Sécurité des Systèmes d'Information

CM1: Principes Fondamentaux

Sommaire

Sommaire

1. SI et réseaux informatiques

Avec le développement d'internet, de plus en plus d'entreprises ouvrent leurs systèmes d'informations et il faut :

- connaître les ressources de l'entreprise à protéger ;
- maîtriser les contrôles d'accès ;
- maîtriser les droits des utilisateurs ;
- contrôler l'ouverture de l'accès de l'entreprise sur internet.

Les réseaux informatiques constituent la base qui va relier l'entreprise au monde extérieur et ils permettent :

- d'accéder au SI ;
- de stocker des données ;
- d'utiliser des outils métiers ;
- ...

Assurer la sécurité du SI c'est assurer la sécurité du réseau sur lequel il repose !

Problèmes :

- il est très souvent négligé ;
- perçu uniquement comme un moyen de relier l'entreprise avec ses différents intervenants ;
- les décideurs ne votent pas le budget nécessaire pour qu'il soit correctement implémenté ;

Depuis quelques années:

- lois ***Sarbanes-Oxley*** et accords ***Bâle II*** (US) ;
- loi sur la Sécurité Financière (***LSF***) en France ;

→ obligent les dirigeants à rendre des comptes aux actionnaires par le biais de bilans

→ ils ne faut pas négliger la sécurité des réseaux informatiques qui renferment les données des bilans

La contrainte sécuritaire donne naissance à une nouvelle fonction au sein des entreprises :

Responsable de la **S**écurité du **S**ystème d'**I**nformation (***RSSI***)

Le RSSI :

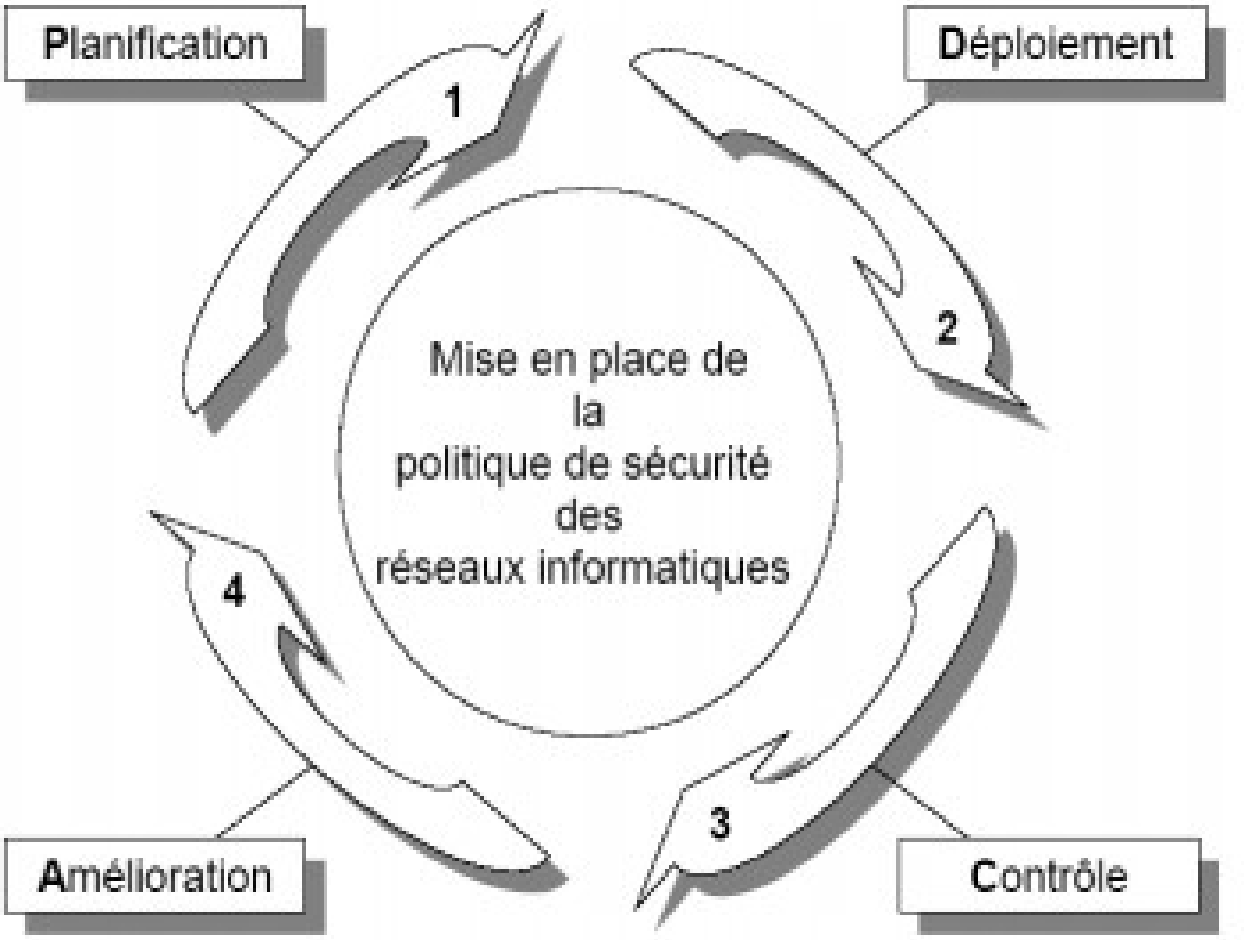
- est un manager ;
- inscrit la sécurité de l'information dans un programme de management ;

Le rôle du RSSI :

- déployer les mesures ;
- prendre les dispositions ;
- mobiliser les hommes ;
- qualifier les outils et les moyens ;

Pour assurer la sécurité.

Le RSSI peut mener son projet avec une approche de type PDCA :



L'approche PDCA se décompose en quatre phases :

- Planification : elle consiste à préparer un programme et un calendrier en fonction des objectifs fixés ;
- Déploiement : elle doit donner les moyens financiers, techniques et humains définis dans la phase de planification ;
- Contrôle : vérifie que les objectifs fixés dans la phase de planification sont bien mis en place et s'il ne le sont pas, à calculer les écarts ;
- Amélioration : elle sert à mettre en place les actions correctives qui vont permettre de diminuer les écarts calculés dans la phase précédente.

2. Problématiques spécifiques

La politique de sécurité réseau comprend les domaines suivants :

- audit des éléments physiques, techniques et logiques constituant le SI de l'entreprise ;
- sensibilisation des responsables de l'entreprise et du personnel aux incidents de sécurité ;
- formation du personnel utilisant les moyens informatiques du SI ;
- **structuration** et **protection** des locaux abritant les systèmes informatiques ;

La politique de sécurité réseau est une démarche impliquant toute ou partie de l'entreprise :

→ la définition d'un périmètre d'application doit être faite pour qualifier les parties critiques du réseau (à sécuriser).

→ le déploiement de la politique de sécurité se fait progressivement pour que l'entreprise ne se retrouve pas mobilisée pour cette tâche.

La définition du périmètre est **très** importante et déterminera la réussite du projet !

Expérience d'Alexandre Fernandez-Toro

→ British Telecom (BT) s'est lancé dans plus de 20 certifications ISO 27001 simultanément ;

→ mauvaise définition du périmètre qui a rallongé le temps d'obtention ou fait échouer les certifications ;

- ingénierie et maîtrise d'œuvre des projets, qui doivent inclure les contraintes de sécurité dès leurs phases de conception ;

- définition du cadre juridique et réglementaire de l'entreprise à l'égard de la politique de sécurité et aux actes de malveillance ;

- classification des informations de l'entreprise selon différents niveaux de confidentialité et de criticité.

3. Notions protégées par la PSSI

L' identification est l'information qui permet d'indiquer qui une personne prétend être :

- nom d'utilisateur ;
- empreintes digitales ;
- analyse faciale ;
- analyse rétinienne ;
- ...

L'authentification est l'information qui vient valider l'identification :

- faible → mot de passe ;
- forte → combinent une chose possédée et une chose connue (eg. carte bancaire / code personnel).

L'autorisation est l'information permettant de déterminer à quelles ressources de l'entreprise une personne authentifiée est autorisée à accéder et les actions qu'elle peut entreprendre.

La confidentialité est l'ensemble des mécanismes permettant qu'une communication de données reste privée entre un émetteur et un destinataire :

La cryptographie ou le chiffrement, IPsec (couche 3 OSI) et SSL (couche 7 OSI) sont les seules solutions fiables pour garantir la confidentialité des données.

L'intégrité est l'ensemble des mécanismes qui permettent d'assurer qu'une information n'a pas été modifiée.

La disponibilité est le fait de garantir que les ressources de l'entreprise sont accessibles :

- réseau ;
- bande passante ;
- ...

La non-répudiation permet de garantir qu'un message a bien été échangé entre un émetteur et un destinataire.

La traçabilité est l'ensemble des mécanismes permettant de retrouver les opérations réalisées sur les ressources de l'entreprise constituant le SI.

L'application de la PSSI est confrontée aux trois contraintes suivantes :

- Contrainte technique ;
- Contrainte économique ;
- Contrainte politique.

La contrainte technique est liée aux limites de la technologie → certaines applications sont difficilement filtrables ou ne tolèrent pas les remplacements d'adresse (eg. H323 pour la VoIP ou Ipsec pour les VPNs)

Une contrainte économique peut surgir et oblige alors à choisir une solution moins onéreuse.

Si cette nouvelle solution ne répond pas aux besoins de sécurité → **acceptation des risques**.

Le décideur devra disposer d'une **synthèse des risques** qui correspond à une description des menaces associées à leurs probabilités d'occurrence et leurs conséquences.

La contrainte politique survient souvent sans justification technique ou logique et peut engendrer de gros problèmes de sécurité qui doivent être suivis d'une acceptation de risques de sécurité.

Le risque en terme de sécurité est généralement caractérisé par l'équation suivante :

$$risque = \frac{menace \times vulnérabilité}{contre-mesure}$$

- la menace : représente le type d'action susceptible de nuire dans l'absolu ;
- la vulnérabilité, appelée parfois faille ou brèche, représente le niveau d'exposition face à la menace ;
- la contre-mesure est l'ensemble des actions mises en œuvre pour prévenir la menace.

4. La **P**lanification

La phase de planification est composée de quatre parties :

- la vision ;
- les objectifs de sécurité ;
- les moyens ;
- la stratégie de mise en œuvre.

La vision est la représentation partagée, décrite en termes précis et qui permet de qualifier le futur souhaité.

→ nécessite un état des lieux
→ recenser tous les biens de l'entreprise
→ évaluer leurs importances.

Une fois cette « représentation partagée » décrite et validée par la **direction générale**, elle servira de ligne directrice sans **aucun consensus possible**.

Les objectifs de sécurité sont élaborés grâce à une échelle de besoin qui va permettre d'associer un objectif à une importance.

Une fois les objectifs de sécurité définis, les actions à entreprendre apparaissent clairement et il est temps de leur associer des moyens.

Les moyens sont la **partie la plus critique** car ils arrivent à un moment où le projet est souvent embryonnaire et où la visibilité est faible.

→ dimensionnés pour atteindre les objectifs ;
→ fonction d'une stratégie de mise en œuvre.

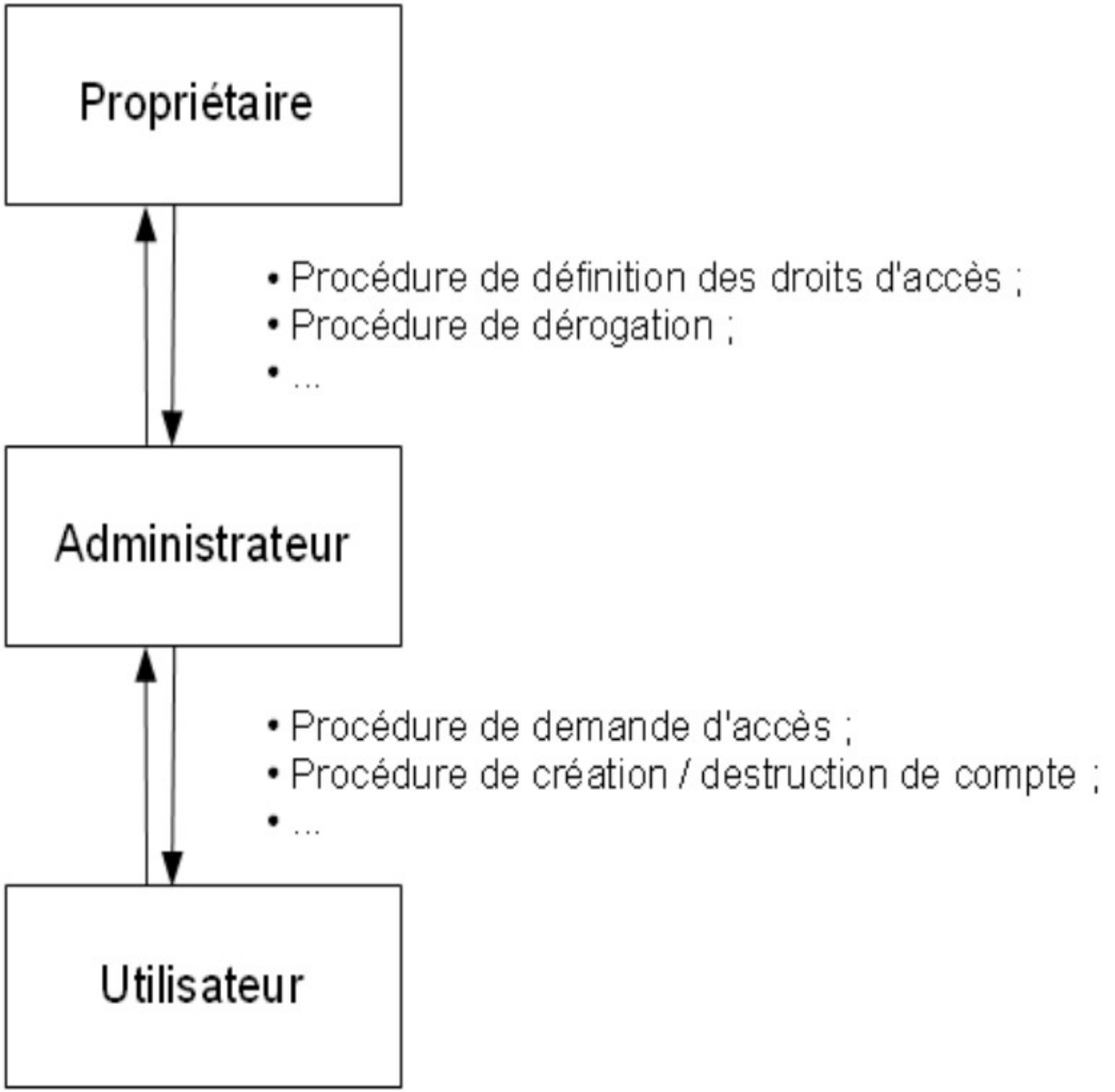
La stratégie de mise en œuvre est le chemin qui permet de passer de la situation actuelle à la vision

→ représente les modes d'actions et d'allocation des moyens.

Le principe de propriété exige que la PSSI décrive pour chaque ressource de l'entreprise un propriétaire fonctionnel.

Le propriétaire se porte garant :
- garant de la pérennité ;
- garant de la protection ;
- dicte les conditions d'accès à sa ressource.

La **P**lanification : principe de propriété



Le principe de propriété fait intervenir :
- un propriétaire ;
- un administrateur ;
- un utilisateur.

Le propriétaire définit les règles d'utilisation de la ressource et les donne à l'administrateur.

L'administrateur est en charge de les appliquer à la demande d'un utilisateur. Il peut demander une dérogation aux droits d'accès au propriétaire.

Cela garantit une certaine **indépendance** de **l'administrateur** face à **l'utilisateur** qui n'est jamais en contact direct avec le propriétaire de la ressource.

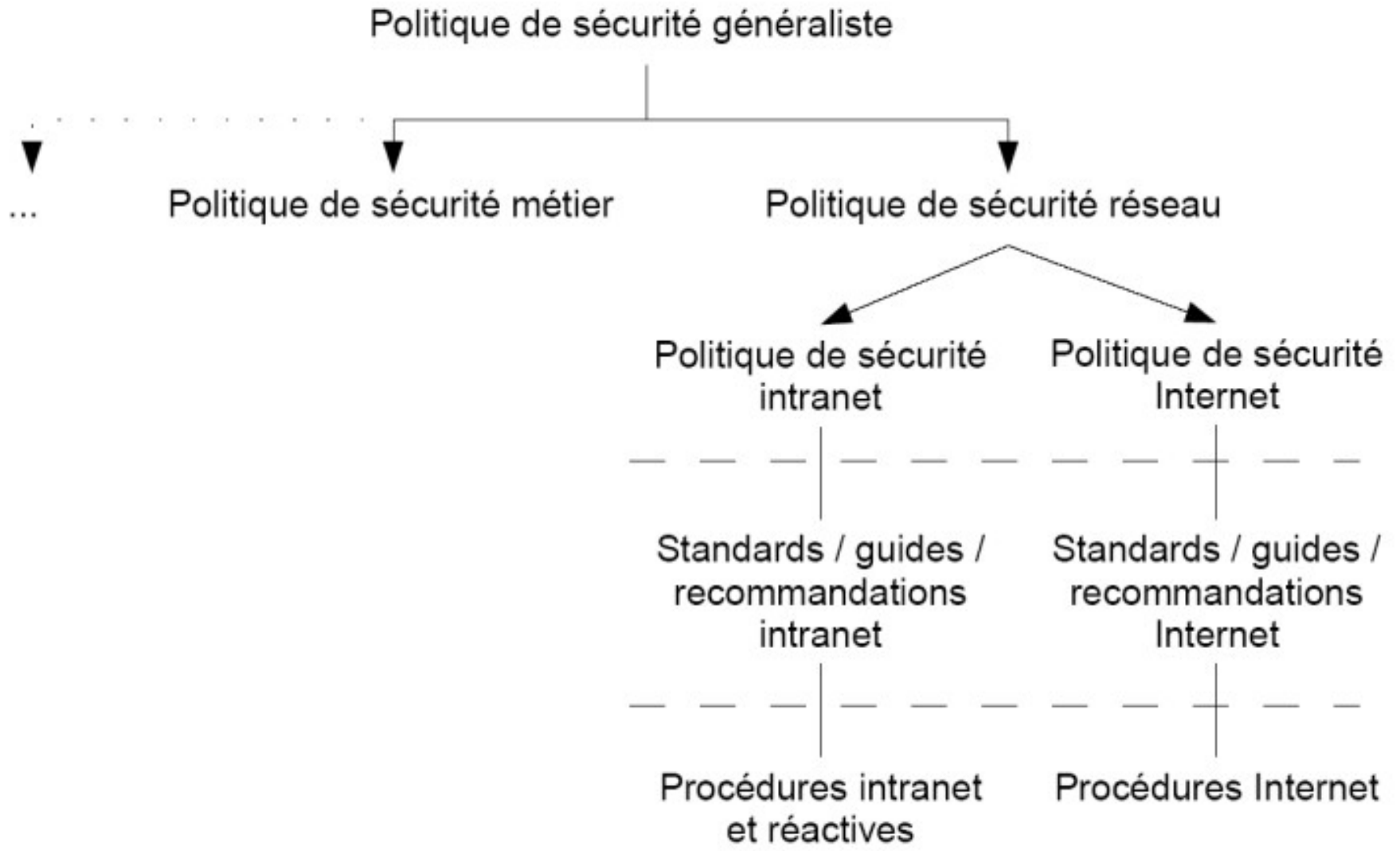
La découpage d'une PSSI en différents niveaux n'est pas chose facile et demande une parfaite connaissance du domaine visé.

Seule l'expérience de l'entreprise et de son historique permet d'éviter les pièges et de ne retenir que les éléments principaux et critiques pour son fonctionnement.

La politique de sécurité réseau est généralement éclatée en trois niveaux composés :

- d'une politique générale de sécurité de l'entreprise ;
- de standards, guides et recommandations de sécurité ;
- de procédures de sécurité.

La **P**lanification : découpage



5. Le **D**éploiement

La phase de déploiement peut être mise en place grâce à l'utilisation d'un « framework ».

Ce « framework » met en place l'éventail de documents qui composent la politique de sécurité « cadre » et le panel opérationnel.

Les méthodes de déploiement, appelées stratégies de sécurité, vont permettre d'implémenter les objectifs spécifiés dans la politique de sécurité.

Un « framework » est une structure basique permettant la résolution de problèmes complexes.

C'est un guide de recommandations de **haut niveau**, qui va ensuite être décliné en plusieurs guides et règles pour traiter les sujets suivants :

- organisation et management ;
- ressources humaines ;
- gestion de projets ;
- gestion des accès logiques ;
- exploitation et administration ;
- vérification des configurations ;
- sécurité physique ;
- plan de désastre ;
- vérification de l'application de la PSSI.

Organisation et management

→ une politique de sécurité doit faire partie intégrante de la stratégie de l'entreprise.

→ l'implication et le support du management sont primordiaux car la sécurité a des impacts sur les projets informatiques en terme de priorité, de ressources.

→ définition d'un comité constitué des dirigeants de l'entreprise

Ressources humaines

La politique de sécurité nécessite l'implication des salariés.

→ le facteur humain dépasse souvent les aspects purement techniques.

→ les contrats d'embauches doivent inclure un paragraphe relatif à la politique de sécurité de l'entreprise.

→ les cadres juridiques et réglementaires doivent être connus de tous.

→ des procédures disciplinaires doivent être définies suite à l'implication d'un salarié dans un acte de malveillance.

Gestion de projets

La politique de sécurité doit tenir compte des évolutions des produits et services de l'entreprise afin de coller à la réalité.

→ la gestion de projets doit tenir compte de la politique de sécurité et intégrer les contraintes de sécurité.

→ les procédures de développement des produits et services doivent tenir compte de la politique de sécurité dès la phase de conception.

→ des tests de non régression doivent être définis lors du développement et ont pour unique objectif de valider que le niveau de sécurité préalablement défini reste valide.

Gestion de projets

→ les éléments « hardware » et « software » nécessaires au développement des produits doivent être connus et approuvés et tout élément critique doit être clairement identifié.

→ l'environnement de développement des produits et services doit être sécurisé et les accords avec des tierces parties clairement définis.

→ la documentation relative aux projets informatiques est accessible au personnel de l'entreprise, classée en fonction de la confidentialité et maintenue à jour.

Gestion des accès

Le volet le plus dur à mettre en place, compte tenu de l'importance des facteurs humains et des procédures de gestion associés.

→ La gestion des accès logiques repose à 90% sur des aspects organisationnels et à 10% sur des aspects techniques.

→ Il est nécessaire de définir au préalable les rôles et besoins d'accès associés aux ressources de l'entreprise, puis d'attribuer à chaque utilisateur un ou plusieurs rôles pour définir ses droits d'accès. (**principe de propriété**)

→ toutes les activités d'un utilisateur vers des ressources critiques sont chiffrées, authentifiées et sauvegardées à des fins d'investigation, notamment en cas d'incident de sécurité.

Exploitation et administration

L'exploitation des services de l'entreprise suit un ensemble de procédures opérationnelles afin d'en assurer l'intégrité et la sécurité à moyen terme.

→ procédures opérationnelles à jour pour la supervision des éléments critiques et pour la maintenance préventive

→ une sauvegarde des informations critiques doit être effectuée dans un lieu physique distinct de la source.

→ les problèmes doivent être connus de tous et sont remontés en particulier par les procédures opérationnelles aux responsables des domaines visés.

Vérification des configurations

Les configurations des équipements réseau détiennent toute l'information permettant de construire le réseau et ses services.

→ des règles de sécurité génériques doivent être définies pour garantir la disponibilité et l'intégrité des services.

→ la configuration des équipements doit être consistante c'est à dire que tout élément de configuration doit être appliqué et tout élément appliqué doit être vérifié.

Sécurité physique

La sécurité physique consiste essentiellement à se protéger contre les vols, fuites d'eau, incendies, coupures d'électricité et autres problèmes qui pourraient nuire au fonctionnement du SI.

→ une salle informatique n'est jamais installée au rez de-chaussée pour éviter les risques d'inondation en cas de brusque montée des eaux.

→ plusieurs **périmètres de sécurité** physique à accès restreint équipés d'appareils de vidéo surveillance peuvent être définis et les ressources les plus critiques doivent être installées dans le périmètre le plus sécurisé.

Plan de contingence

Les éléments critiques doivent faire partie d'un plan global de contingence dont le but est de protéger le périmètre de l'entreprise.

→ temps de restauration d'un service après désastre

→ impacts : de perte de revenus ou d'image de marque.

Audit de la sécurité

→ audit interne par l'équipe de sécurité ;

→ audit externe par une tierce partie.

Primordiale pour s'assurer du degré d'application ou de déviation de la politique de sécurité réseau.

→ identifie les vulnérabilités techniques et organisationnelles.

Ce « framework » permet d'identifier les processus qui composent l'entreprise, un peu comme le ferait une certification ISO 27001.

L'objectif est d'accroître l'efficacité en proposant une approche transversale.

Prenons comme exemple l'embauche d'un nouvel administrateur de serveurs de mails :

1) La Direction des Ressources Humaines (DRH) définit la procédure avec laquelle le service informatique va pouvoir définir la fiche de poste.

2) Une deuxième procédure indique que pour les postes rattachés à la Direction du Service Informatique (DSI), les entretiens d'embauche sont menés avec un employé de la DRH et un autre de la DSI.

3) Pour assurer sa fonction d'administrateur de serveurs de mails, le nouvel embauché a besoin d'accéder à la salle machine où se situent les serveurs.

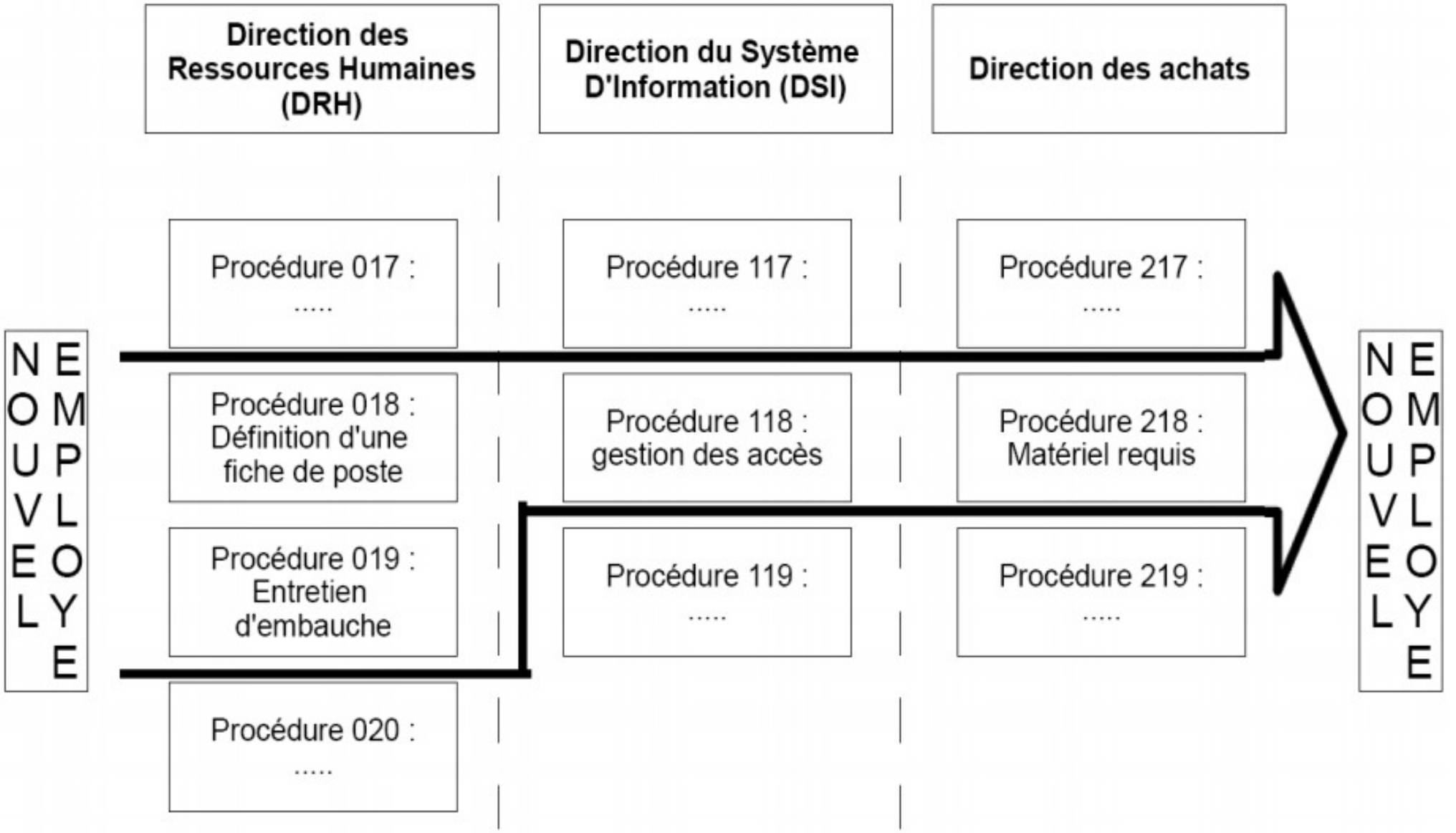
3) Pour obtenir un badge avec des privilèges suffisants, la DSI utilise une procédure qui définit pour le poste en question un profil de sécurité associé avec les bons droits d'accès.

4) le département achat fournit une procédure qui définit, en fonction du poste, le matériel requis pour que le nouvel embauché puisse travailler (bureau, poste fixe, portable, etc...).

→ ces procédures appartiennent au processus d'embauche ;

→ elles utilisent de manière transversale trois services de l'entreprise : la DSI, la DRH et les achats.

Le **D**éploiement : objectif du framework



6. Le **C**ontrôle et l'**A**mélioration

Les phases de contrôle et d'amélioration sont constituées de la mise en place de tableaux de bord et d'audits de sécurité.

Le tableau de bord, composé d'indicateurs de fonctionnement, permet de s'assurer de la performance du système et de l'avancement des travaux qui soutiennent la vision et la stratégie de l'entreprise.

L'audit de sécurité constitue un outil central pour détecter les écarts de conformité et ainsi déclencher les corrections nécessaires.

Contrôle externe

Les contrôles externes de la sécurité consistent à vérifier, de l'extérieur, sans droit d'accès, que les règles de sécurité sont fonctionnelles.

→ ces contrôles doivent être réguliers et automatisés au maximum afin de gagner du temps pour l'analyse.

→ ils doivent tenir compte de la politique de sécurité et de l'évolution des architectures et des services réseau.

→ ils peuvent être fondés sur des outils de balayage, ou de scan réseau, ou même des outils d'attaque pour vérifier que les règles de sécurité définies sont correctement appliquées.

Contrôle par balayage réseau

Une personne malveillante attaque une cible directement accessible depuis le réseau.

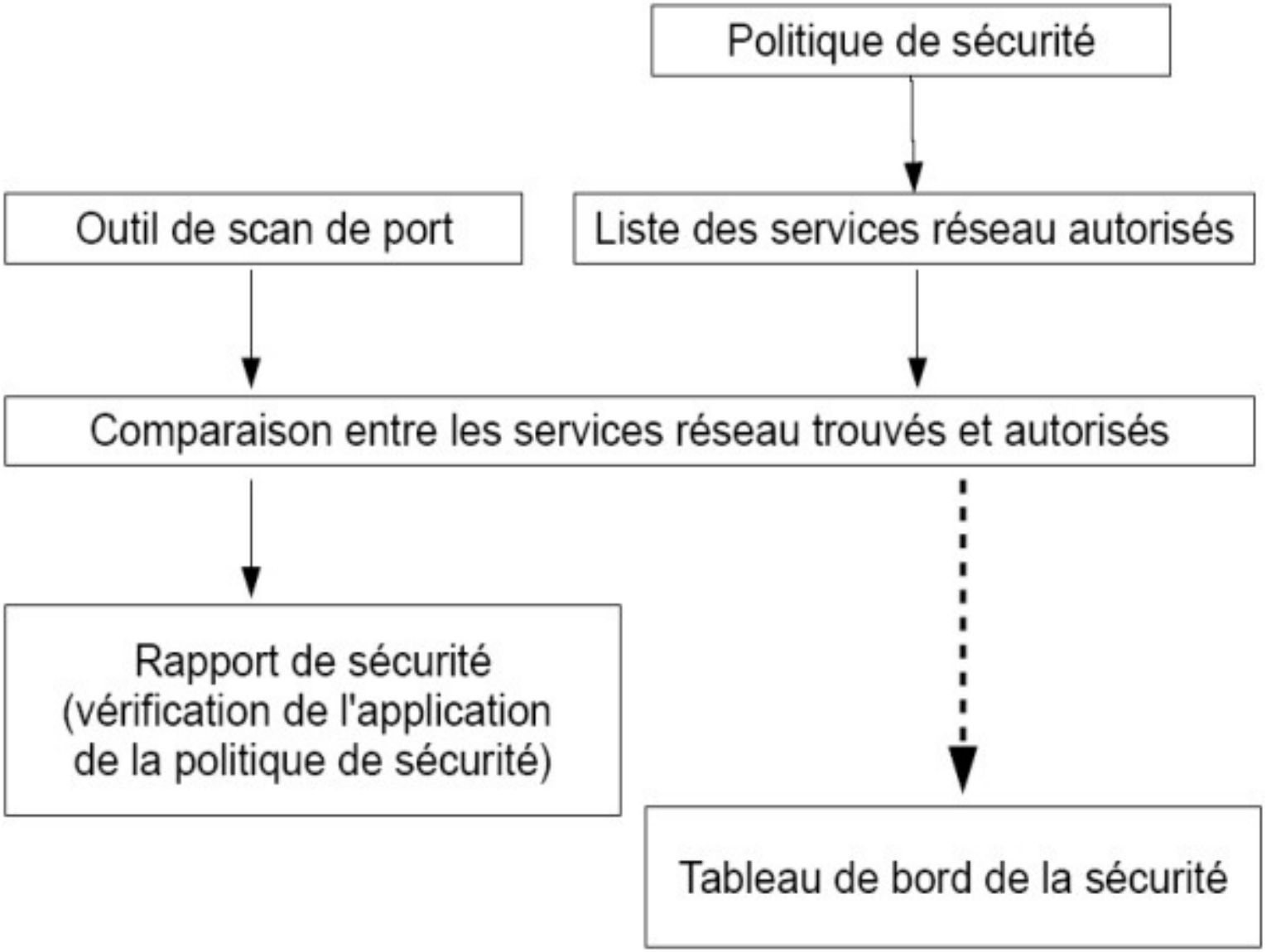
→ les contrôles externes doivent reproduire le même scénario en plus d'être automatisés.

Prenons comme exemple la politique de sécurité simple suivante :

« l'accès aux équipements de l'entreprise n'est possible qu'au travers de flux chiffrés et authentifiés. »

→ un réseau d'entreprise est généralement fondé sur le **protocole IP** et cette politique de sécurité peut être déclinée en guide détaillant la liste des logiciels à utiliser à des fins d'administration :

- Pour des systèmes UNIX, SSH (22/TCP) ;
- Pour Windows, PC Anywhere (5631/TCP et 5632/UDP) ;
- Pour le reste, l'autorisation de l'équipe de sécurité est nécessaire.


Politique de sécurité
Outil de scan de port
Liste des services réseau autorisés
Comparaison entre les services réseau trouvés et autorisés
Rapport de sécurité
(vérification de l'application
de la politique de sécurité)
Tableau de bord de la sécurité

Contrôle interne

Analyse de la configuration des équipements réseau

La configuration des équipements réseau représente la sécurité logique du réseau au travers de la configuration des règles de filtrage d'un **pare-feu** ou d'un **routeur**.

Imaginons qu'une personne mal intentionnée prenne pied sur un routeur suite à une faiblesse de configuration des accès en administration.

Cette personne peut :
- modifier des filtres ;
- les mots de passe ;
- écouter le réseau ;
- faire chuter le réseau ;

→ plus de routage = plus de trafic = plus de réseau !

Pour analyser et corréler les événements de manière efficace, de nouveaux outils sont apparus sur le marché sous le nom de ***Security Information Management***.

Ces outils permettent :

- d'estimer le risque actuel, fondé sur des événements en temps réel ;
- de centraliser les événements ou messages émis par les équipements de sécurité ;

L'intervention humaine est primordiale dans le processus de contrôle et d'analyse des incidents de sécurité.