Gestion des cibles critiques

SG/DSEC/GOUV/MIV

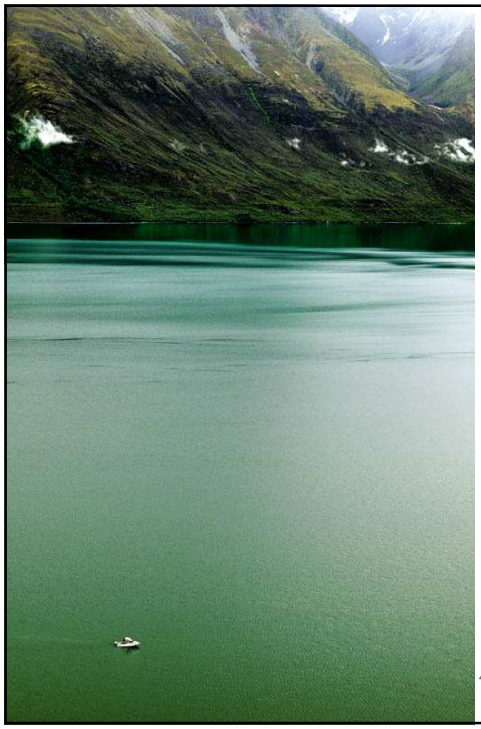
Juin 2008

- Pierre-Dominique Lansard
- Directeur Mission Infrastructures Vitales
- Direction de la Sécurité Groupe

- pierredominique1.lansard@orange-ftgroup.com
- +331 4444 7330

Sommaire

1. **Résilience: France Telecom est Opérateur d'Infrastructures Vitales**
2. **Le contexte de la Gestion de Continuité d'Activité**
3. **Critères Généraux de détermination des éléments critiques**
4. **Le risque de cyber-criminalité : La veille aujourd'hui chez France Telecom**



- 1. Resilience
- La capacité de survivre à l'interruption de composants majeurs

France Telecom est Opérateur d'Importance Vitale

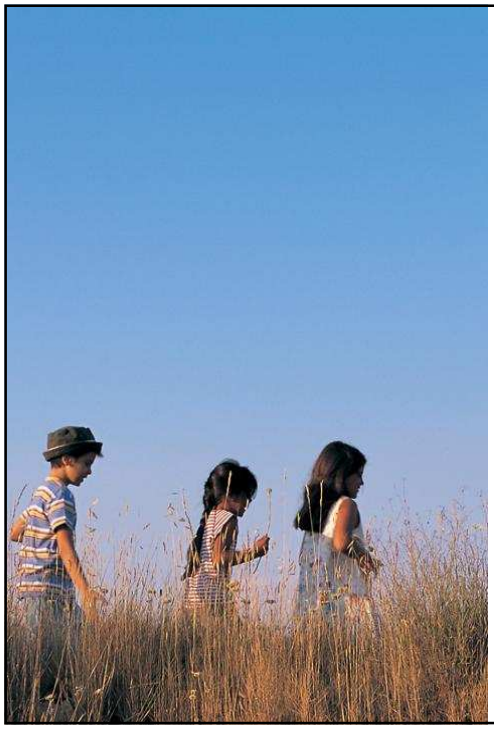
- **Le Cadre**
  - **Décret SAIV de Février 2006**
  - **Directive Nationale de Sécurité**
  - **Membre du Conseil National des OIV**
- **Les Obligations**
  - **Plan de Sécurité Opérateur**
  - **Gestion de la Continuité d'Activité**
  - **Gouvernance**

mesures pour assurer la résilience

- Le Développement en prenant les risques en compte
  - l'Architecture des Infrastructures
  - les Services
  - Le choix de composants robustes
- Les Opérations orientées Business
  - Qualité
  - Gestion de la Sécurité
  - Gouvernance
- Les Contrats gagnants-gagnants
  - Le niveau de Résilience des services est fournie par contrat en accord avec le niveau de prise de risque des clients

des orientations « marché » en lien avec la réglementation

- La sécurité est considérée comme un facteur de différentiation
- De puissants leviers pour la qualité (incluant la sécurité, la résilience) résultent des demandes des grands clients y compris les agences gouvernementales
- De nombreuses options sont possibles. Il n'y a pas de solution standard
- Un rythme de changement sans précédent quant aux aspects offres et demandes; La sensibilisation n'est pas symétrique.
- L'émergence de standards pour les bonnes pratiques



2.Le Contexte de la Gestion de la Continuité d'Activités

Une politique: La Gestion de la Continuité d'Activité

- Un futur standard avec un grand potentiel

La BS 25999 (du BSI) pour la GCA (BCM)

- Cinq briques majeures
  - La Connaissance de l'Organisation
  - Les Bilans d'Impact sur les Affaires (BIA)
  - Le rétablissement des lieux de travail
  - Le redressement après sinistre
  - La Gestion de Crise

● Planifié ● En tant que de besoin

actions: GCA, Gestion de Crise

- **La Gestion de la Continuité d'Activité**

  Une version adaptée de la BS 25999 est en cours de déploiement dans l'ensemble du Groupe France Telecom

- **La Gestion de Crise**

  a été jugée en 2005 trop dépendante de la technique, mal adaptée au nouveau contexte du Groupe et ne prenant pas assez en compte de nouveaux risques (pandémie, financiers,…).

  A l'été 2006, un nouveau cadre général pour la Gestion de Crise a été défini au niveau du Groupe.

  La déclinaison de ce cadre général est en cours dans toutes les entités du Groupe en tenant compte des spécificités Business et des particularités locales.

actions: Le PCA Pandémie

- Un PCA spécifique a été mis au point en lien avec le plan National Gouvernemental permettant de prendre en compte la dimension ressources humaines, pour déclinaison en France et dans les autres pays où le Groupe est présent.
- Ce PCA a été validé en 2006.
- C'est un véritable nouvevau challenge pour le Groupe

actions: un système de management de la sécurité

Une transformation majeure pour l'ensemble du Groupe

- 2006 Décision de développer un outil SMS conforme avec l'ISO 27 001.
  Plan, Do, Check, Act (PDCA)
- 2007 Questionnaires Globaux mis au point et premier retour des entités du Groupe.
  (sur les incidents de sécurité et les facteurs de sinistralité)
- 2007 Décision de déployer SMS pour l'ensemble des entités du Groupe reprise dans la PSG.
  (Politique de Sécurité Globale)
- 2008 Mars: Première Version du manuel SMS
- 2008 Début du déploiement

actions: la construction d'un service

Le Processus TTM (TIME TO MARKET) étapes obligatoires :

Etape	Action	Porteur
T0	Opportunité, inclue une évaluation générale du Risque	Equipes Marketing
T1	Définition, inclue une détermination du risque Sécurité	Equipes Techniques
T2	Construction	Equipes Techniques
T3	Déploiement	Equipes Techniques
T4	Exploitation	Equipes Operations
T5	Evaluation de la nouvelle offre	Equipes Marketing

Le niveau d'atteinte de la Résilience doit être prouvé aux étapes T0 et T1

- **3.Détermination des cibles**

Les cibles critiques

- **Est « critique » un processus, un équipement, une tâche qui est:**
  - **« essentiel » au sens de la GCA pour l'Entreprise**

  et/ou

  - **« vital » au sens des besoins de la Nation exprimés dans la DNS (Directive Nationale de Sécurité)**

- **Il en est de l'IT comme des autres composantes**

La détermination des cibles critiques

- **Fait l'objet d'un processus rigoureux et protégé**
- **Permet une connaissance approfondie de l'ensemble du Groupe**
- **Repose sur des critères de bon sens**
- **A pour finalité de minimiser le nombre des cibles potentielles**
- **Ecarte les cibles critiques appartenant de fait à d'autres acteurs de Secteur d'Activités d'Importance Vitale**

La protection des cibles critiques

- **s'inscrit dans le Plan de Sécurité de l'Opérateur**
- **fait l'objet d'un Plan de Protection Externe**
- **est suivie de très prêt par les services spécialisés**

- 4. **Le risque de cybercriminalité : La veille aujourd'hui chez France Telecom**

L'activité de veille sécurité

Observer

- en temps réel
- les produits et les infrastructures utilisés par le groupe

Analyser

- les vers, virus et les vulnérabilités
- les composants matériels ou logiciels
- réseaux, systèmes, applications, produits de sécurité …

Informer

- sur les vulnérabilités potentielles
- pour aider à la mise en place de mesures correctives
- pour réussir à limiter les impacts

La mission de la veille

Prévenir France Télécom des problèmes de sécurité

Couvrir tous les produits et services

Diffuser les informations en temps réel

Aider les MOE à analyser les impacts

Les services proposés

- Suivi & Diffusion des vulnérabilités
  - Publication sous différents formats
  - Alerte email par liste de diffusion
  - Site web du CERT-IST
- Les autres services …
  - Analyse de sécurité des produits logiciels ou matériels
  - Intégration de nouveaux produits dans la veille
  - Veille sécurité sur les produits et services Orange™
  - Déclaration de vulnérabilités aux organismes de veille

Le processus de veille

Veille & Gestion des correctifs

Contribution de la veille

- Deux processus distincts à forte synergie
- Avis de vulnérabilités
  Matière première de la gestion des correctifs
- Criticité des vulnérabilités
  ⇨ **Délais d'applications des correctifs**

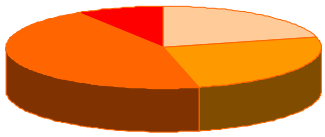
Veille & Gestion de crise

Rôle de la veille sécurité

- Supporter le processus de gestion de crise
  Information d'une attaque en cours
- **Observer & Analyser**
- Couvrir les risques en HNO
  Service de veille 7/7 du CERT-IST

La veille en quelques chiffres …

Pour l'année 2007



- Plus de **620** vulnérabilités traitées
- Une vulnérabilité critique concernant la LiveBox™
- Remontée de plusieurs vulnérabilités sur les portails Orange™
- Remontée de plusieurs dizaines de cas de phishing ou d'abus sur les portails internet Orange™
- Plus d'une dizaine de produits ajoutée dans la base Cert-IST

• 5. Questions ?


dziekuje
multumesc
ありがとう
gracias
謝謝
شكراً
thank you
dakujem
merci
orange