Sécurité

- assurer la sécurité d’un système

  opportunités et obstacles

Sécurité

1. Constat
2. Approche
3. Méthodologie

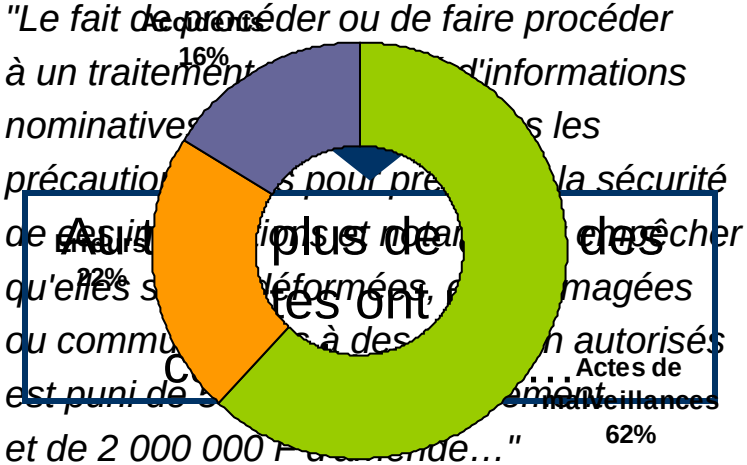
Constat

Des enjeux considérables

- Les pertes liées à l'informatique représentent aujourd'hui 0,2 à 0,4% du PIB des pays industrialisés
- **35%** des entreprises européennes ont subi au moins une attaque informatique l'an passé (source IDC)
- Une "valeur stratégique" de l'information de plus en plus critique pour l'entreprise (informations sur les clients, les produits, les contrats, les résultats financiers…) et une tendance au développement de la criminalité informatique qui ne cesse de croître depuis 10 ans
- Enfin, une responsabilité "lourde" pour l'entreprise

Que recouvrent les sinistres informatiques ?

"Le fait de procéder ou de faire procéder à un traitement d'informations nominatives sans les précautions pour préserver la sécurité de ces informations et notamment empêcher qu'elles soient déformées, endommagées ou communiquées à des tiers non autorisés est puni de 5 ans d'emprisonnement et de 2 000 000 F d'amende…"



***Source**: CLUSIF – APSAD*

Une réponse "technique" limitée

- Des solutions techniques, certes nécessaires, mais qui ne permettent de répondre que partiellement aux besoins des utilisateurs.
- Toutefois, les responsables ont besoin d'outils de diagnostic simples, rapides à mettre en œuvre et de conseils leur permettant d'améliorer efficacement le niveau de sécurité de leurs systèmes d'information.

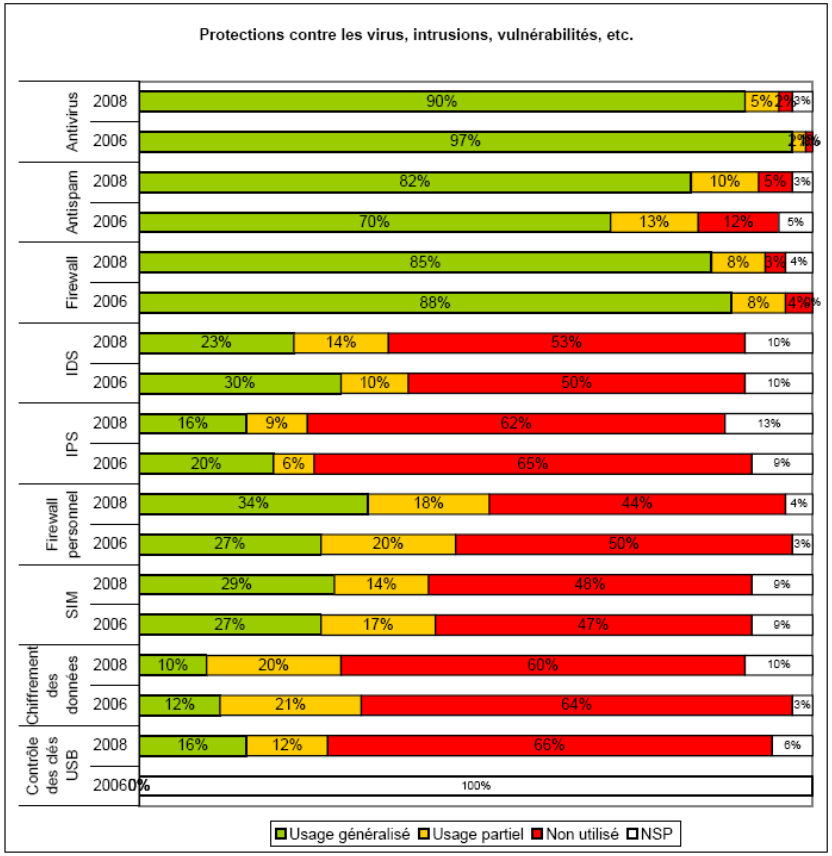


Figure 16 : technologies de sécurité / lutte antivirale, anti-intrusion, gestion des vulnérabilités

Source : Clusis 2008

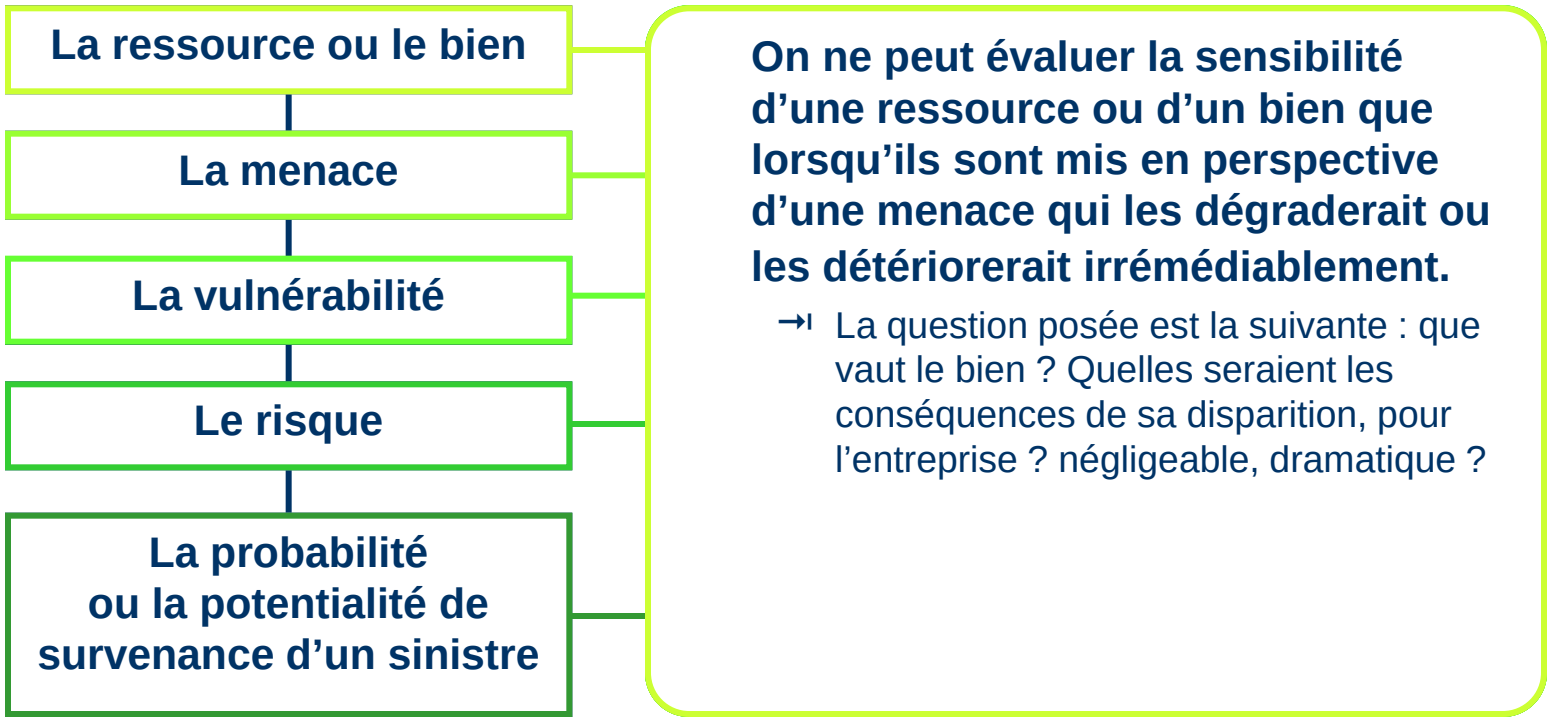
Approche

Une démarche globale portée par l'entreprise

- La sécurité est une question d'esprit, de culture d'entreprise et de comportement. Il est évident que la sécurité repose d'abord sur les hommes et l'organisation, elle nécessite un encadrement et un effort permanent.
- La participation complète et active de chacun des collaborateurs de l'entreprise s'obtient par une politique de communication qui maîtrise ses effets sur les hommes, comme dans tout autre domaine de la gestion.
- Dans tous les cas, le personnel doit être informé des règles et procédures de sécurité en vigueur dans l'entreprise (charte de sécurité, règlement intérieur, voire clauses particulières au contrat de travail) et doit être parfaitement conscient de ses obligations et des conséquences (disciplinaires, pénales) encourus en cas de manquement à ces dispositions.

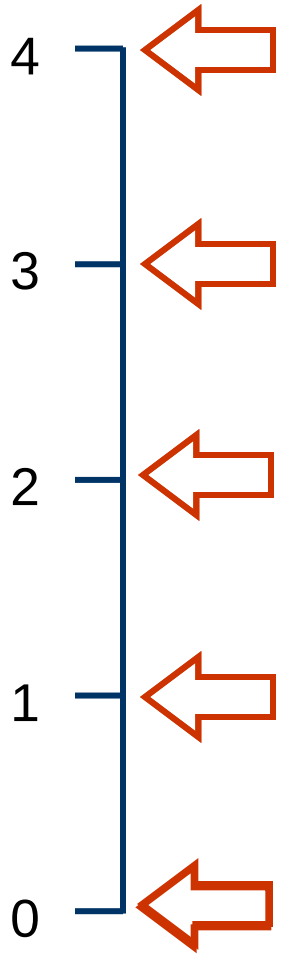
Une approche méthodologique "systémique"

- La sécurité des systèmes d'information doit être examinée selon cinq points de vue différents :



- Aucun des items énuméré n’a de valeur intrinsèque. Ils n’ont un sens que s’ils sont examinés en perspective des autres items. C’est cette vision interactive qui fonde la politique générale de sécurité sur la spécificité des enjeux propres à l'entreprise.
- Un niveau de sécurité basique appliqué uniformément à l’ensemble des informations, ne peut satisfaire aux exigences spécifiques de sécurité des composantes sensibles des systèmes. Une approche discriminante permet de faire porter principalement les efforts de sécurité sur les ressources ou les biens jugés particulièrement sensibles, avec une optimisation des ressources et des investissements engagés.
- La méthode consiste à sélectionner les ressources ou biens sensibles (criticité égale ou supérieure à 3 dans l’échelle de gravité ci-après).

Échelle de criticité : 0 = nulle / 4 = maximale



- Criticité : 4
  - Tout événement susceptible d'entraîner la cessation immédiate (ou rapide) et totale d'une activité de l'entreprise ou d'entraîner des sanctions pénales.
  - Tout événement susceptible d'entraîner une perte importante de clientèle.
  - Tout événement susceptible d'être considéré comme une infraction majeure à la législation.
  - Tout événement pouvant entraîner une nuisance organisationnelle jugée significative par l'utilisateur.
  - Tout événement susceptible de nuire aux décisions et orientations de l'établissement.

Un exemple de scénario de risque : Coexistence des documents papier et des documents technologiques

Inefficacité organisationnelle en gestion de l'information.

- Outils actuels parfois inadaptés à cette situation.
- Risque de perdre des documents administratifs, légaux et financiers.
- Perte possible de la mémoire institutionnelle.

Besoin de sécurité

Adapter le système de numérisation et faire le choix des documents à numériser en fonction des besoins de votre organisme.

Documenter le processus de numérisation.

Vérifier la qualité et la quantité de la numérisation.

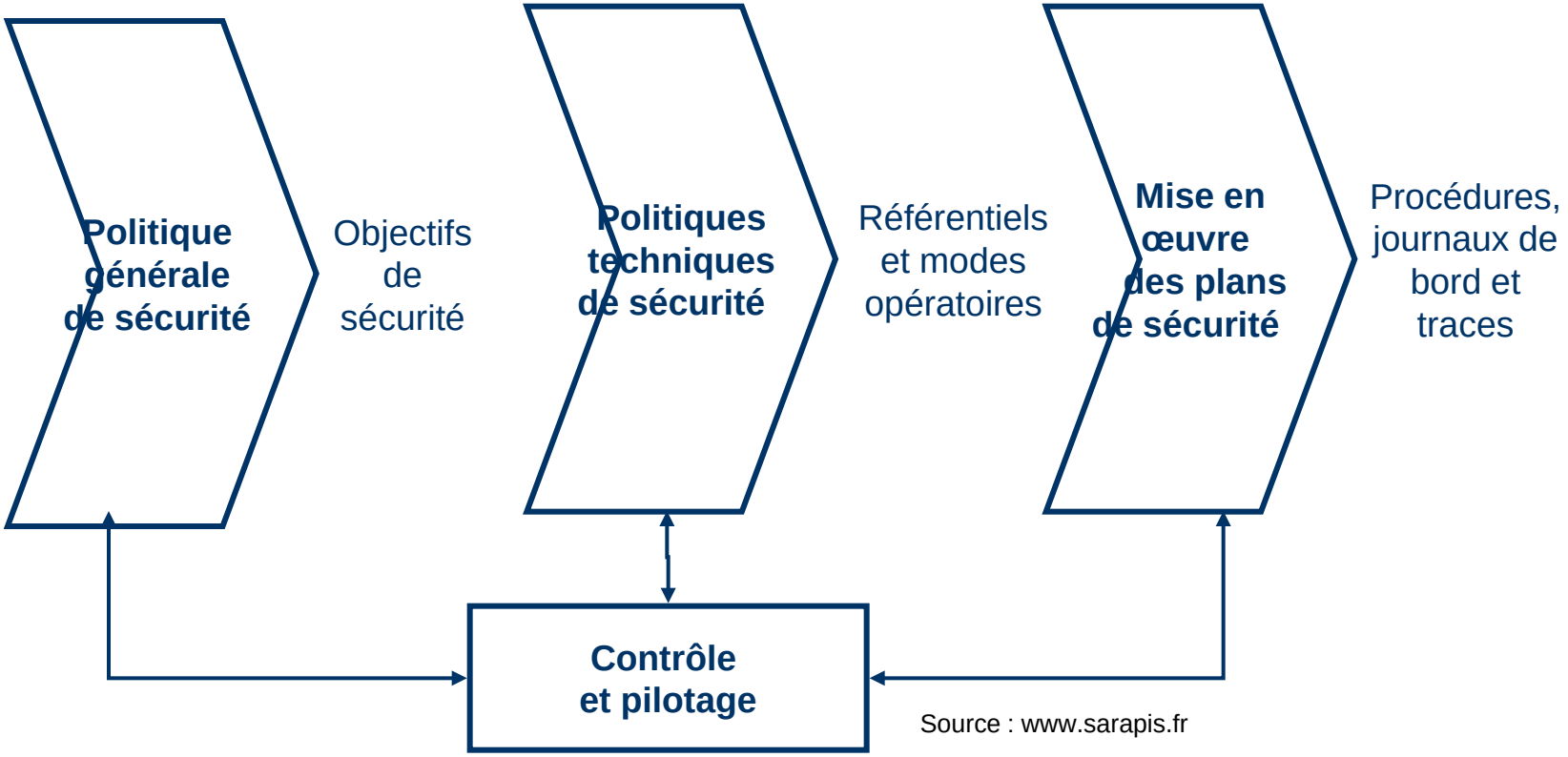
Mettre à jour et faire approuver les règles de conservation concernées.

La sécurité ou l'art de gérer le risque

- Notre méthodologie consiste à :
  - ➡ Définir un modèle de sécurité permettant de répondre à 3 questions de fond :
    - Quelles sont les menaces qui visent l'information en regard des enjeux ?
    - Que doit on protéger ?
    - Et pourquoi ?
  - ➡ Ce modèle intègre à la fois les risques commerciaux, financiers, pénaux, réglementaires, sociaux ainsi que le risque de perte d'image.
  - ➡ Appliquer une méthode globale et transversale,
  - ➡ Viser la conformité à la norme ISO IEC 2700x.
- Les orientations proposées visent la cohérence du dispositif tant sur les plans de la sécurité logique que physique et organisationnelle.

Méthodologie

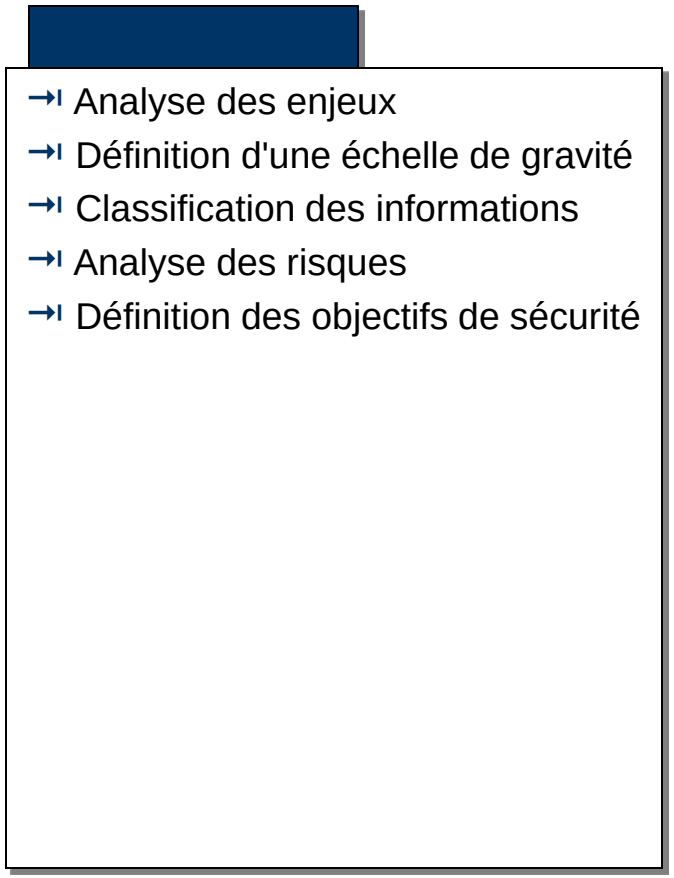
Une approche transversale et globale en 4 étapes



Source : www.sarapis.fr

La politique générale de sécurité

- Le rapport de politique générale de sécurité du système d'information constitue le référentiel de l'entreprise :
  - Il rappelle les objectifs de sécurité fixés par la direction générale,
  - Il indique les moyens à mettre en œuvre à travers les plans techniques de sécurité afin de satisfaire ces objectifs,
  - Il démontre le soutien et l'engagement de la direction en ce qui concerne la sécurité.
- La politique générale de sécurité est élaborée en procédant à une analyse des risques en regard des enjeux qui s'imposent à l'entreprise.



Les Politiques Techniques de Sécurité

- Définir l'ensemble des éléments organisationnels, opérationnels et techniques relatifs à un domaine technique ou fonctionnel du système d'information.
- Les directives, règles et modes opératoires à respecter dans l'entreprise sont constitués en référentiels.

- Organisation de la sécurité
- Intégration de la sécurité dans les processus de Conduite de projet, Conception, Développement et Intégration de logiciels
- Intégration de la sécurité dans les processus d'exploitation
- Plan de sécurité système
- Plan de sécurité réseaux
- Plan de continuité des activités de l'entreprise, plans de secours
- Infrastructure à clé publique
- Plan de communication sécurité

Mise en œuvre des plans de sécurité

- Les procédures et les règles traduisent les politiques techniques de sécurité.
- La journalisation et les traces des opérations informent sur leur application.

- Elaboration de règlement
- Conception et élaboration des procédures
- Élaboration de chartes de sécurité
- Elaboration de clauses contractuelles
- Conception des tableaux de bord
- Conception et élaboration des journaux de bord
- …

4

Audit et contrôle interne

- Le but du contrôle interne est de vérifier la bonne application des procédures de sécurité et de donner l'assurance raisonnable de la maîtrise des risques par les moyens mis en œuvre.
- Le contrôle Interne relève du Responsable Sécurité et de l'encadrement de l'entreprise.
- Le système de contrôle permet :
  - De vérifier la bonne application des procédures, règles et directives,
  - D'avoir une parfaite visibilité sur le pilotage de la sécurité dans un contexte de technologies en évolution,
  - D'adapter la politique de sécurité à l'évolution de l'architecture du système d'information et des menaces

- Audit de la sécurité de l'information en référence aux normes ISO 2700x
- Audit de vulnérabilités
- Audit de progrès sur le processus sécurité
- Audit de conformité :
  - des plans d'action aux politiques techniques de sécurité
  - des politiques techniques aux objectifs de la politique générale de sécurité
- Conception du dispositif de contrôle (organisation, fonctionnement)
- Méthodologie et d'outils d'élaboration
- des procédures
- Modélisation et élaboration des procédures

Questions ?

Merci