Chapitre III :

Audit de sécurité

Préparé par : Hajer Gahbiche

Plan

1.1 Définition de l’audit de sécurité

1.2 Objectifs de l’audit de sécurité

1.3 La démarche d’un audit

Définition de l’audit de sécurité [1]

- Un audit de sécurité consiste à valider les moyens de protection mis en œuvre au regard de la politique de sécurité.
- Un audit de sécurité consiste à s'appuyer sur un tiers de confiance (généralement une société spécialisée en sécurité informatique).
- L'audit identifie les points forts, et points faibles (vulnérabilités) d’un système.
- L'auditeur dresse une série de recommandations pour supprimer les vulnérabilités découvertes

Objectifs de l’audit de sécurité

- L' audit de sécurité à pour objectifs :
  - Analyser les risques aux quels est exposé le système d’information
  - Proposer des recommandations et un plan d'actions pour corriger les vulnérabilités
  - Réduire l'exposition aux risques

La démarche d'un audit [1]

- Un audit d'un système est composé par trois phase :
  - L'audit organisationnel
  - L'audit technique
  - L'audit intrusif

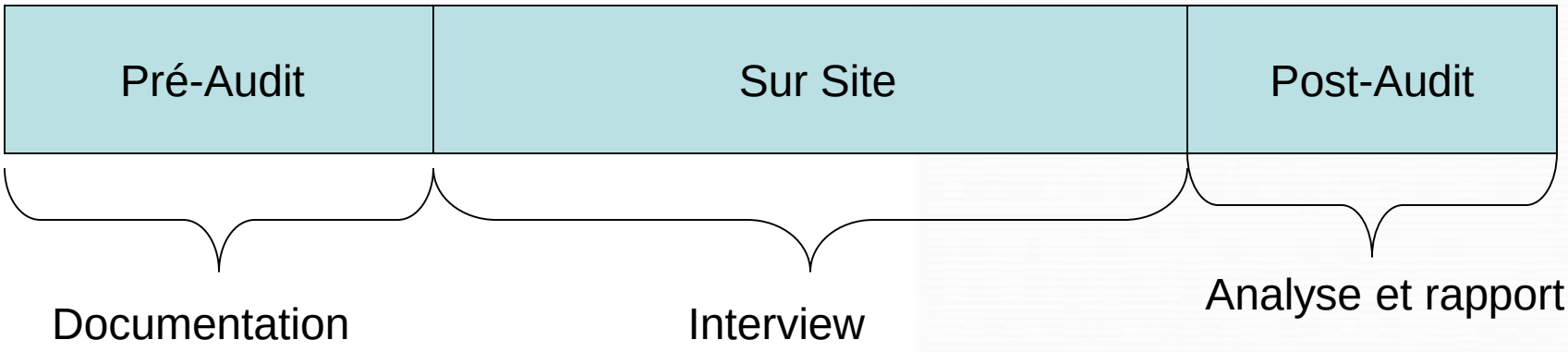
- Chaque phase est dépendante de la phase précédente.

- On ne peut pas passer d'une phase à une autre sans avoir à valider la phase précédente.(on ne peut pas faire un audit intrusif, sans avoir fait l'audit technique)

L’audit organisationnel

- Au niveau de cette phase, il n’y a pas d’utilisation d’outils/logiciels ou de test de vulnérabilités.
- Les objectifs de l’audit organisationnels sont:
  - L’identification des données et des processus critiques à protéger.
  - L’identification des failles du système d’information, ainsi que leur impact.
  - Le développement d‘une stratégie pour la réduction des risques
  - Implémentation de cette stratégie.

Déroulement de l'audit organisationnel (1/2)



•**Documentation** : cette phase consiste à donner aux auditeurs la documentation sur : l'architecture réseau utilisée au niveau de la société, le type d'application utilisée (base de données, serveur Web,..), le nombre de poste clé…

Déroulement de l'audit organisationnel (2/2)

- **Interview:** au niveau de cette phase les auditeurs essaient de déterminer comment les utilisateurs exploitent :
  - leur ordinateur (mots de passent, système d'exploitation, connexions Internet, les logiciels utilisés au niveau de chaque ordinateurs),
  - les applications de la société,..

- **Analyse et rapport:** au niveau de cette phase les auditeurs donnent à la société considérée un rapport contenant
  - les faiblesses du système d'information (telque par exemple : mauvais emplacement des équipements d'interconnexion, les utilisateurs doivent se connecter à Internet à travers le proxy et non à travers une clé 3G..)
  - Les recommandations pour remédier à ces faiblesses

Approches de l’audit organisationnel

»Approche descendante

»Approche ascendante

Approche ascendante (Bottom-UP)

- Avantages : Mise en œuvre rapide
- Inconvénients : Manque de précision et de complétude
- Préalables : Connaître
  - » Quoi protéger
  - » Contre Qui
  - » A quel degré

Création du profil d‘un attaquant :

- •Cibles intéressantes pour un éventuel attaquant
- •failles organisationnelles exploitables.
- •Vulnérabilités des systèmes critiques

Analyse de l‘existant

- • Politique de sécurité
- • Architecture réseau,
- • Architecture de sécurité.

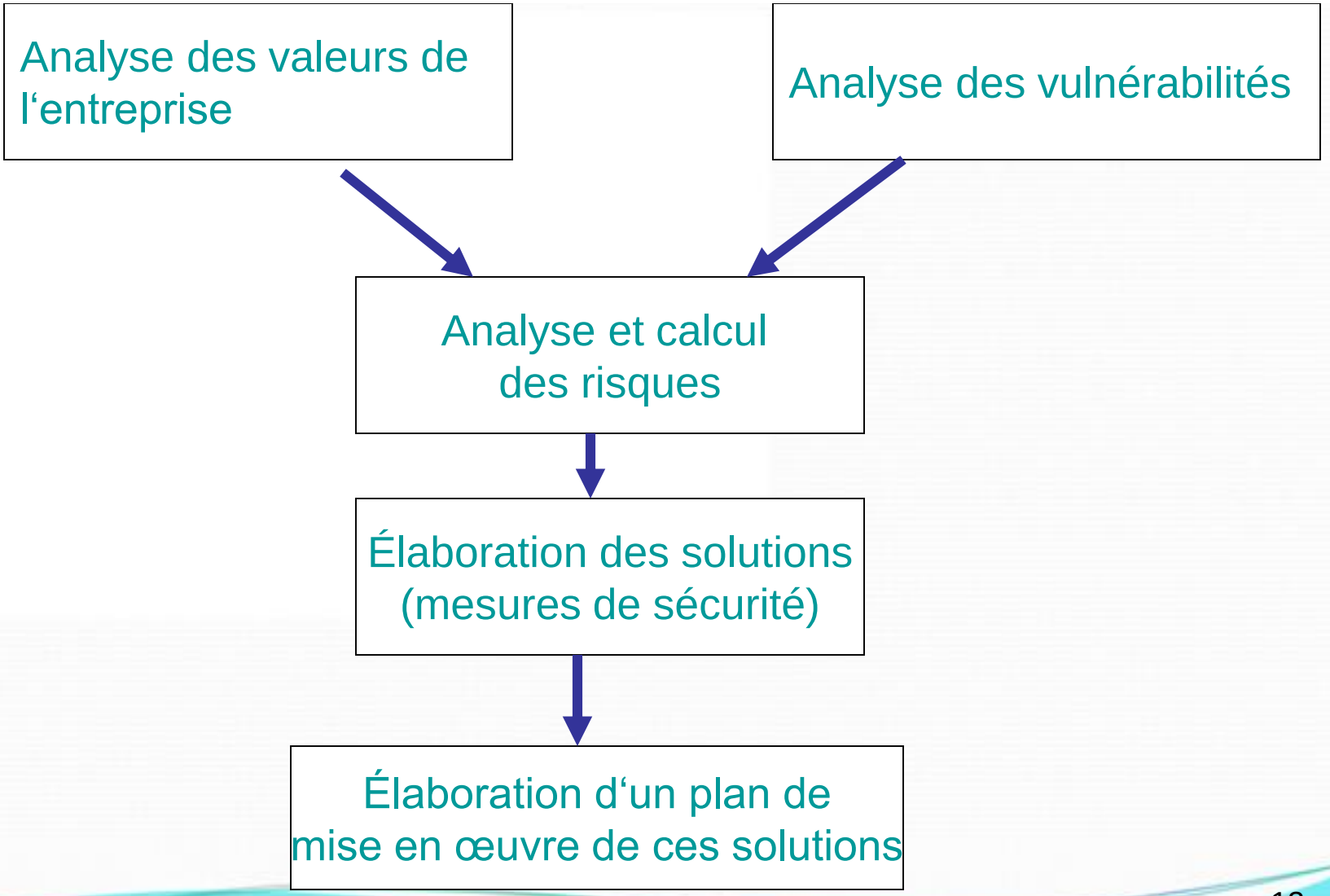
•Identification des failles majeures

- • Modification des aspects organisationnels à travers le responsable de la sécurité du système d’information, ..)
- • La définition d‘une politique de sécurité formelle
- • La sensibilisation et formation des utilisateurs/exploitants.

Approche descendante (Top-Down)

- Avantages : Complétude
- Inconvénients : Coût et durée de mise en œuvre.
- Pas de préalables

Approche descendante (Top-Down)



La démarche d'un audit

Un audit d'un système est composé par trois phase :

- L'audit organisationnel
- L'audit technique
- L'audit intrusif

L’audit technique (1/2)

- Cette phase de l’audit nécessite une grande expertise technique.
- Au niveau de cette phase, les auditeurs:
  - Valident de l’architecture réseau décrite par le responsable du système d’information.
  - Valident la politique de sécurité de cette société
  - Utilisent des logiciels libres, comme ceux qui sont utilisés par les hackers , pour voir l’impact de cette utilisation sur le système d’information
  - Déterminent techniquement les failles possibles du système d’information (exemple de failles : la non utilisation d’un firewall, le serveur Web peut être attaquer à travers l’injection SQL, …)

L’audit technique (2/2)

- À la fin de cette phase les auditeurs mettent en place techniquement les mécanismes de sécurisation nécessaire au niveau de la société exemple :
    - Déploiement d’un firewall
    - Déploiement d’un serveur proxy
    - Sécurisation des serveurs Web, de bases de données…

La démarche d'un audit

Un audit d'un système est composé par trois phase :

- L'audit organisationnel
- L'audit technique
- L'audit intrusif

L’audit intrusif

- Au niveau de cet phase de l’audit les auditeurs simulent des attaques sur la société de l’extérieur.
- Cette phase de l’audit est inutile si l’audit organisationnel, ou l’audit technique n’a pas été réalisé.
- Les auditeurs doivent garantir la non perturbation du fonctionnement du système, lors des tests intrusif.

Annexe

Responsable de la Sécurité du Système d'Information (RSSI)

- Le RSSI doit :
  - Assurer l'intégrité, la cohérence et la confidentialité des données de tout le système d'information.
  - Optimiser l'infrastructure de sécurisation et assurer la veille technologique dans le domaine.
  - Assurer la sensibilisation et formation des employés.

Politique de sécurité

- C’est un ensemble de règles qui régissent la manipulation des informations et des ressources sensibles.
- Elle Constitue un guide de bonnes pratiques et précise les risques et responsabilités