Stratégie d'élaboration des PSSI d'établissement

Dominique MAILLOT (HFADS)
Isabelle MOREL (HFDS/FSSI)

Exercice Piranet 12

Scénario de l'exercice

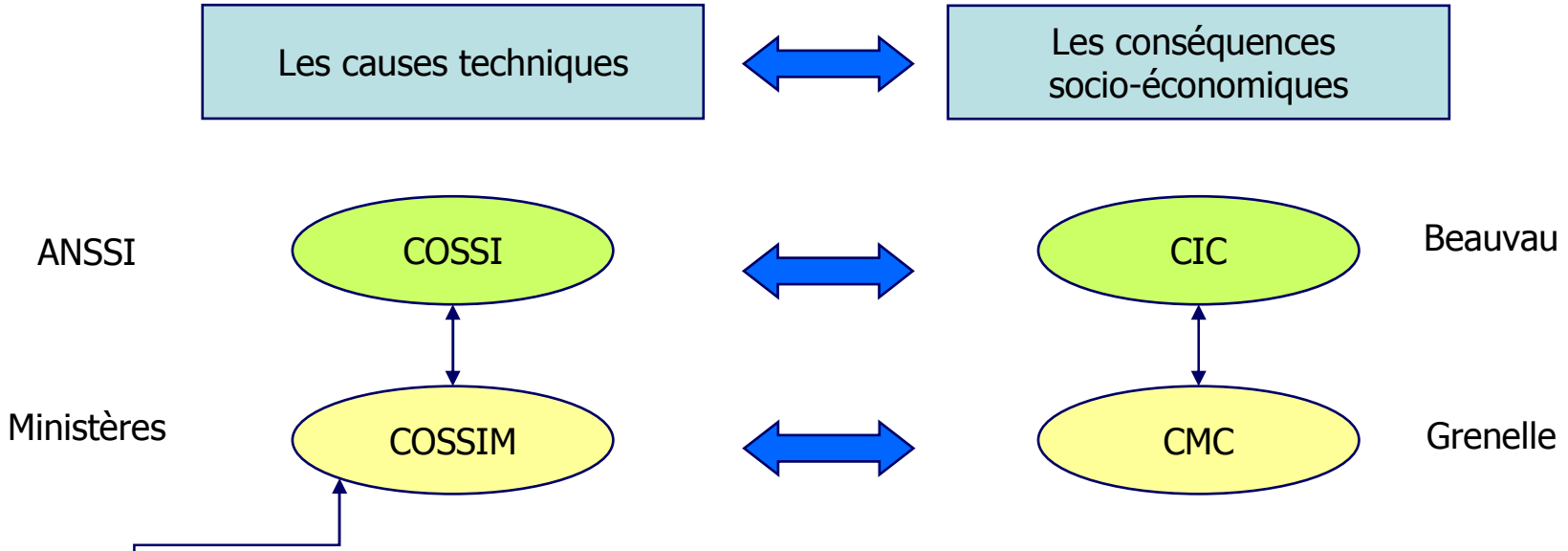
- Attaque massive des systèmes d'information français, suivant deux axes:
  - Compromission de postes de travail des réseaux ministériels
    - Installation de chevaux de Troie depuis novembre 2011
    - Exfiltration de données sensibles
  - Attaque des box grand public du réseau internet
    - Prise de contrôle des box
    - Attaque du réseau internet et des postes de travail en France et à l'étranger

- Conséquences
  - Perte de l'internet le 8 février 2012
  - Perte des intranets ministériels le 9 février 2012
  - Situation dégradée durable (> 2 semaines)

- Mise en place de l'organisation de crise nationale le 8 février

Exercice Piranet 12

organisation de crise



- La gestion technique repose sur le COSSIM
  - Interfaces
    - **Votre interface**
    - **RENATER**
    - ANSSI/COSSI
    - Organisation nationale de crise
    - STSI
    - MOA
    - Opérateurs, OIV
  - Gestes techniques

COSSI : centre opérationnel de la sécurité des systèmes d'information
COSSI : centre opérationnel de la sécurité des systèmes d'information ministériel
CIC : cellule interministérielle de crise
CMC : cellule ministérielle de crise

STSI Service des technologies et des systèmes d'information du MENJVAMESR
MOA Maîtrise d'ouvrage
OIV Opérateur d'importance vitale

Exercice Piranet 12

Gestion de la crise : mesures phares

- Déconnexion des box grand public
  - NB : 54000 box grand public assurent la connexion des établissements du 1er degré
- Cloisonnement
  - Internet / administration centrale
  - Internet / RENATER
- Mise en œuvre des PCA
  - Pour les activités dont vous souhaitez maintenir le service
- Redémarrage à froid des systèmes d'information des ministères
  - Cloisonnement
  - Reconfiguration de tous les postes de travail

Exercice Piranet 12

Enseignements

- RENATER est un atout important
  - Supervision CERT RENATER
  - Maîtrise de l'infrastructure avec capacité de filtrer et cloisonner
- La gestion centralisée des postes de travail est un atout déterminant
  - Ce devrait être la règle
- Le COSSIM est la cheville ouvrière de la gestion de crise
  - Consolider son organisation
- Elaborer des PCA
  - Recenser les systèmes d'information critiques (cartographie)
  - Planifier les mesures permettant d'assurer la continuité du service
- Intégrer ces éléments dans la PSSI de l'établissement
  - Analyse des risques -> description des mesures de maîtrise
  - Description des axes d'amélioration

Politique de sécurité des systèmes d'information

- Définir et mettre en œuvre une politique de sécurité globale des SI
  - Analyser les risques
  - Mettre en œuvre les mesures adéquates
    - Exemples (d'après la norme ISO 27001)
    - Gestion des ouvertures/fermetures des comptes
    - PCA/PRA
    - Gestion des actifs
    - Contrats de sous-traitance
    - Sécurité physique/ sécurité du matériel/ sécurité du réseau
    - Sécurité liées aux RH
    - Etc.
- Intégrer la sécurité tout au long de la vie du système
  - Dès la conception d'un SI
    - Identifier les objectifs de sécurité (MOA)
    - Déterminer les exigences de sécurité devant satisfaire les objectifs (MOE)
  - Jusqu'à la fin de vie
- S'organiser
  - AA, AQSSI, RSSI
  - Qualification des produits
  - Qualification des prestataires
  - Homologation des systèmes
  - Contrôler, ou auditer

PSSI

- Notre objectif aujourd'hui :
  - Que chaque établissement soit en mesure de maîtriser ses risques
  - Qu'il élabore sa PSSI
    - Outils
    - accompagnement

Initiative d'un projet de PSSI générique pour les universités

- **En 2005, le SDSSI** (schéma directeur de la sécurité des systèmes d'information) pour la communauté éducative
  - Document d'orientation de la sécurité dans le système éducatif
  - Cadre commun de la SSI
  - Plan d'actions
- **En 2006**, un prolongement de cette initiative dans le monde de l'enseignement supérieur : le **groupe SDS-SUP**, mandaté par la CPU, la DR, la DES et le HFDS.

  Constitué de RSSI d'universités, d'organismes de recherche, d'écoles et co-animé par le CRU (Comité réseau des universités) et la FSSI (HFDS)

- **En 2009, un GT PSSI « générique »** pour les universités pour faciliter la démarche de chaque établissement.
  - 7 universités pilotes : Université Aix-Marseille2 (Université Aix Marseille), Université Bordeaux1, UNR-RUNN Normandie, Grenoble Universités, Université de Limoges, Nancy-Université (Université de Lorraine), Rennes1
  - Une contribution financière de chaque université
  - Un co-financement ministériel dans le cadre du S3IT pour se doter d'un appui par une société de conseil,
  - Une collaboration CPU, CRU, HFDS

Initiative d'un projet de PSSI générique pour les universités

- En 2010-2011,
  - mise en place d'un comité de pilotage local dans chaque établissement pilote
  - formation aux entretiens d'analyse de risques par la société de conseil
  - entretiens en établissements
  - 3 réunions d'étape
  - une réunion de validation des documents diffusables avec l'assistance du bureau conseil de l'ANSSI

- Les **acteurs impliqués** dans une PSSI d'établissement
  - le Chef de l'Etablissement ou son représentant direct
  - le Fonctionnaire de Sécurité de Défense (FSD)
  - la Direction des Systèmes d'Information (DSI)
  - le Responsable de la Sécurité des Systèmes d'Information (RSSI)
  - les directions métier
  - le service des Ressources Humaines
  - le représentant du service juridique
  - le Correspondant Informatique et Libertés (CIL)

- L'information et l'adhésion de tous les usagers au travers de la validation de la PSSI par le Conseil d'administration d'établissement

Initiative d'un projet de PSSI générique pour les universités

- 2012-2013, des mesures d'accompagnement,

  – Conférence d'information et de sensibilisation aux enjeux de la sécurité de l'information dans les établissements d'enseignement supérieur et de recherche à destination de la gouvernance des établissements
    - Les enjeux
    - Les menaces
    - Les dispositifs de réponse aux menaces
    - Un référentiel de PSSI générique pour les établissements
    - Le partage d'expérience des 7 université pilote
    - Les conseils de l'ANSSI

  - Modules de formation pour les établissements

  - Club des utilisateurs de la PSSI génériques pour partage d'expériences