Forum 2006 du CERT-IST

Le Management de la sécurité, un enjeu stratégique

Philippe Duluc
Directeur de la Sécurité Groupe
de France Télécom
Secrétariat général

Diffusion Libre

Fil directeur

- Un environnement qui évolue de plus en plus vite
- La nécessité de globaliser la sécurité et de la gérer
- La convergence des managements de sécurité
- L'apport des CSIRT
- Quels nouveaux services?
- Perspectives

Diffusion Libre

La révolution de l'information

- La révolution d'Internet
  - **Le 5 décembre 1969 : Arpanet, 4 sites, 20 utilisateurs**
  - 1980 : 200 sites, 50 à 100 000 utilisateurs
  - 1990 : 300 000 sites, 2 à 3 millions d'utilisateurs
  - 2000 : 10 millions de sites internet et 60 millions intranet, 260 à 300 millions d'utilisateurs
  - **Le 8 juin 2006 : plus de 400 millions de sites, plus d'un milliard d'utilisateurs, soit plus d'un humain sur six**
- La révolution de la cryptologie asymétrique
  - Diffie-Hellman (1976, Stanford), Rivest-Shamir-Adleman (1978, MIT)
- L'avènement de la société de l'information : du techno-push au market-pull. Les grandes tendances :
  - interconnexion généralisée des réseaux entre eux, poussée par les usages et par la réduction des coûts
  - convergence IP : elle s'accélère (VoIP)
  - convergence fixe-mobile : elle arrive (**IMS** : *IP Multimedia Subsystem, **UNIK***)
  - **dynamisme et rapidité**

Un nouvel espace à civiliser

- Ces révolutions technologiques et la frénésie autour de l'information et la communication ouvrent un nouvel espace à l'activité humaine : le cyberespace
- De nouveaux horizons insoupçonnés :
  - MMORPG : 5 millions d'abonnés à **WoW**
  - une énigme littéraire Flaubertienne (1840) résolue par Google
  - **Wikipedia** : 3,8 millions d'articles (01/01), 13000 contributeurs, 5 milliards de pages consultées par mois, etc.
- De nouvelles incivilités et délinquances :
  - ver **Slammer** : le tour du globe en 10 minutes (2003)
  - botnet : un réseau de **100 000 PC** zombies (troyen W32-Toxbot) démantelé aux Pays-Bas (2005)
  - spam : le canadien Eric Head en a envoyé 94 millions en un mois (2004)
  - rootkit : 4,7 millions de CD musicaux Sony (2005)
  - malware PtoP à venir, etc.
- Ce nouvel espace ressemble au **Far West**, royaume de la gratuité, de l'abondance, de la liberté et des fortunes faciles. L'impunité peut encore y régner. La police et les autorités judiciaires doivent s'y adapter, et les comportements civiques s'y développer.

La sécurité globale

- De la sécurité informatique à la **sécurité de l'information**
  - standards britanniques, le CLUSIF change de nom, etc.
- On ne peut réduire la lutte contre les cybercrises à la seule SSI, la sécurité doit être globale
  - pas de sécurité globale si la sécurité physique n'est pas au niveau (contrôle d'accès, sécurité incendie, etc) : tentative avortée de vol de **220 millions £** à la Sumitomo Mitsui Bank de Londres en mars 2005 (keylogger)
  - pas de sécurité globale si le personnel n'est pas sensibilisé et formé : contre l'ingénierie sociale (par téléphone, par mail, **phishing**), aux procédures de traitement de l'information sensible (évaluation, marquage) ou de réaction aux crises (exercices, planification), etc.
- Elle doit être démontrable (auditabilité) à des clients, des assureurs, des autorités réglementaires, etc. le cas échéant par l'intermédiaire de tiers de confiance
- La dynamique de l'évolution de la société de l'information nécessite une adaptation permanente de la posture de sécurité globale

L'approche métier du SI

- Une adaptation permanente de la posture de sécurité globale
  - la sécurité de l'information doit s'inscrire dans une démarche d'amélioration continue similaire au **contrôle qualité**
  - W. Edwards Deming, père du contrôle qualité et du cycle perpétuel d'amélioration : **Plan/Do/Check/Act**
  - mise en place d'un système de management (***ISMS***)
- **ISO/IEC 27001** (BS 7799-2 R-U) novembre 2005 :
  - spécifications pour ISMS, inclut PDCA, donner l'assurance, via une certification, qu'un système a été implémenté suivant l'état de l'art
- Nécessite au préalable une définition du périmètre et une analyse de risques, plusieurs méthodes disponibles :
  - **EBIOS** (Fr), mais aussi CRAMM (R-U), ISF, IT Baseline (All), MEHARI (Fr) ,voire MELISA (Fr), OCTAVE (E-U), future ISO/IEC27005
- Bonnes pratiques de sécurité (**BS 7799-1**) ou plus générales orientées process (**ITIL**, *Information Technology Infrastructure Library*)

Approche gestion de risques

- **FERMA** (*Federation of European Risk Management Association*) : cadre de référence de la gestion des risques 2002
  - risque **=** probabilité d'occurrence **x** intensité des conséquences
  - approche d'origine britannique, couvrant tous types de risques et d'opportunités possibles : de cause interne ou externe, stratégiques, financiers ou opérationnels, etc.
- Approche utilisable pour la sécurité globale (uniquement risques) :
  - accepter, prendre les risques de sécurité **ou**
  - ne pas les prendre (si possible dans l'opération considérée) **ou**
  - réduire les risques de sécurité (probabilité d'occurrence et étendue des dégâts) et prendre les risques résiduels devenus acceptables **ou**
  - transférer les risques de sécurité (assurance, contrat client ou fournisseur) en totalité ou en partie (partager les risques de sécurité)
- Vision auditeurs (**ISACA**) : **COBIT** (*Control objectives for information and technology*), qui s'étend à la gouvernance des SI
- Vision métiers bancaires (**Bâle II**, Eur., 2004) : risques de crédit, risques de marché, et risques opérationnels (approche gestion de crise, BCP)

Approche gestion de crise

- Inéluctabilité de certaines crises, qu'elles soient d'origine naturelle ou criminelle (effets de seuil du modèle gestion de risques)
  - risques extrêmes de **Bâle II**
- Nécessité de planifier la continuité / reprise d'activité : tout système de management de la sécurité doit inclure cette dimension
- Standards
  - **NFPA 1600** (E-U, 1991) : disaster/emergency management et business continuity
  - **BS 25999** (R-U) : standard for business continuity management, reprend la norme PAS56 (R-U, Business Continuity Institute) et comptatible ITIL
    - partie 1 : code de bonnes pratiques
    - partie 2 : système de management
  - **ISO/IEC 24762** en gestation : *Guidelines for Information and Communication Technology Disaster Recovery Scenario*

Approche financière

- **Sarbanes-Oxley Act** (juillet 2002)
  - moralisation aux E-U suite aux scandales Enron et Worldcom
  - certification des comptes par les CEO et CFO qui encourent **personnellement** jusqu'à 20 ans de prison
  - pas de comptes solidement certifiés sans un SI bien sécurisé
  - cite l'usage du référentiel COSO (qualité du reporting financier))
- **COSO** (***COmmittee of Sponsoring Organizations*** *of the Treadway Commission*) : contrôle des processus financiers et mise en place du contrôle interne, a évolué en 2004 vers la gestion de risques : **ERM COSO** ou **COSO2** comprend 3 objectifs et 5 composantes :
  - *Concourir à la réalisation des 3 objectifs suivants :*
    - la réalisation et l'optimisation des opérations,
    - la fiabilité des informations financières,
    - la conformité aux lois et règlements.
  - *Analyser pour chacun de ces 3 objectifs les 5 composantes du contrôle interne suivantes :*
    - l'environnement de contrôle,
    - l'évaluation des risques,
    - les activités de contrôle,
    - l'information et la communication,
    - le pilotage du contrôle interne

Prestataires de services

- Les CERTs constituent des organismes indissociables de la sécurité des réseaux et de l'information
  - ver **Morris** le 2 novembre 88 : création du CERT-CC 15 jours après
- Évolution des services rendus, plus globaux et plus adaptés à l'évolution des usages : les CERTs deviennent des **CSIRTs** (*Computer Security Incident Response Team*)
- **ENISA** (voir http://www.enisa.eu.int/), 3 thèmes de travail 2005 :
  - **1)** sensibiliser à la sécurité de l'information dans les Etats membres
  - **2)** analyse de risques, management des risques : répertoire, bonnes pratiques
  - **3)** CERT – CSIRT
    - http://www.enisa.eu.int/doc/pdf/deliverables/enisa_cert_inventory_v1.2_060210.pdf
    - Inventaire des activités (jusqu'aux *abuse-team*) dans l'UE : une centaine de CSIRT répertoriés
- Analyse par le CERT-CC des nouveaux services (voir http://www.cert.org/archive/pdf/csirt-handbook.pdf)

Services possibles

- services **réactifs** : répondent directement à la révélation d'une compromission, d'une faille de sécurité ou d'un début d'attaque,
  - Alerte, analyse d'incident ou de vulnérabilité, examen postmortem, préservation de preuves, coordination en cours d'incident, conseil sur suites à donner, etc.
- services **proactifs** : aider à se préparer à la révélation d'une compromission, faille, attaque
  - Conseils ciblés ou thématiques, bonnes pratiques, veille technologique, audits de sécurité, configuration et exploitation des outils de sécurité, développement d'outils de sécurité adaptés, IDS (détection d'intrusion), tenue de référentiels de sécurité, etc.
- services de **management de la sécurité**
  - Analyse de risques, *business continuity planning*, *disaster recovery planning*, conseil, communication de sécurité, sensibilisation, formation évaluation de produits, etc.

Perspectives

- Convergence des systèmes de management liés à la sécurité
  - initiative de Business Software Alliance, RSA, Entrust : « information security gouvernance » (convergence COSO, BS7799), avril 2004
  - du COSO au ERM COSO (*enterprise risk management*), septembre 2004
  - ASIS, ISACA et ISSA ont formé **AESRM** « the alliance for enterprise security management », février 2005
  - étude Booz/Allen commanditée par AESRM : « convergence of enterprise security organization », novembre 2005
  - série des **ISO/IEC 2700x**
  - **convergence à venir : responsabilité sociale (IS0/IEC 26000)**
- On peut s'attendre à une évolution normative (d'origine anglo-saxonne) de tout le secteur s'appuyant sur de la certification par des tiers de confiance et sur de l'évaluation par des experts, dans un cadre général de responsabilité sociale d'entreprise
- Les CERT, ou plus généralement les CSIRT, seront des partenaires naturels dans cette évolution