Quel audit de Sécurité dans quel contexte ?

Hervé Morizot (herve.morizot@solucom.fr)

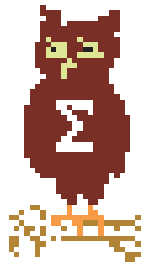
09 avril 2002

Agenda

- Quel audit ?
- Selon quelle démarche et avec quels outils ?
- Une "stratégie d'audit"
- Conclusion

I Quel audit ?

Quel audit ?
Quelques définitions ...



- Audit
  - Mission d'examen et de vérification de la conformité (aux règles) d'une opération, d'une activité particulière ou de la situation générale d'une entreprise
- Système d'Information
  - Ensemble des moyens matériels, logiciels et organisationnels qui permettent de recevoir, de stocker et de traiter l'information
- Donc un audit nécessite :
  - Un périmètre
  - Un référentiel
  - Une méthode
  - Des moyens et compétences

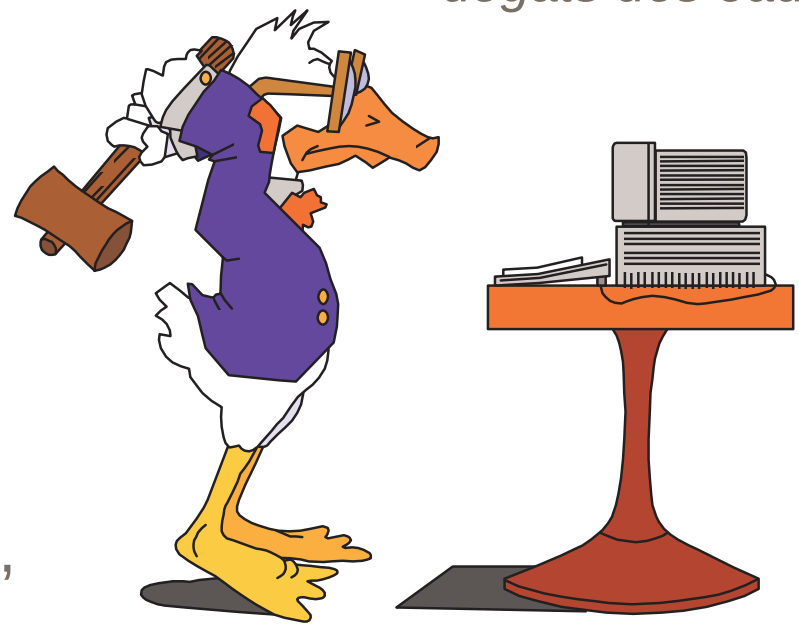
Quel audit ?
Les risques ...

Malversations
et fraudes

Accidents
(incendie,
dégâts des eaux, …)

Divulgation,
desinformation

Pannes



Sabotages
(*physiques et logiques)*

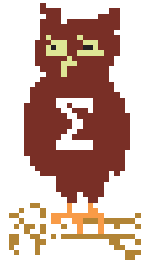
Erreurs
(conception,
utilisation,
exploitation)

Engorgement,
dénis de services,
...

...

- Particulièrement variable selon les environnements -

Quel audit ?
Des besoins très variés ...

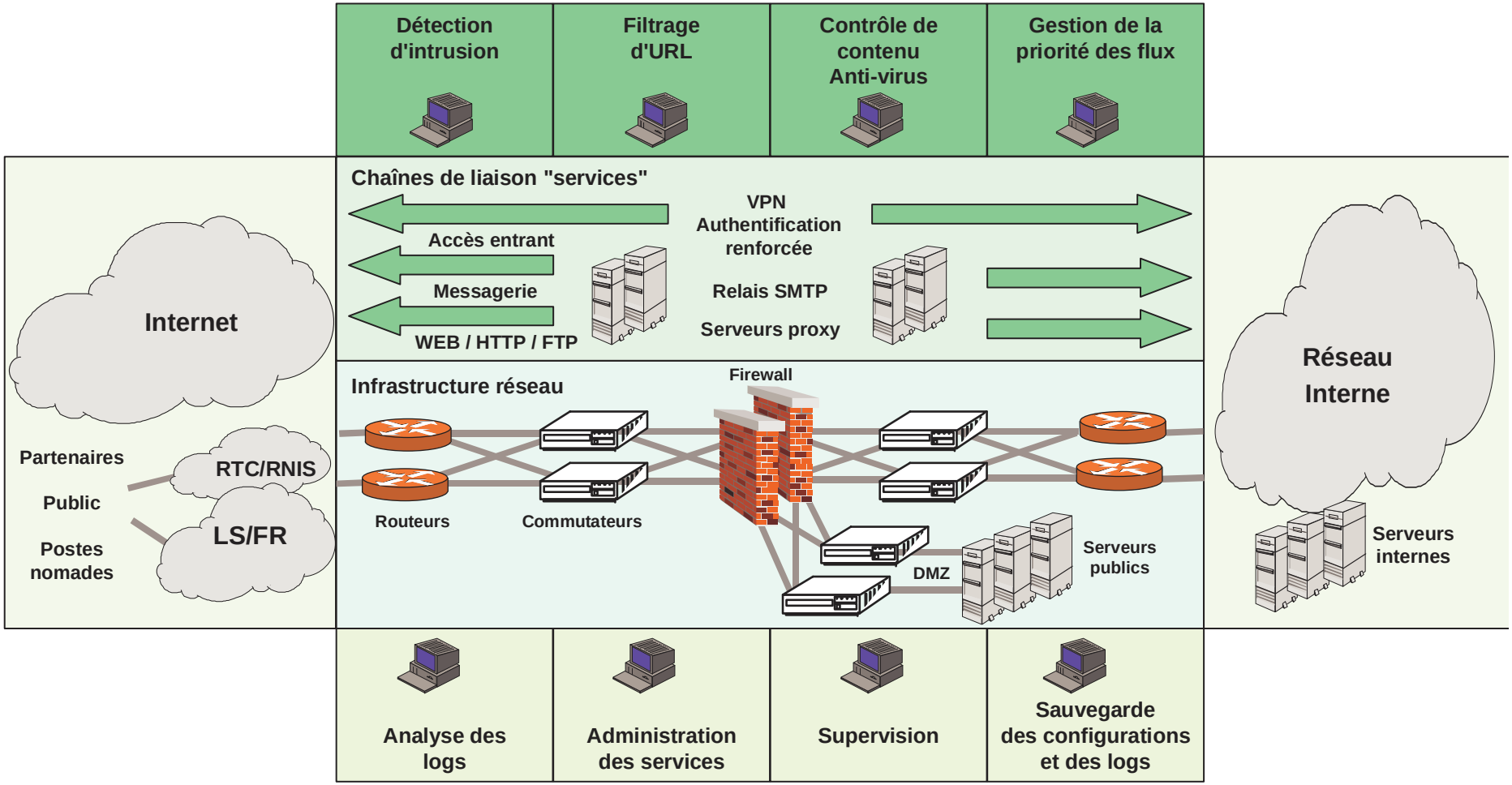


- Évaluer / comparer
- Améliorer
- Sensibiliser
- Analyser, sur incident
- Certifier / prouver
- ...

Quel audit ?
Quel périmètre *(1/2)* ?

- Le périmètre organisationnel et fonctionnel
  - Organisation de la sécurité
    - La répartition des responsabilités
    - La sensibilisation / formation des intéressés
    - Contrôle et audit
  - Politique et les guides de sécurité
  - Procédures de sécurité
  - Respect de la législation en engagements contractuels
- La sécurité physique
- Les procédures d'administration / exploitation
  - Gestion des habilitations / accès
  - Sauvegardes et secours
- La sécurité des systèmes et applications

Quel audit ?
Quel périmètre *(2/2)* ?

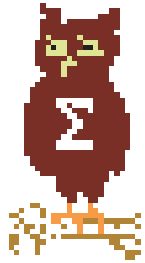


II Selon quelle démarche et avec quels outils ?

Selon quelle démarche et avec quels outils ?

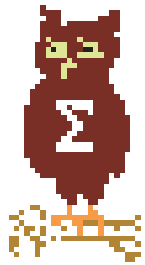
- Pour auditer, il faut :
  - Un besoin clairement exprimé
  - Un périmètre bien défini
  - *Une méthode formelle …*
  - *Des outils …*
  - Des moyens et des compétences
  - …

Selon quelle démarche et outils ?
Les méthodes (1/4)



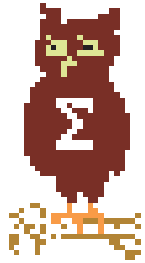
- Quelle méthode ?
  - Les méthodes "globales"
    - Mehari
    - EBIOS
    - Marion
    - Melisa
    - ...
  - Les méthodes "propriétaires"
  - *Les auto - évaluations ...*
  - *Les évaluations / certification ...*
  - Sans méthode formelle
  - ...

Selon quelle démarche et outils ?
Les méthodes (2/4)



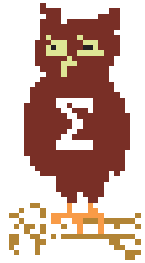
- Les méthodes "globales"
  - Pourquoi une méthode ?
    - Être efficace
    - Être crédible
    - Se comparer
    - ...
  - Oui, mais ...
    - C'est trop lourd !
    - C'est pas adapté !
    - C'est théorique (*analyse et plan d'action*) !
    - ...
- Les méthodes "propriétaires"
  - Objectif : personnaliser et simplifier ...

Selon quelle démarche et outils ?
Les méthodes (3/4)



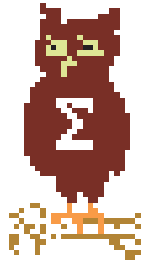
- Les auto-évaluations
  - Léger
  - Excellent en sensibilisation
    - Implication des intéressés
  - Exige un référentiel rodé *(détaillé, clair, didactique, ...)*
  - Demande confiance / engagement formel du "signataire"
  - Demande des contrôles *(aléatoires, par priorité, ...)*
  - Mais :
    - Difficile dans des environnements hétérogènes
    - Les résultats dépendent du "type de répondant"
    - Les plans d'actions sont aussi en majorité à décentraliser ...

Selon quelle démarche et outils ?
Les méthodes (4/4)



- Les évaluations / certifications
  - Mandat d'un CESTI
    - Agréés par la DCSSI et accrédité par le COFRAC
    - Encore orienté "matériel" (*chiffrement, cartes à puce, ...*)
    - Des conditions de développement encore "floues"
    - Un démarrage lent (*une poignée de CESTI en France*)
    - Un avenir potentiellement prometteur (*signature électronique, ...*)
  - Nécessite des documents formels
    - Profil de protection
    - Cible de sécurité
    - Cible d'évaluation

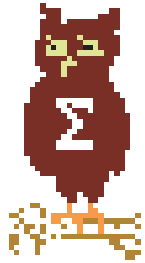
Selon quelle démarche et outils ?
Les outils (1/5)



- Quels outils ?
  - Outils méthodologiques

    Attention aux limites de l'automatisation !
  - *Référentiels de sécurité*
  - *Tests de configuration ...*
  - *Tests de vulnérabilité ...*
  - *Tests d'intrusion ...*
  - ...

Selon quelle démarche et outils ?
Les outils (2/5)

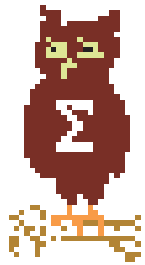


- Les référentiels de sécurité
  - La Politique de sécurité de l'entreprise
  - Les guides de sécurité par environnement
  - Les normes applicables
    - ISO 17799
    - ...

Pertinents pour déterminer le "référentiel"

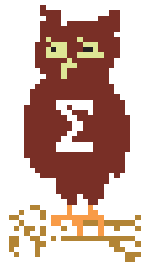
et les questionnaires associés

Selon quelle démarche et outils ?
Les outils (3/5)



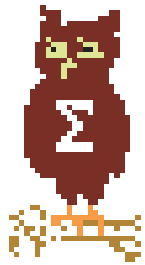
- Les tests de configuration "système"
  - Outils pour NT, W2K, UNIX, Mainframe ... *(ESM de Symantec, System Scanner de ISS, W2K, logiciels libres, ...)*
  - Nécessite de définir sa politique technique de sécurité / pas d'analyse de failles ...
  - Différents modules sont disponibles *(mots de passe, protection d'accès, configuration LAN, niveaux de patchs, ...)*
  - Non intrusif, ni perturbateur
  - Modulaire et progressif
  - Nécessite une forte expertise pour la configuration

Selon quelle démarche et outils ?
Les outils (4/5)



- Les tests de vulnérabilités "réseaux"
  - Outils publics *(Nessus, Satan, ...)* ou commerciaux (*NetRecon de Symantec, Internet Scanner de ISS, ...)*
  - Utilisent des bases de vulnérabilités et des bases de recommandations
  - Indiquent des vulnérabilités "potentielles" / potentiellement intrusif
  - Demande une adresse / plage(s) IP, domaine NT, ...
  - Nécessite une expertise
  - Utilisé par les "hackers" ...

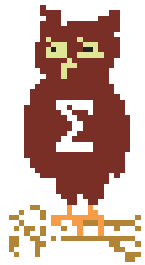
Selon quelle démarche et outils ?
Les outils (5/5)



- Les tests de vulnérabilités en ligne
  - Pléthore d'offres en mode ASP
  - Vision externe uniquement et test de réactivité des équipes
  - Bases de vulnérabilités à jour, complètes, Plug in spécifiques
  - Coût d'investissement "réduit"
  - Service "complet", récurent, peu d'implication client
  - Chacun a sa méthode de restitution / notation
  - Intrusif possible mais non souhaité
  - Rapports très (trop ?) automatisés
    - Prestations complémentaires ...

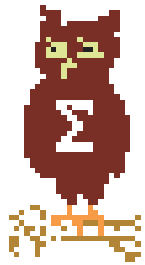
III Une "stratégie" d'audit sécurité

Une stratégie d'audit (1/2)



- Évaluation **globale** de la sécurité du SI
  - Dans le cadre d'une ré-organisation (*rachat, refonte, …*)
    - Audit complet, indépendant, méthode "incontestable"
  - Dans un cadre de consolidation globale de la sécurité
    - Analyse des risques souhaitable *(fonctionnels / techniques / juridiques)*
    - Plan d'actions détaillé et "participatif"
    - Audits réguliers à large périmètre
  - Dans le cadre d'une mise en cohérence de la sécurité
    - Comparaison site à site ou vis à vis de "la profession"
    - Méthode rigoureuse et applications régulières
  - Dans le cadre d'une sensibilisation
    - Audits participatifs / auto évaluation
  - Dans le cadre d'une obligation *(Administrations, …)*

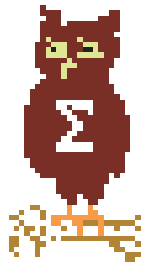
Une stratégie d'audit (2/2)



- Évaluation "par composant" (*projet, système, …*)
  - Évaluer la sécurité d'un composant du SI
    - Sécurité d'un produit (*objectif commercial / marketing*)
      - **Évaluation Critères Communs**
    - Qualifier / recetter / labelliser / …
      - **Méthode interne / ISO 17799 / …**
  - Analyser, sur incident
    - Sur mesure …
    - Nécessite une très forte expertise technique
  - …

Conclusion

Conclusion



- Le "sur mesure" est indispensable
  - Définir ses besoins et en déduire sa stratégie
  - Mettre en œuvre les recommandations
- Approche technique ou fonctionnelle ?
  - Les outils automatisés sont utiles, voire indispensables
  - Oui mais
    - Ils offrent une photo à un instant T mais pas dans le temps ni sur les cas "exceptionnels"
    - Il faut les paramétrer et exploiter les résultats
    - Ils ne couvrent pas tout le périmètre *(organisation, procédures, juridiques, traitement des incidents, …)*
    - Ils ne sensibilisent pas
  - Donc des audits "organisationnels", voire fonctionnels sont aussi indispensables
    - *Organisation / responsabilités, principes, procédures, analyse de risque, respect des obligations juridiques, …*
- Une double compétence s'impose …