Cybersécurité et sécurité de l'information : le contexte français

Séminaire EURORAI de Rotterdam, 19 avril 2018

Fabrice NICOL, Chambre régionale des comptes Occitanie (Montpellier)

La cybersécurité en France : un « art de la guerre »

L'intervention précoce de l'Etat dans la lutte contre la cybercriminalité

- L'Etat intervient très tôt par le biais des agences de renseignement (DST puis DGSE), dès la fin des années 80.
- Aboutit à la création de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) , juillet 2009.
- N'est pas une autorité administrative indépendante : rattachement au SGDSN (secrétariat général de la défense et de la sécurité nationale)
- Stratégie de surveillance des communautés de hackeurs, infiltration, repérages dans le milieu du logiciel libre, recrutements.
- Toujours d'actualité : la nuit du hack du ministère de la défense (juin 2017). Tentative de conciliation des valeurs de la société civile et de la défense nationale.

L’aggravation des menaces : une prise de conscience tardive

- La France a été victime de cyberattaques très graves en 2011-2012 : Présidence de la République, ministère des finances, Areva.
- Qui ont suscité une prise de conscience et des réactions (enquête du Sénat)
- Diagnostic des faiblesses de l’organisation et de la protection : le premier audit public de grande ampleur. Egalement en 2011 : Création du Conseil national du numérique, nouvelle stratégie nationale.
- Conseil supérieur de la formation et de la recherche stratégique (CSFRS) : groupe de travail sur les « Menaces contemporaines et technologies de l'information, nouvelles criminalités ». Diagnostic critique (2012) et besoin d’une méthodologie nationale pour l’évaluation et de certification de la sécurité des SI.

Les opérateurs d'importance vitale (OIV)

- La militarisation du champ : article 22 de la loi de programmation militaire (18 décembre 2013), qui fait suite aux préconisations du Livre blanc sur la défense et la sécurité nationale de 2013. Renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent : les systèmes d'information d'importance vitale (SIIV).

- Le 27 mars 2015, deux décrets d'application sont publiés :
  - décret n°2015-351 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale
  - décret n°2015-350 relatif à la qualification des produits de sécurité et des prestataires de services de confiance pour les besoins de la sécurité nationale.

Ce dernier décret définit les **normes d'audit** et de contrôle des prestataires d'audit.

- Une définition large des entités protégées : peut correspondre à des entités publiques ou semi-publiques (grandes sociétés mixtes) **entrant dans le champ des institutions supérieures et régionales de contrôle**. Exemples:
  - SNCF (Cour des comptes)
  - Centres hospitaliers universitaires ou réseaux d'eau potable (Chambres régionales)

12 secteurs d'activités d'importance vitale répartis en 4 dominantes

HUMAINE

Alimentation
Gestion de l'eau
Santé

REGALIENNE

Activités civiles de l'Etat
Activités judiciaires
Activités militaires
de l'Etat

ECONOMIQUE

Energie
Finances
Transports

TECHNOLOGIQUE

Communications électroniques,
audiovisuel et information
Industrie
Espace et recherche

SGDSN

L’actualisation de la stratégie nationale

- Stratégie nationale pour la sécurité du numérique (octobre 2015) : une stratégie essentiellement civile mais d’origine militaire (article R.1132-3 du code de la défense).
- Objectifs : souveraineté nationale ; lutte contre la cybercriminalité ; information du public ; la sécurité numérique comme avantage concurrentiel des entreprises ; action internationale de la France.
- Nouvelle doctrine nationale de cyberdéfense (décembre 2016) dans le contexte de la lutte contre le terrorisme sur internet. Riposte et de neutralisation : « un art de la guerre » (Le Drian).
- Dimension préventive, répressive et proactive : riposte (représailles) et neutralisation (élimination)

De nouveaux défis pour l'audit et le contrôle

- La forteresse assiégée : les mesures de protection classiques (hiérarchie de droits, pare-feu, détection d'intrusions par signature, compartimentation des SI) ne suffisent plus. Menaces persistantes avancées (APT) : piratage informatique furtif et continu, souvent orchestré par des humains ciblant une entité spécifique (Pernet 2014)
- Les causes :
  1. L'extension des réseaux et du nombre de serveurs
  2. La démocratisation du cryptage et de l'obfuscation des traces (Tor, VPN dans des paradis fiscaux…) et du code source malveillant (le hacking comme discipline d'excellence)
  3. L'inefficacité du droit à déterminer l'imputabilité des attaques et à les réprimer.

L'inefficacité du droit

"Whether in Europe, the United States, Russia, China, Africa, or Brazil, few cases of 'cyber-crimes' are effectively treated by the judicial system, and much less have been sanctioned. The mechanisms of judicial co-operation are very often ineffective in the areas of cybercrime, not through a lack of talent,—as State forces usually have decisive talents in this area—but by the unworkable nature of the technical cooperation on cybercrime." (Baumard 2017, p.39, Fleck 2012, Kenneth 2010)

- Les divergences d'interprétation de la convention sur la cybercriminalité du Conseil de l'Europe et l'absence de large ratification
- Comment évaluer les réponses des organismes audités à ces nouveaux défis ? Leur responsabilité en cas de sinistre ?

L’extension de la stratégie de sécurité

- La directive européenne UE n°2016/1148 Network and Information Security (NIS, 6 juillet 2016) : assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d’information de l’Union européenne. La loi française du 26 février 2018 transpose la directive.
- Elle renforce la protection face à des attaques informatiques plus nombreuses et sophistiquées qui *« peuvent désormais avoir des impacts très forts dans le monde physique »* (ANSSI).
- Elle élargit la stratégie de nombreux autres acteurs non-OIV des secteurs public et privé, qui demeurent très vulnérables aux attaques informatiques type WannaCry : les **opérateurs de services essentiels**.
- Conséquence : toujours plus d’organismes dans le périmètre de compétences des institutions d’audit et de contrôle.

Les institutions de contrôle de plus en plus concernées

- Détermination par la loi des règles de sécurité et de certification **(= axes de contrôle**) :

  « 1° La gouvernance de la sécurité des réseaux et systèmes d'information
  2° La protection des réseaux et systèmes d'information
  3° La défense des réseaux et systèmes d'information
  4° La résilience des activités.
  Les règles prévues au même premier alinéa peuvent notamment prescrire que les opérateurs recourent à des dispositifs matériels ou logiciels ou à des services informatiques dont la sécurité a été certifiée. » (article 6 loi 27 février 2018)

- **Consécration de l'ANSSI comme institution de contrôle** de plein exercice et délégation partielle au secteur privé :

  « Les contrôles sont effectués, sur pièce et sur place, par l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense ou par des prestataires de service qualifiés par le Premier ministre. » (article 8)

- Une **nouvelle concurrence** pour les institutions traditionnellement chargées du contrôle des comptes et de la gestion ?

L’audit et le contrôle de la sécurité de l’information : les enjeux français

Evaluer la performance financière des contre-mesures

- Le renforcement des contre-mesures est une nécessité (détection des intrusions). Trois axes de détection:
  - Méthodes classiques de détection des signatures des intrusions (antivirus)
  - Méthodes comportementales (analyse des réponses du SI)
  - Intelligence artificielle / apprentissage profond
- Mesures de plus en plus coûteuses : l'arbitrage entre efficacité et efficience devient plus délicat à évaluer. Le point d'équilibre dépend du coût potentiel des sinistres en cas d'attaque : or ce coût est rarement connu avec certitude
- Les coûts se déplacent du matériel vers l'immatériel (logiciels et ressources humaines).

Evaluer la mise en œuvre des méthodes normalisées en France

- Méthode EBIOS (ANSSI) : contexte, événements redoutés, scénarios de menaces, risques, mesures de sécurité. Compatible normes ISO 13335 (GMITS), ISO 15408 (critères communs) et ISO 17799.
- Claire, exhaustive et adaptative mais pas de solutions immédiates : méthode surtout diagnostique
- Méthode MEHARI 2010 du CLUSIF (Club de la sécurité de l'information français, association indépendante ouverte à toutes les entreprises et collectivités) désormais développée au Québec (CLUSIQ) : norme ISO 27005:2009. Peut être utilisée aussi dans le cadre d'un Système de management de la sécurité de l'information (ISO 27001:2005). Divers degrés. Version PRO pour les PME. Libre et gratuite.
- Pas de méthode des juridictions financières spécialisée sur la sécurité des SI à ce jour mais un guide général sur le contrôle des SI (Centre d'appui métier de la Cour des comptes).

Les freins financiers

- Un marché oligopolistique : faible nombre d'organismes privés (environ 25) : Airbus Defense and Space, Bull, CGI, CS, Ernst and Young, Steria, Orange,PWCA, Sogeti, Thales. 10 % de jeunes pousses PME.

- Des coûts élevés : 60 000€ en moyenne (Baumard 2017) pour un audit de sécurité de base.

- Ces coûts de contrôle ne sont qu'occasionnellement à la portée des juridictions financières françaises.

Quelques axes de contrôle prioritaires dans un contexte de ressources rares

- Nos institutions ont un atout : l'expérience d'une approche globale et systémique.
- Ne pas se focaliser exclusivement sur les techniques informatiques : apprécier leur insertion dans une politique cohérente : stratégie, budget, ressources humaines, contrôle interne, processus, conformité réglementaire, modernisation de l'outil, veille technologique.
- Tous les référentiels internationaux comprennent un volet d'audit fonctionnel portant sur ces domaines et sur le rôle du RSSI (Responsable de la sécurité des systèmes d'information - CISO).

L’enjeu des audits d’évaluation

- Audit des menaces et audit de validation des réponses : à ce jour seules l’ANSSI et les entreprises certifiées sont en mesure de réaliser les audits.
- Pour les audits d’évaluation (*assessment audit*), les juridictions financières ont un rôle à jouer et peuvent monter en compétence :
  - déterminer si les mesures sont conformes à la réglementation ou aux normes
  - établir la cartographie des réponses aux menaces
  - évaluer l’efficacité et l’efficience de ces réponses
  - évaluer la posture de sécurité : la prise en compte stratégique et tactique
- Le contrôle de la protection des données personnelles est un cas particulier techniquement et financièrement à la portée des juridictions financières.

Le contrôle de la protection des données personnelles

- Une tradition française (loi Informatique et libertés du 6 janvier 1978), actualisée par le RGPD (Règlement général de la protection des données) à compter de mai 2018.
- La CNIL diffuse des outils pratiques (logiciel PIA). Elle met en place un nouvel outil de conformité, la certification, qui remplacera la labellisation.
- Elle promeut des **plans d'action qui peuvent aussi servir au contrôle**: pilotage, cartographie, priorisation, identification des risques, organisation des processus internes, documentation des procédures et de la conformité.

La manipulation des données personnelles par les juridictions financières

- Les JF utilisent les données personnelles des bases de paye pour des traitements automatisés de masse
- Cas différents selon les niveaux de contrôle :

- la base des personnels de l'Etat est anonymisée et cryptée, avec levée de l'anonymisation régulée par le ministère des finances, au besoin.
- les bases de certains établissements publics et des collectivités territoriales sont nominatives et non cryptées, principalement sous format XML et conservées 4 à 6 ans voire davantage.
- Logiciels Xemelios, CDGD, ORC, Altaïr : obtention ou traitement de données de masse jusqu'à 20 millions de lignes de paye par an pour la ville de Paris.

- La question se pose de la conformité des pratiques au regard du RGPD

Quelques règles et précautions à observer (I)

- *Considérant 45* - « Lorsque le traitement est effectué conformément à une obligation légale à laquelle le responsable du traitement est soumis ou lorsqu'il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, le traitement devrait avoir un fondement dans le droit de l'Union ou dans le droit d'un État membre. [le droit doit déterminer…] **la durée de conservation** et d'autres mesures visant à garantir un traitement licite et loyal. »

- Pas de durée de conservation normée à ce jour pour les bases conservées par les chambres régionales des comptes et certaines bases d'établissement d'Etat (Cour des comptes).

Quelques règles et précautions à observer (II)

- *Considérant 97* - « Lorsque le traitement est réalisé par une autorité publique, à l'exception des juridictions ou des autorités judiciaires indépendantes **agissant dans l'exercice de leur fonction juridictionnelle**, lorsque, dans le secteur privé, il est effectué par un responsable du traitement (…) Ces délégués à la protection des données, qu'ils soient ou non des employés du responsable du traitement, devraient être en mesure d'exercer leurs fonctions et missions en toute indépendance. »
- Les juridictions financières utilisant les données de paye devraient donc, en principe, nommer un délégué à la protection des données, dès lors que ces données ne sont pas utilisées en procédure juridictionnelle (exemples en France : contrôles de gestion ; contrôles budgétaire des chambres régionales de comptes).
- Une rédaction à actualiser du Code des juridictions financières et des normes professionnelles ?

Références

Baumard, Philippe (2017) *Cybersecurity in France*, Springer Briefs in Cybersecurity, Springer

Donaldson, Scott E.; Siegel, Stanley G. ; Williams, Chris K. and Aslam, Abdul (2015) Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats, Springer Science, Apress.

Fleck D (2012) *Searching for international rules applicable to cyber warfare—a critical first assessment of the New Tallinn manual*. Int J Conflict Secur Law 18(2):331–35

Kenneth G (2010) *The challenge of cyber attack deterrence*. Comput Law Secur Rev 26(3):298–303

Pernet, Cédric (2014) *Sécurité et espionnage informatique : Connaissance de la menace APT (Advanced Persistent Threat) et du cyberespionnage*, Eyrolles