu
  - Protection des données, des systèmes et de la valeur
  - Conformité aux obligations professionnelles, réglementaires, légales
  - Responsabilité vis-à-vis des tiers

Historique et évolutions (1/4)

- Loi Informatique et Libertés (1978)
- Infractions loi Godfrain (1988)
- Directive européenne de protection des données personnelles (1995)

✓*Livre blanc sur la défense et la sécurité nationale (2008)*

- Création de l'ANSSI (2009)

✓*Livre blanc sur la défense et la sécurité nationale (2013)*

- Loi de programmation militaire - LPM (2013)

✓*Stratégie nationale pour la sécurité du numérique (octobre 2015)*

Historique et évolutions (2/4): LPM 2013

- Protection des systèmes d'information sensibles des opérateurs d'importance vitale (Art. L. 1332-6-1 du code de la défense, issu art. 22 loi 2013-1168 du 18/12/2013):

  « Le Premier ministre fixe les règles de sécurité nécessaires à la protection des systèmes d'information des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 et des opérateurs publics ou privés qui participent à ces systèmes pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation. Ces opérateurs sont tenus d'appliquer ces règles à leurs frais.

  Les règles mentionnées au premier alinéa peuvent notamment prescrire que les opérateurs mettent en œuvre des systèmes qualifiés de détection des événements susceptibles d'affecter la sécurité de leurs systèmes d'information. Ces systèmes de détection sont exploités sur le territoire national par des prestataires de service qualifiés en matière de sécurité de systèmes d'information, par l'autorité nationale de sécurité des systèmes d'information ou par d'autres services de l'Etat désignés par le Premier ministre.

  Les qualifications des systèmes de détection et des prestataires de service exploitant ces systèmes sont délivrées par le Premier ministre. »

Historique et évolutions (3/4): LPM 2013

- Référentiels d'exigences ANSSI (Procédure expérimentale avec un panel de prestataires en cours):
  - Référentiel « Prestataires de réponse aux incidents de sécurité » (PRIS), version 1.0 du 06 octobre 2015
    http://www.ssi.gouv.fr/uploads/2014/12/PRIS_Referentiel-d%E2%80%99exigences-v1.0.pdf
  - Référentiel « Prestataires de détection des incidents de sécurité » (PDIS), version 1.0 du 06 octobre 2015
    http://www.ssi.gouv.fr/uploads/2014/12/PDIS_referentiel-d%E2%80%99exigences-v1.0.pdf

Historique et évolutions (4/4) : textes à venir

En France

- Enrichissement des référentiels ANSSI
  - Cf. Référentiel des exigences pour les prestataires d'intégration et de maintenance de systèmes industriels (mars 2016)

En Europe

- General Data Protection Regulation 2016?
- Directive NIS 2016?

Enjeux

1. Répondre aux nouvelles obligations légales de notification
2. Répondre au renforcement des obligations de gestion de la sécurité
3. Gérer la banalisation de risques forts
4. Couvrir les risques de responsabilité liés aux traitements d'informations

1. Répondre aux nouvelles obligations légales de notification

- Multiplication des obligations de notifier les incidents de sécurité
  - Opérateurs d'infrastructures vitales (Art. L. 1332-6-2 c. défense)
  - Opérateurs de télécom (Art. 34 bis loi Informatique et Libertés)
  - Règlement vie privée (GDPR)
    - ✓ Obligation assortie d'une sanction jusqu'à 2% / 10M EUR
  - Directive cybersécurité (SRI)
  - Directive sur les services de paiement n°2 (DSP2)

➢ Notification à l'autorité et/ou aux personnes concernées

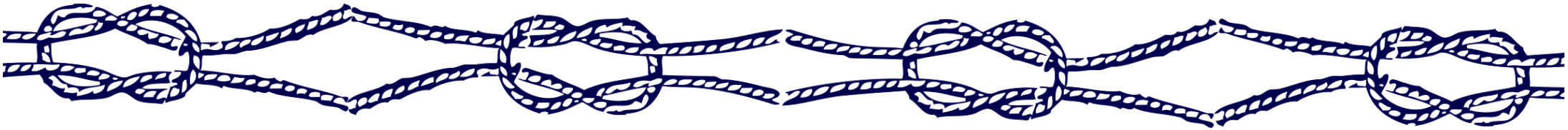
➢ Nécessité de mettre en place des outils pour répondre efficacement à ces obligations et limiter le risque de sanction

2. Répondre au renforcement des obligations de gestion de la sécurité

- La tendance législative est au renforcement des exigences, dans le cadre d'une gestion globale de la sécurité des SI
  - Obligations générales en matière de protection des données personnelles
  - Obligations sectorielles: banque, assurance, santé, infrastructures critiques, etc.

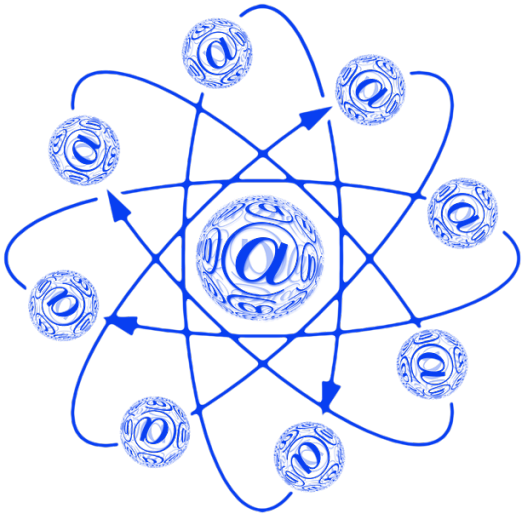
➢ Intégrer une dimension de processus et d'organisation

➢ Approche par le risque



3. Gérer la banalisation de risques forts (1/2)

- L'innovation apporte de nouvelles possibilités d'intrusion dans les systèmes d'information:
  - Objets connectés
  - BYOD
  - Cloud computing
  - Internationalisation des échanges
  - Généralisation des usages du numérique et des réseaux
  - Etc.

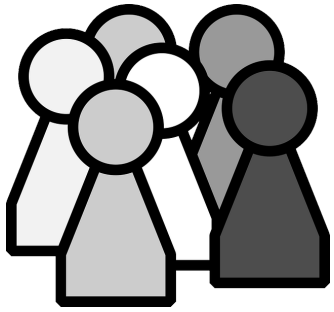


3. Gérer la banalisation de risques forts (2/2)

- Quel encadrement de ces risques au vu des opportunités, voire de la nécessité, de recourir à ces pratiques?
  - Outils juridiques d'encadrement:
    - Recommandations et référentiels ANSSI
    - Obligations réglementaires en matière d'externalisation (par ex. arrêté du 3 novembre 2014 en matière de banque/finance/paiements), d'hébergement (décret du 4 janvier 2006 pour l'hébergement agréé de données de santé), etc.
    - Clauses contractuelles et documents opposables aux salariés (charte informatique, etc.)

4. Couvrir les risques de responsabilité liés aux traitements d'informations (1/2)

- Conséquences étendues des incidents de sécurité:
  - Risque de responsabilité vis-à-vis des tiers affectés par l'incident de sécurité (clients, partenaires, salariés)
    - Responsabilité contractuelle
    - Responsabilité délictuelle
    - Responsabilité pénale?
  - Risque de réputation pour l'entreprise
    - Publications de décisions par les autorités ou la justice
    - Notifications individuelles aux clients
  - Risque de sanctions
    - Sanction maximale prévue par le projet de GDPR: 4% CA mondial ou 20M EUR



4. Couvrir les risques de responsabilité liés aux traitements d'informations (2/2)

- Protéger les actifs de l'entreprise:
  - Droits de propriété intellectuelle
  - Secret des affaires: directive en projet, débat au Parlement le 13 avril 2016
    - Contexte: « *L'utilisation accrue de services en ligne pour les affaires et la recherche, le stockage accru de données confidentielles dans des espaces de stockage virtuels, l'utilisation accrue du commerce électronique et la numérisation dans son ensemble appellent à une législation harmonisée dans toute l'Union afin d'empêcher l'appropriation et l'utilisation abusives de secrets d'affaires. Cette législation garantirait la confiance et la protection des entreprises et des consommateurs et favoriserait la mise en place du marché numérique unique, l'un des fondements d'un marché intérieur efficace.* » (considérant 12 bis)
    - Objectif: Protéger les savoir-faire et les informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites
    - Exécution: Réparation du préjudice, sanctions, procédures

LISE BRETEAU
Avocat au Barreau de Paris

7 rue d'Argenteuil
75001 Paris

Tél. 01 44 01 66 92

lb@breteau-legal.fr

www.breteau-legal.fr

@BreteauLegal

GS Days
LES JOURNÉES FRANCOPHONES DE LA SÉCURITÉ

Merci

#Notification, risques réglementaires, vie privée, approche par le risque, risque de responsabilité, sanctions financières, accountability, politique de sécurité