

# La politique de sécurité

D'après le gestionnaire

# Introduction

- ▶ Depuis les années 2000, la sécurité informatique s'est généralisée dans les grandes structures
- ▶ Maintenant, même les petites structures sont sensibles à ces problèmes de sécurité
- ▶ L'objectif est de réussir à
  - ▶ Pérenniser le matériel
  - ▶ Rationaliser les investissements

## Quelques notions

- ▶ Une politique de sécurité exprime la volonté managériale de protéger les valeurs informationnelles et les ressources informatiques de l'organisation
- ▶ Elle spécifie les moyens (ressources, procédures, outils, ...)
- ▶ Evite que le système d'information ne devienne une cible et qu'il ne se transforme pas en un acteur d'attaques par prise de contrôle à distance
- ▶ Cette protection est assurée par exemple par
  - ▶ Des règles: classification de l'information
  - ▶ Des outils: chiffrement, firewall
  - ▶ Des contrats: clauses, obligations
  - ▶ Enregistrement, identification, tatouage, marquage
  - ▶ Le dépôt de marques, brevets et protection de droit d'auteur

# Le projet d'entreprise

- ▶ Sa validité en sera renforcée si l'organisation développe une éthique d'entreprise et si elle stipule également ses exigences
- ▶ La gestion des risques doit également être évaluée avec précision car elle guide toutes les décisions de sécurité
  - ▶ Qui doit être le responsable de l'analyse des risques, de la gestion des risques ?
  - ▶ Comment effectuer une telle analyse ?
  - ▶ Quels sont les outils et méthodologies disponibles ?
  - ▶ Quels sont leur niveaux de fiabilité ?
  - ▶ Quelle est l'importance à accorder aux résultats ?
  - ▶ Combien cela coûte ?
  - ▶ Faut-il externaliser cette fonction ?

# Des risques à la politique de sécurité

- ▶ Identification des risques: origine, cause, potentialité, impacts, effets, conséquences, gravité
- ▶ Risques subis, encourus ou de perte
- ▶ Après identification: faire une quantification
  - ▶ Quels sont les risques acceptables ?
  - ▶ Quels seront les risques pris ?
- ▶ Ensuite, il est possible de s'orienter vers une politique de sécurité

# Propriétés d'une politique de sécurité

- ▶ La définition de la politique de sécurité doit être
  - ▶ Simple et compréhensible
  - ▶ Adoptable par un personnel préalablement sensibilisé voire formé
  - ▶ Aisément réalisable
  - ▶ De maintenance facile
  - ▶ Vérifiable et contrôlable
- ▶ Elle ne doit pas être statique mais périodiquement évaluée et adaptée
- ▶ Elle doit pouvoir être configurable et personnalisable
  - ▶ « Accès aux jours ouvrés entre 7h et 20h » mais occasionnellement, accès le week-end

# La politique de sécurité

Normes et méthodes

# Principales méthodes

- ▶ Une démarche de sécurité traite de
  - ▶ l'organisation de la sécurité
  - ▶ de l'inventaire des risques relatifs aux actifs informationnels
  - ▶ de la définition d'une architecture de sécurité
  - ▶ de l'établissement d'un plan de continuité
- ▶ On débute par une check list des points à sécuriser
  - ▶ Politique de contrôle d'accès: gestion des identités, des profils, ...
  - ▶ Politique de protection: prévention des intrusions, vulnérabilités, ...
  - ▶ Politique de réaction: gestion des crises, des sinistres, ...
  - ▶ Politique de suivi: audit, évaluation, optimisation
  - ▶ Politique d'assurance

# Méthodes françaises

- ▶ Les méthodes préconisées par le CLUSIF (Club de la Sécurité de l'Information Français) sont MARION (Méthode d'Analyse des Risques Informatiques et Optimisation par Niveau) et MEHARI (Méthode Harmonisée d'Analyse des Risques). Les méthodes sont disponibles sur le site web du clusif: <http://www.clusif.asso.fr>
- ▶ La DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) propose une méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), téléchargeable sur son site web: <http://www.ssi.gouv.fr/fr/dcssi>
  - ▶ Cette méthode est adoptée par les administrations françaises

# Norme internationale ISO/IEC 17799

- ▶ La norme ISO 17799 adoptée par l'ISO à la fin de l'année 2000 est la norme BS 7799 élaborée par l'association de normalisation britannique en 1995
- ▶ Certaines compagnies d'assurances demande que les applications soient conforment à cette norme
- ▶ Elle est basée sur la gestion de risques et propose un code de pratique pour la gestion de la sécurité
- ▶ Cette norme peut être considérée comme un référentiel ou une liste de points de risques à analyser: un sorte de check list
- ▶ La version de 2000 traite de 10 domaines de sécurité, de 36 objectifs de sécurité et de 127 points de contrôle
- ▶ La dernière version de 2005 ajoute aux domaines de sécurité l'évaluation et l'analyse des risques, la gestion des valeurs et des biens ainsi que la gestion des incidents

# Les domaines de la norme ISO 17799

- ▶ Les 10 domaines de la version de 2000
  - ▶ Politique de sécurité
  - ▶ Organisation de la sécurité
  - ▶ Classification et contrôle des actifs
  - ▶ Sécurité et gestion des ressources humaines
  - ▶ Sécurité physique et environnementale
  - ▶ Exploitation et gestion de systèmes et de réseaux
  - ▶ Contrôle d'accès
  - ▶ Développement et maintenances des systèmes
  - ▶ Continuité de service
  - ▶ Conformité

# Méthodes et « meilleurs pratiques »

- ▶ L'AFAI (Association Française de l'Audit et du Conseil Informatique, [www.afai.asso.fr](http://www.afai.asso.fr)) diffuse une méthode de gouvernance et d'audit des systèmes d'information: la méthode CobiT (Control objectives for information and Technology)
  - ▶ Cette méthode peut être vu comme un outil pour optimiser des politiques, des mesures et des procédures de sécurité
- ▶ La méthode Octave élaborée à l'université de Carnegie Mellon (USA) est également adoptée par de nombreux consultants en politique de sécurité
- ▶ Les meilleurs pratiques qui peuvent également constituer des guides de référence sont celles du
  - ▶ CERT (<http://www.cert.org>): Guide to System and Network practices
  - ▶ NCSA (<http://www.ncsa.edu>): Guide to Enterprise Security
  - ▶ Internet Security Alliance (<http://www.isalliance.org>): Common sense guide for senior manager
  - ▶ Information Security Forum: The standard of good practice for senior manager

# La politique de sécurité

Mesures de sécurité

# Classification des ressources

- ▶ La réalisation d'un inventaire complet et précis de tous les acteurs de la chaîne de sécurité contribue à une meilleure connaissance et donc à la maîtrise de l'environnement à protéger
- ▶ L'analyse de l'existant et cet inventaire vont permettre de déterminer le degré de criticité de chacune des ressources et d'en faire une classification
  - ▶ C'est à dire son importance en cas de perte, d'altération ou de divulgation des données
- ▶ Pour chaque classe, il faut identifier
  - ▶ les risques possibles (erreur d'utilisation, de paramétrage, accidents, malveillance, sabotage, ... )
  - ▶ les mécanismes de sécurité applicables
  - ▶ Les contraintes techniques et organisationnelles afin de déterminer la faisabilité de la politique de sécurité pour chaque classe de ressources

# Degré de sensibilité

- ▶ Le degré de sensibilité d'une ressource, également appelé degré de criticité peut être défini de la façon suivante pour un entreprise
  - ▶ Ressources publiques: degré de sensibilité 0
  - ▶ Ressources financières: degré de sensibilité 1
  - ▶ Ressources privées: degré de sensibilité 2
  - ▶ Ressources secrètes: degré de sensibilité 3

# Mesures de sécurité

- ▶ Après identification des risques, des mesures de sécurité peuvent être mises en place
- ▶ Plusieurs types génériques de mesures de sécurité sont identifiés
  - ▶ Avant sinistre
    - ▶ Mesures préventives: détecteur d'intrusion, anti-virus, contrôle d'accès
    - ▶ Mesures structurelles: occultation des ressources, fragmentation de l'information afin de réduire la vulnérabilité des ressources
    - ▶ Mesures de dissuasion: peut être des protections juridiques ou administratives
  - ▶ Après sinistre
    - ▶ Mesures palliatives et correctives: les sauvegardes, plan de continuité, redondances
    - ▶ Mesures de récupération: limitent les pertes et réduisent les préjudices, utilisation d'assurance ou attribution de dommages et intérêts par des actions en justice

# Plan de secours

- ▶ Permet d'assurer un fonctionnement minimal des applications critiques après un sinistre
- ▶ Un plan de secours doit être suivi comme un vrai projet et suivre une vraie méthodologie qui pourrait être en 4 phases et audit

# Phase 1: analyse stratégique

- ▶ Analyse stratégique se structure autour de 4 grandes tâches
  - ▶ Organisation et conduite de projet
    - ▶ Identification de l'équipe, planification du plan de secours, formation et assistance
  - ▶ Analyse des risques
    - ▶ Évaluation des risques et définition des sinistres potentiels
  - ▶ Analyse d'impact
    - ▶ Identification des critères de fragilité et de sensibilité aux risques des applications
    - ▶ Analyse des conséquences des différentes pannes, ...
  - ▶ Définition des modes de fonctionnement normal et minimal de chaque application critique
    - ▶ Définition du délai maximal d'inactivité toléré, des consignes opérationnelles, des priorités de restauration, des procédures de reprise

## Phase 2: Analyse des solutions

- ▶ Identifier et évaluer les solutions de reprises possibles et de choisir la meilleure en fonction des critères stratégiques de l'entreprise
- ▶ C'est dans cette phase que l'on procède à la rédaction des documents définitifs

## Phase 3: mise en oeuvre opérationnelle

- ▶ Attribution des responsabilités, la sensibilisation et la formation des personnes responsables de l'exécution des procédures de reprise
- ▶ Une documentation complète du plan de secours doit être également établie

## Phase 4: validation et suivi

- ▶ Permet de tester le plan de secours, son efficacité par des simulations d'alertes et la réalisation de tests de bascule programmés
- ▶ Permet de documenter et analyser les résultats
- ▶ Permet de mettre à jour le plan et éventuellement de réorganiser la répartition des tâches aux membres de l'équipe

# Audit

- ▶ Peut faire partie de la phase 4
- ▶ Permet de déterminer la qualité du plan établi et d'élaborer des recommandations

# La politique de sécurité

Certification des produits de sécurité

# Critères communs

- ▶ En 1985, le département de la Défense américain définissait dans son orange book des critères d'évaluation de la sécurité des systèmes informatiques: TSEC, *Trusted Computer System Evaluation Criteria*
  - ▶ Associés à des jeux de tests effectués par le NCSC (National Computer Security Center), ces critères permettent de définir le niveau de sécurité d'un produit
- ▶ En 1987, un livre complémentaire intégrant la dimension réseau fut édité: le TNI (Trusted Network Interpretation)
- ▶ En 1991, les critères ont été repris au niveau européen: ITSEC (Information Technology Security Evaluation Criteria)
- ▶ Une mise en commun de tous ces critères ont donné naissance aux *Common Criteria for Information Technology Security Evaluation* en 1996
- ▶ Une version 2 est apparue en 1998 et donne lieu en 1999 à la norme ISO/IEC 15408
- ▶ Une version 3 des critères communs en Juillet 2005

# La norme ISO/IEC 15408

- ▶ Disponible sur le site <http://www.commoncriteriaportal.org> (document de plus de 500 pages)
- ▶ Cette norme se découpe en 3 parties:
  - ▶ Modèle général de la certification
  - ▶ Les exigences fonctionnelles de sécurité
  - ▶ Les exigences d'assurance de sécurité

# Les acteurs concernés

- ▶ 3 groupes de personnes sont concernés par les critères communs
  - ▶ Les évaluateurs
  - ▶ Les utilisateurs
  - ▶ Les développeurs

# Les niveaux d'assurance de sécurité

- ▶ 7 niveaux dit EAL (Evaluation Assurance Level) définissent la sécurité dans les critères communs.
  - ▶ EAL1: Testé fonctionnellement
  - ▶ EAL2: testé structurellement
  - ▶ EAL3: testé et vérifié méthodiquement
  - ▶ EAL4: conçu, testé et revu méthodiquement
  - ▶ EAL5: conçu et testé semi-formellement
  - ▶ EAL6: vérifié, conçu et testé semi-formellement
  - ▶ EAL7: vérifié, conçu et testé formellement

# Les limites des critères communs

- ▶ Le champ d'application et l'intérêt du label « certifié critères communs » restent faibles au regard de la lourdeur des démarches de certifications
- ▶ Le processus de certification d'un produit débute par la rédaction des documents à déposer en vue d'une accréditation
  - ▶ Cette procédure demande une formation par rapport à l'organisme vérificateur car chaque organisme a ses propres démarches
- ▶ Le processus est long et couteux, environ 1 an et 200 000 Euros
- ▶ La durée d'expertise peut inclure un décalage si une nouvelle version des critères communs sort
- ▶ Autres problèmes: certifié à un temps donnée, indépendance de l'organisme, une version précise de l'application ou un sous-ensemble est certifié, les produits n'ont pas besoin de répondre aux exigences de sécurité mais aux tests de conformité

# Les certifications professionnelles

- ▶ Les personnes en charge de la sécurité peuvent faire reconnaître leurs compétences en passant des tests de certifications professionnelles
  - ▶ CISSP de l'ISC2, ISSAP, ISSEP, ISSMP, GIAC, CISM de l'ISACA