Mémoire

Les réseaux informatiques et la politique de sécurité

Comment les réseaux informatiques
permettent-ils de garantir
la sécurité du système d'information ?

Présenté par Jean-Christophe FORTON

Examinateurs : F.MILLER
R.KOBYLANSKI

Tuteur : H.GUESDON
O. FAMBON
L. AUBLET-CUVELIER

Master Réseau Informatique d'Entreprise

Année 2008 / 2009

Remerciements

Je tiens à remercier Hervé GUESDON, mon tuteur d'apprentissage, pour m'avoir fait confiance pendant ces deux ans, pour m'avoir laisser mener des projets de bout en bout et n'avoir jamais douter de ma motivation. Je suis très heureux de pouvoir lui exprimer ma très sincère reconnaissance pour m'avoir soutenu et accompagné dans le lancement de ma carrière professionnelle malgré l'accablante charge de travail qu'il doit gérer au quotidien.

Mes remerciements vont également à Olivier FAMBON, Laurent Aublet-Cuvelier et Romain KOBYLANSKI pour leurs conseils sur l'organisation du contenu de cette étude.

Je tiens également à remercier toute l'équipe technique d'UBIqube, Antoine, Olivier, Badia, Eric, Yves, Vincent, Christophe, Jean-Christophe et Pascal pour m'avoir si bien accueilli et pour la bonne ambiance qu'ils font régner au sein de l'équipe.

Sommaire

Table des illustrations

Introduction

J'ai choisi d'aborder la sécurité des réseaux informatiques car elle compose la majeure partie de mon travail à UBIqube, entreprise dans laquelle j'effectue mon alternance. En effet, UBIqube fournit une boîte à outils qui permet de déployer une PSSI au niveau des réseaux informatiques avec une forte composante sécurité. Les outils composants cette boîte à outils s'intègrent dans les différentes étapes de l'approche PDCA et, c'est pourquoi j'aborde le déploiement de la politique de sécurité des réseaux informatiques avec cette même approche.

Comme pour l'**EBT**, ce mémoire est destiné avant tout au DSI (*« **D**irecteur du **S**ystème d'**I**nformation »*) ou RSSI (*« **R**esponsable de la **S**écurité du **S**ystème d'**I**nformation »*) souhaitant mettre en application sa PSSI au niveau des réseaux informatiques. Cependant, si dans l'**EBT** la PSSI tenait compte de toutes les composantes, dans ce mémoire ne sera abordée que la composante réseau. Il propose, dans une première partie, de décrire les réseaux informatiques pour mieux les cerner et rappeler les quatre phases de l'approche processus. Cette partie est l'occasion de mettre en avant les spécificités de la sécurité des réseaux. Ensuite s'enchaine les parties **P**lanification, **D**éploiement, **C**ontrôle et **A**mélioration (**PDCA**), qui forment l'approche processus. Ces parties sont abordées en faisant des interconnexions avec la PSSI généraliste, décrite dans l'**EBT,** pour mettre en exergue les aspects techniques, organisationnel et la conduite du changement nécessaire pour l'appliquer au niveau des réseaux informatiques. La dernière partie balaye les technologies, outils et produits pour proposer une implémentation concrète de la politique de sécurité des réseaux. Cette partie concrète se termine par une analyse de la position des différents équipementiers.

1. Les réseaux informatiques et la politique de sécurité réseau

Ressources bibliographiques utilisées : [B1], [B2]

L'**É**tude **B**ibliographique **T**utorée (**EBT**), menée en amont de ce mémoire, a permis de prendre conscience de l'importance de la sécurité du **S**ystème d'**I**nformation (SI) aujourd'hui au centre de toutes les entreprises. Cet enjeu, abordé au travers d'une **P**olitique de **S**écurité du **S**ystème d'**I**nformation (**PSSI**), est décomposé en quatre phases : **P**lanification, **D**éploiement, **C**ontrôle et **A**mélioration (**PDCA**). Ces quatre phases, qui composent l'approche processus, mettent en place un mécanisme d'amélioration perpétuel et permettent d'aborder le projet de la sécurité du SI avec un souci de gestion de la qualité, comme le permettent également les normes ISO 27001 (« *Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information - Exigences* ») ou 17799 (« *Code de bonnes pratiques pour la gestion de la sécurité d'information* »). La sécurité de l'information dépend en grande partie de la sécurité du dispositif sur lequel elle repose : les réseaux informatiques.

1.1. Les réseaux informatiques

La définition communément admise qualifie un réseau informatique ou d'ordinateurs « d'un ensemble d'équipements reliés entre eux pour échanger de l'information ». Cependant, cette définition, certes concise, ne permet pas de cerner pleinement la notion de réseau informatique et surtout la composante sécurité qui y est étroitement liée. Les paragraphes qui suivent clarifient la nuance entre systèmes répartis et réseaux informatiques, discriminent les réseaux informatiques par leurs modes de connexion et leurs tailles ou étendues géographiques et abordent le modèle OSI (« ***O**pen **S**ystem **I**nterconnection* ») de l'ISO (« ***I**nternational **O**rganization for **S**tandardization* ») qui spécifie les différentes fonctionnalités des réseaux informatiques.

a) Réseau informatique ou système réparti

Il règne souvent une confusion entre la notion de réseau informatique et de système réparti ou distribué. A la différence du réseau informatique, le système réparti est d'un niveau d'abstraction plus important. En effet, même s'il est composé d'un ensemble d'ordinateurs comme le réseau informatique, ces derniers sont indépendants et présentés à l'utilisateur comme un système unique et cohérent. C'est généralement une couche logiciel, située au-dessus du système d'exploitation, appelé « *middleware* » qui est responsable de l'implémentation d'un tel modèle. Un exemple connu de système réparti est le Web (« ***W**orld **W**ide **W**eb* »). Il est composé d'une multitude d'ordinateurs, indépendants les uns des autres, et pourtant il présente son information de manière cohérente sous la forme de pages Web. Avec les réseaux informatiques, les notions de cohérence, de modèle et de « *middleware* » disparaissent. L'utilisateur est alors livré à la réalité des machines et à leurs spécificités. Les systèmes ne tentent pas de se présenter ou d'agir de manière cohérente, et les différences sont d'autant plus visibles qu'il y a de systèmes variés. Pour exécuter un programme sur une machine distante l'utilisateur devra, au préalable, ouvrir une session sur cette dernière. Un système réparti est donc un logiciel élaboré au-dessus d'un réseau et qui apporte un certain degré de cohésion et de transparence. La différence avec un réseau informatique se situe donc plus au niveau du logiciel (système d'exploitation) qu'au niveau du matériel.

On peut constater, sur la figure 1, que le système réparti offre une interface unifiée à l'utilisateur qui n'a donc pas besoin de connaître les rouages de chaque ordinateurs composants le système. Dans le cas du réseau informatique, aucune interface cohérente n'est proposée à l'utilisateur, qui doit donc connaître chacune des particularités des systèmes d'exploitations avec lesquels il désire interagir.

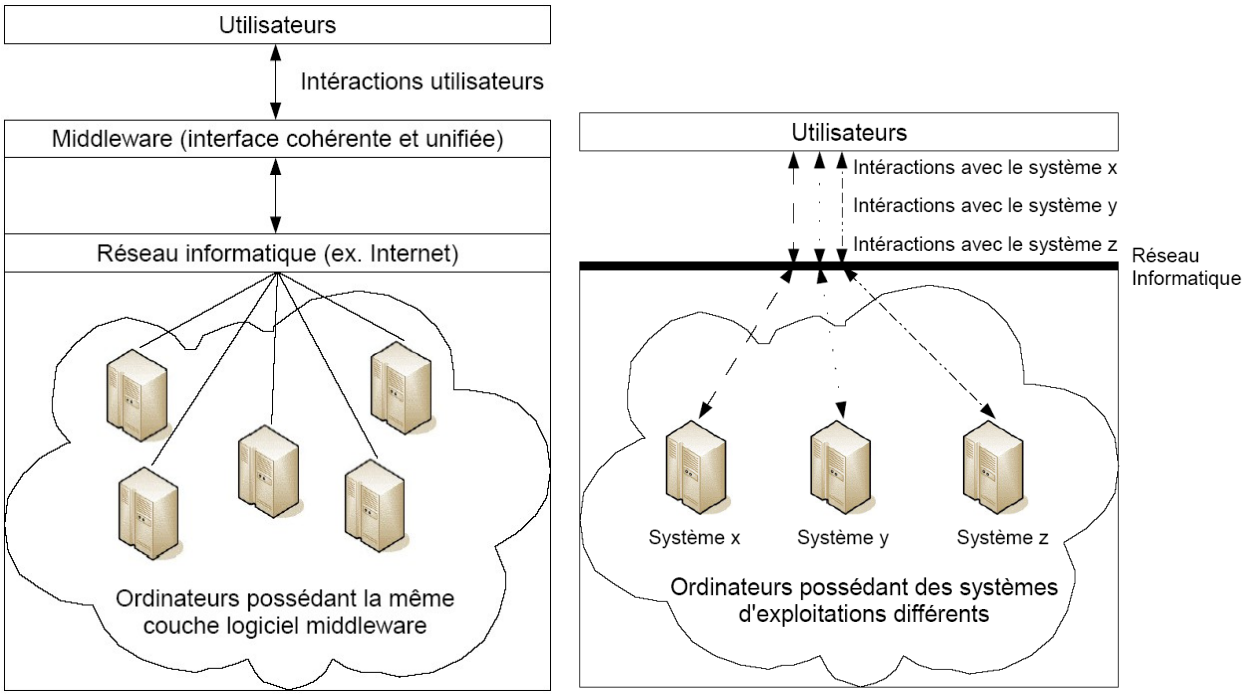

Figure1. Différences entre systèmes répartis et réseaux informatiques

Maintenant que l'ambiguïté entre systèmes répartis et réseaux informatiques est levée, décrivons un peu mieux les réseaux informatiques en nous attardons sur leurs caractéristiques physiques.

b) Caractéristiques physiques

- Technologie de diffusion

On peut différencier les réseaux informatiques en fonction de la technologie de communication qui est utilisée et on en distingue deux : la diffusion et le point à point. Un réseau à diffusion, également appelé « *broadcast* » possède un seul canal de communication qui est partagé par tous les équipements qui y sont connectés. De la sorte, chaque message envoyé, appelé paquet, est reçu par toutes les machines du réseau. Un réseau à diffusion a également la possibilité d'adresser un paquet à tous en utilisant une valeur spéciale dans le champ « adresse ». Certains réseaux permettent également d'adresser un paquet à un sous ensemble de machines et on parle alors de diffusion restreinte.

Par opposition aux réseaux de diffusion, les réseaux point à point ne permettent d'interconnecter que deux machines entres elles. Cette manière de procéder multiplie le nombre de connexions pour pouvoir interconnecter le même nombre de machines. Dans de tel réseaux, un paquet peut transiter par plusieurs machines pour atteindre sa destination et souvent il existe plusieurs chemins possibles pour arriver à la même destination (cf. figure 2). Cette transmission point à point est appelée diffusion individuelle ou « *unicast* ».

La technologie de communication n'est pas la seule manière de discriminer les réseaux informatiques, on peut le faire aussi en fonction de leurs tailles ou étendues géographiques.

- Étendue géographique

Le plus petit réseau qui existe, le réseau personnel ou PAN (*« **P**ersonal **A**rea **N**etwork »*), est destiné à une seule personne. Il peut être sans fil comme avec le bluetooth ou filaire comme avec l'USB et sert principalement à interconnecter des équipements de bureau comme des souris, claviers ou encore imprimantes. Sa grandeur géographique ne dépasse pas le mètre carré.

Vient ensuite le réseau local ou LAN (*« **L**ocal **A**rea **N**etwork »*) qui sert à relier plusieurs ordinateurs entre eux. Il est fréquemment utilisé dans les maisons, bureaux, usines ou campus pour relier des ordinateurs, stations de travail ou des équipements (comme des imprimantes) et ainsi leurs permettre d'échanger des informations ou d'utiliser des ressources communes. Les LAN sont de taille restreinte, en général moins d'un kilomètre.

Les réseaux métropolitains, également appelés MAN pour « *Metropolitan Area Network »*, servent principalement à câbler une ville. Ils ont été conçus à la base pour pouvoir fournir la télévision dans les zones souffrant d'une mauvaise réception. En effet, une antenne était placée sur un point haut permettant ainsi une bonne réception, et le signal était ensuite acheminé par câble vers les abonnées. Avec l'utilisation de plus en plus massive de l'Internet, les cablo-opérateurs ont réalisé qu'ils pouvaient réutiliser ces réseaux pour offrir un service d'accès à Internet bidirectionnel en plus du service de télévision. On peut remarquer que les cablo-opérateurs, comme **Numéricâble** à Grenoble, remplacent peu à peu les câbles de cuivre, sujets aux perturbations électro-magnétique, par des fibres optiques plus performantes.

Le réseau permettant d'interconnecter deux villes entre-elles s'appelle réseau longue distance ou WAN pour *« Wide Area Network »*. Ce réseau peut couvrir un pays, voire un continent, et englobe un ensemble d'ordinateurs appelés hôtes. Ces hôtes sont affectés à l'exécution de programmes utilisateur ou applications, et sont reliés entre eux par le biais de sous-réseaux de communication. Les hôtes sont souvent la propriété de particuliers ou d'entreprise et sont composés d'ordinateurs personnels ou encore de serveurs, alors que les sous-réseaux sont la propriétés des opérateurs de télécommunication ou de fournisseurs d'accès à Internet et sont composés essentiellement d'équipements de commutation appelés routeurs. Les sous-réseaux ont pour unique but d'acheminer les paquets ou messages d'un hôte à un autre et sont décorrélés des applications, ce qui simplifie grandement leurs conceptions. La figure ci-dessous montre la pluralité des chemins qu'un paquet peut emprunter.

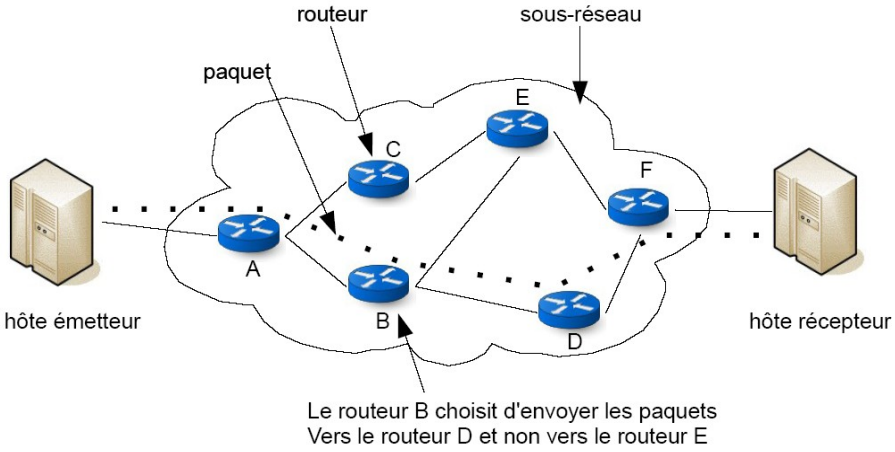

Figure2. Pluralité des chemins possibles dans un WAN

Pour conclure cette discrimination géographique des réseaux, on peut dire que le plus grand réseau informatique qui existe est incontestablement Internet et permet de relier les WAN entre eux.

Le tableau ci-dessous classe les différents réseaux en fonction de leurs étendues géographiques.

Réseaux	Distance entre les équipements	Exemple de localisation
Réseau personnel (PAN)	1 m	Un bureau
Réseau local (LAN)	10 m	Une salle
	100 m	Un immeuble
	1 km	Un campus
Réseau métropolitain (MAN)	10 km	Une ville
Réseau longue distance (WAN)	100 km	Un pays
	1000 km	Un continent
Internet	10 000 km	Une planète

Figure3. Classement des réseaux en fonction de leurs étendues géographiques

c) Représentation des réseaux dans le modèle OSI

Le modèle OSI de l'ISO est une première étape vers la normalisation internationale des protocoles utilisés à différents niveaux, appelés couches, dans les réseaux. Le modèle OSI ne sert pas à spécifier un réseau informatique car il ne spécifie pas les services ni les protocoles à utiliser dans chaque couche, mais précise uniquement ce qu'elle doit faire. Il permet, à travers ces sept couches, d'aborder toutes les fonctionnalités des réseaux informatiques, chose que nous allons faire.

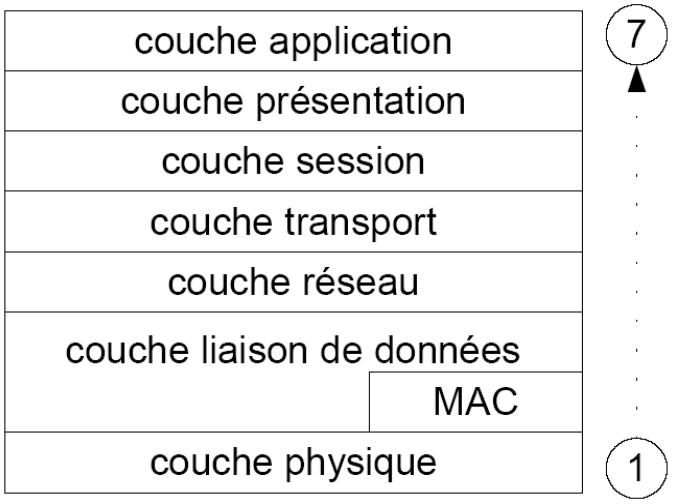

Figure4. Représentation des réseaux informatiques par le modèle OSI

La couche physique est la partie visible des réseaux informatiques et se charge de la transmission des bits sur le canal de communication. Un des objectifs de ce niveau est de s'assurer qu'un bit à « 0 » envoyé sur une extrémité arrive à « 0 » de l'autre côté. Cette couche détermine le nombre de volt à fournir pour représenter les bits, leurs durées, les paramètres des connexions, etc... Cette couche sert donc à spécifier les interfaces mécaniques, électriques ou optiques, la synchronisation et les supports physiques de transmission comme les câbles en cuivre ou encore les fibre optiques.

La couche suivante, appelée liaison de données, a pour rôle de proposer un moyen de communication brut et exempt d'erreur à la couche réseau (couche supérieure). Pour cela elle décompose les données sur l'émetteur en trame de données, de taille comprise entre la centaine et le millier d'octets, et envoie ces trames en séquences. Cette couche gère également les mécanismes de flux qui évitent qu'un récepteur lent ne soit submergé par les trames d'un émetteur rapide ainsi que la gestion d'erreur. Les réseaux à diffusion, abordés au paragraphe 1.2.a, sont confrontés à la difficulté supplémentaire de l'accès au canal partagé. C'est la sous-couche, appelé MAC (« ***M**edium **A**ccess **C**ontrol »*), et visible à la figure 4 qui est chargée de résoudre ce problème. Il est possible d'identifier les hôtes à ce niveau (niveau 2) grâce à leurs adresses MAC (« ***M**edia **A**ccess **C**ontrol Address »*), appelés également adresses physiques. Ces adresses, composées de 6 octets, sont uniques et représentées en séparant les octets par deux points : « 00:18:DE:5E:1C:2B ».

La couche réseau, contrôle le fonctionnement du sous-réseau. Elle permet de déterminer la façon dont les paquets sont routés, c'est à dire aiguillés, comme dans l'exemple de la figure 2 avec le routeur B. Le routage peut être effectué à l'aide de tables statiques, déterminé au début de chaque conversation ou à chaque fois qu'il faut envoyer un paquet pour tenir compte de la congestion (utilisation) du sous-réseau. Lorsqu'un paquet transite d'un réseau à un autre, des problèmes peuvent survenir, et cette couche doit les gérer et garantir l'interconnexion de réseaux hétérogènes. Il est possible d'identifier les hôtes à ce niveau (niveau 3) grâce à leurs adresses IP (*« **I**nternet **P**rotocol »*). Ces adresses permettent d'identifier un hôte sur un sous-réseau utilisant le protocole IP et, à contrario de l'adresse MAC, permettent de communiquer avec des hôtes situés sur d'autres sous-réseaux (utilisant IP). Il existe deux types d'adresses IP, les plus anciennes de version 4 sont constituées de 4 octets et les plus récentes de version 6 sont constitués de 16 octets. Elles sont représentés par des nombre de 0 à 255 séparés par des point : 212.217.0.1 (adresse IP de version 4 du serveur DNS de Maroc Télécom).

La couche transport a pour rôle d'accepter les données de la couche supérieure, de les scinder en unités plus petites si besoin, de les transmettre à la couche réseau et de s'assurer qu'elles sont bien arrivées à destination. Le type de connexion le plus utilisé est le canal point à point vu au paragraphe 1.2.b, qui peut être exempt d'erreurs grâce au protocole TCP (*« **T**ransfert **C**ontrol **P**rotocol »*), ou non si UDP (*« **U**ser **D**atagram **P**rotocol »*) est utilisé.

La couche session offre aux utilisateurs de différentes machines pléthores de services. Parmi ceux-ci on trouve la gestion du dialogue qui assure un suivi de la transmission, la gestion du jeton qui garantit l'unicité d'une opération critique à un instant t, et la synchronisation qui permet aux transmissions longues distances de reprendre après interruption grâce à la gestion de points de reprises.

La couche présentation s'intéresse à la syntaxe et à la sémantique des informations transmises. Elle permet la communication entre deux ordinateurs qui ont des représentations de données différentes, en définissant une structure de données abstraite et un système d'encodage au « fil de l'eau ». Elle gère ces structures de données et autorise la définition et l'échange de structure de plus haut niveau comme les enregistrement bancaires.

La couche application contient moult protocoles utiles aux utilisateurs comme HTTP (*« **H**yper**T**ext **T**ransfert **P**rotocol »*) qui forme la base du *« **W**orld **W**ide **W**eb »*. Les autres protocoles servent, par exemple, pour le transfert de fichier (*« **F**ile **T**ransfert **P**rotocol »*), le courrier électronique ou encore les nouvelles (*« news »*).

Cette section a permis de mieux appréhender les réseaux informatiques en les discriminant par leurs modes de connexion ainsi que par leurs étendues géographiques. Le faite de les aborder à travers le modèle OSI permet également de comprendre qu'ils ne se limitent pas à la partie visible, représentée par les câbles interconnectant les différents équipements (couche 1). Effectivement, ils servent également à connecter des machines sur un même sous-réseaux (couche 2), à router les paquets entre des machines situées sur des sous-réseaux différents (couche 3), à proposer différents niveaux de services (couche 4), à fournir une variété de protocoles aux utilisateurs (couche 7), et fournissent encore bien d'autres services. Cette mise en avant des différentes composantes qui constituent les réseaux informatiques permet de comprendre qu'assurer la sécurité des réseaux informatiques c'est prendre en compte ces différences. Attardons nous maintenant sur la mise en place de la politique de sécurité.

1.2. La politique de sécurité du Système d'information

a) Les enjeux et intervenants

Les réseaux informatiques constituent la base qui va relier l'entreprise au monde extérieur, par le biais d'Internet, mais ils vont également servir au stockage des données et c'est pourquoi assurer leur sécurité signifie assurer la pérennité de l'entreprise. Cependant, ils sont très souvent négligés et perçus uniquement comme un moyen pour relier l'entreprise avec ses différents intervenants comme les fournisseurs, prestataires, clients, etc... Cette vulgarisation n'incite malheureusement pas les décideurs à voter le budget nécessaire pour qu'ils soient correctement implémentés. Quant on sait que la sécurisation est l'étape qui suit l'implémentation, on peut se demander si la sécurité des réseaux informatiques est bien prise au sérieux par les décideurs. Depuis quelques années, grâce aux lois Sarbanes-Oxley et aux accords Bâle II aux États-unis ou à la **L**oi sur la **S**écurité **F**inancière (**LSF**) en France, on peut observer un changement de situation. En effet, ces lois obligent les dirigeants à rendre des comptes aux actionnaires par le biais de bilans et, de ce fait, à ne pas négliger la sécurité des réseaux informatiques qui renferment les données avec lesquelles sont bâtis ces bilans. Cependant, cette augmentation des dépenses permet une meilleur garantie de la sécurité des réseaux.

b) Planification, Déploiement, Contrôle et Amélioration

Dans l'EBT, le thème de la PSSI englobait tous les domaines de l'entreprise. Au niveau des réseaux informatiques, cette PSSI se transforme en politique de sécurité réseau. Quoique légèrement différentes, ces deux politiques peuvent être abordées avec la même approche dite processus. Cette approche est intéressante car elle insère le projet de la politique de sécurité réseau dans un mécanisme d'amélioration perpétuelle composée de quatre phases, rappelées par la figure 5, à savoir **P**lanification, **D**éploiement, **C**ontrôle et **A**mélioration (**PDCA**).

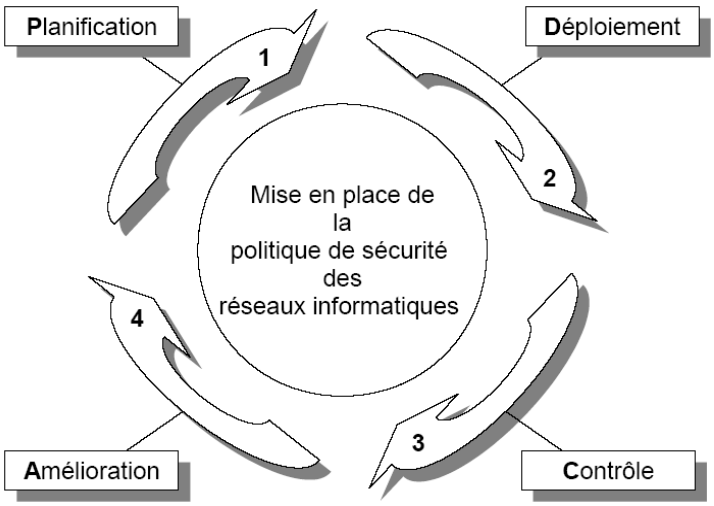

Figure5. Politique de sécurité des réseaux et approche PDCA

Rappelons succinctement l'utilité des quatre phases :

- Planification : elle consiste à préparer un programme et un calendrier en fonction des objectifs fixés ;
- Déploiement : elle doit donner les moyens financier, technique et humain définit 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.

1.3. La politique de sécurité des réseaux

a) Le réseau au sein du SI

La contrainte sécuritaire donne peu à peu naissance à une nouvelle fonction au sein des entreprises qui se soucient de la sécurité de leurs SI : **R**esponsable de la **S**écurité du **S**ystème d'**I**nformation (**RSSI**). Le RSSI est un manager qui inscrit son projet de sécurité de l'information dans un programme de management de la sécurité et son rôle est de déployer les mesures, prendre les dispositions, mobiliser les hommes, qualifier les outils et les moyens qui assureront cette sécurité. Il peut mener son projet au travers d'une politique de sécurité réseau qui, si elle est menée grâce à une approche de type PDCA, est un outil lui permettant de perpétuellement améliorer la sécurité de son réseau informatique. Cependant, effort de sécurité rime avec effort financier et on peut consulter l'étude ([W1]), réalisée par le ***Comp**uting **T**echnology **I**ndustry **A**ssociation* (CompTIA) sur environ 1070 organisations, pour s'en convaincre. Cette étude met en avant la constante augmentation du budget dédié à la sécurité au sein de ces organisations, qui passe de 12% du budget total en 2004, à 20% en 2006.

b) Les problématiques spécifiques

- Domaines impactés

La politique de sécurité réseau s'inscrit dans la démarche sécuritaire entamé par la PSSI généraliste mais se limite aux 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, les équipements de télécommunications et réseaux qui permettent le bon fonctionnement du SI ;
- 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.

- Définition d'un périmètre

La définition de la politique de sécurité réseau est une démarche impliquant toute ou partie de l'entreprise et visant à protéger son personnel et ses biens d 'éventuels incidents de sécurité dommageables pour son activité. La définition d'un périmètre d'application doit être faite pour qualifier les parties critiques du réseau et s'intéresser uniquement à ces dernières. De la sorte, le déploiement de la politique de sécurité se fait progressivement et l'entreprise tout entière ne se retrouve pas mobilisée pour cette tâche. On peut s'appuyer sur l'expérience d'Alexandre Fernandez-Toro qui prend comme exemple, le cas **B**ritish **T**elecom (**BT**). BT s'est lancé dans plus de 20 certifications ISO 27001 simultanées et cette mauvaise définition du périmètre n'a fait que rallonger le temps d'obtention des certifications quand elles n'ont pas échouées. BT a actuellement certifié 15 de ces systèmes et confirme la lourdeur de gestion. Mais maintenant que les systèmes ont été certifiés indépendamment, il est très difficile de les rassembler en un seul pour en simplifier la gestion. Que ce soit pour la certification ISO 27001 ou la politique de sécurité réseau, la définition du périmètre est tout aussi importante et déterminera la réussite du projet.

- Notions protégées par la politique de sécurité

Petites et moyennes et grandes entreprises s'exposent aux mêmes risques si elles ne définissent pas de politique de sécurité et, quelle que soit la nature des biens à protéger, la politique de sécurité réseau visent à satisfaire un certain nombre de critères que nous allons aborder. L'**identification** est l'information qui permet d'indiquer qui une personne prétend être. Une identification de base est constituée d'un nom d'utilisateur mais il en existe des plus évoluées qui utilisent les empreintes digitales ou l'analyse faciale ou rétinienne. L'**authentification** est l'information qui vient valider l'identification. Une authentification de base est constituée d'un mot de passe mais des authentifications forte existent et combinent une chose possédée et une chose connue comme par exemple la carte bancaire et le 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, énoncés au paragraphe 1.1.c avec IPsec (couche 3 OSI) et SSL (couche 7 OSI), est la seule solution fiable 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 faite de garantir que les ressources de l'entreprise sont accessibles qu'il s'agisse du réseau, la bande passante ou une quelconque autre ressource nécessaire au fonctionnement du SI. La **non-répudiation** permet de garantir qu'un message a bien été échangé entre un émetteur et un destinataire. Par exemple, dans le domaine bancaire, la non-répudiation est le faite de pouvoir justifier qu'une transaction s'est bien déroulée entre un personne A et B. La **traçabilité** est l'ensemble des mécanismes permettant de retrouver les opérations réalisées sur les ressources de l'entreprise constituant le SI. Cela suppose que tous les événements applicatifs et réseaux soient archivés et disponibles pour une consultation ultérieure.

- Les aléas de la vie d'entreprise

Quelle que soit la taille de l'entreprise et la politique de sécurité réseau définie, l'application de la politique de sécurité réseaux est souvent confrontée aux trois contraintes suivante : technique, économique et politique. La **contrainte technique** est liée aux limites de la technologie. En effet, certaines applications sont difficilement filtrables ou ne tolèrent pas les remplacements d'adresse (*« **N**etwork **A**drress **T**ranslation »* ou *« masquerading »*) comme le protocole H323, qui permet la signalisation de la voix sur IP, ou IPsec, qui permet le cryptage des données. Pour une solution technique donnée, une **contrainte économique** peut surgir et oblige alors à choisir une solution moins onéreuse. Si cette nouvelle solution ne répond pas scrupuleusement aux besoins de sécurité il va falloir procéder à une 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. Pour finir, la **contrainte politique** survient souvent sans justification technique ou logique et peut engendrer de gros problèmes de sécurité qui doivent être suivi d'une acceptation de risque de sécurité.

- Conseils rédactionnels

Un document de politique de sécurité réseau peut être écrit soit d'un seul tenant soit décomposé en un ensemble de politiques de sécurité. Le choix est souvent dicté par la taille du réseau et de l'entreprise. En effet, les petites entreprises privilégieront un seul document alors que les grandes entreprises préféreront créer des documents séparés, chaque niveau de politique de sécurité faisant référence au niveau supérieur.

Lorsque l'on écrit une politique de sécurité réseau, il n'est pas rare de confondre les besoins et les moyens et c'est pourquoi il est impératif de distinguer les deux. L'objectif d'une politique de sécurité est d'énoncer les résultats attendus et non les moyens par lesquels les obtenir. C'est pourquoi les principes qu'elle énonce ont une pérennité beaucoup plus longue que les procédures de sécurité, qui sont amenées à être modifiées fréquemment, pour tenir compte des avancées technologiques, modification d'architectures et autres points techniques. La politique de sécurité, moins touchée par l'évolution technologique, doit néanmoins être revue tous les deux ans afin de tenir compte des modifications organisationnelles de l'entreprise. Dans une politique de sécurité il convient donc d'écrire : *« L'accès à distance au réseau interne de l'entreprise est autorisé via une connexion réseau chiffrée établie suite à une authentification forte. »* et non : *« Le réseau interne de l'entreprise est accessible depuis l'extérieur via une connexion réseau chiffré par le protocole IPsec et authentifiée grâce à la PKI interne à l'entreprise ».*

c) Garantir la sécurité

La sécurité des réseaux informatiques est multidimensionnelle et doit s'intéresser aux concept vus précédemment à savoir : le canal, l'étendue géographique et les différents services abordés avec le modèle OSI.

- Le canal

Les différentes technologies de diffusion permettent de connecter un hôte à un ou plusieurs autre par le biais de canal. Ce canal peut faire l'objet d'une attaque et doit être sécurisé. En effet, il est possible qu'une personne malveillante usurpe l'identité du destinataire (*« spoofing »*) ou encore procède à une attaque de type *« man-in-the-middle »,* pour masquer à chaque acteur la réalité de son interlocuteur et ainsi récupérer les paquets qui transitent dans le canal de communication. Si dans le premier cas, le destinataire ne reçoit plus de paquets et s'aperçoit de l'attaque, dans le deuxième cas la communication initiale n'est pas interrompue, ce qui rend la détection de l'attaque plus difficile. Ces deux type d'attaques, représentés par la figure 6, peuvent être effectués au niveau 2 (liaison de données) ou 3 (réseau) du modèle OSI. Pour garantir un bon niveau de sécurité, dans le cadre d'échange bancaire par exemple, le canal de communication a la possibilité d'être chiffré pour que seuls émetteur et destinataire puissent déchiffrer les paquets qui y transitent. Cette sécurisation du canal de communication peut être faite à différents niveaux du modèle OSI, comme au niveau 3 avec IPsec, ou au niveau 7 (applicatif) avec SSL (*« **S**ecure **S**ocket **L**ayer »*).

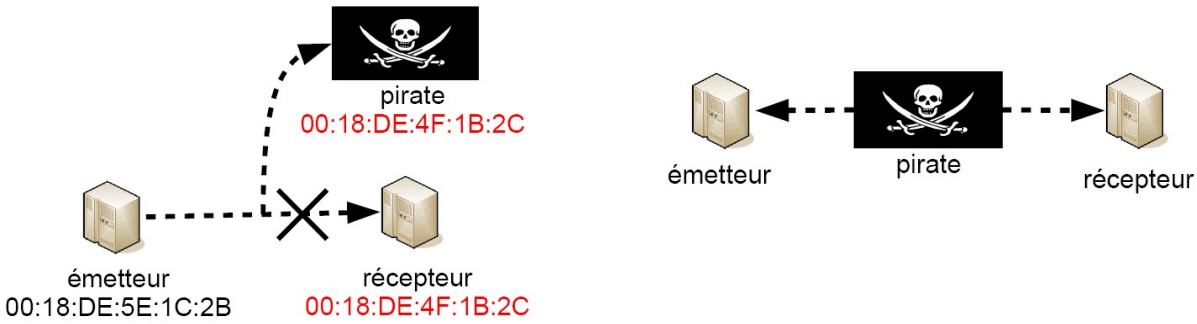

Figure6. Attaques par « *spoofing* » et « *man-in-the-middle* »

- L'étendue géographique

La grandeur du réseau peut aussi constituer un problème de sécurité. En effet, plus le réseau est grand et plus il contient de points de connexion avec d'autres réseaux et d'utilisateurs. Les points de connexion peuvent être assimilés à des postes de douane dans le sens où ils permettent de contrôler ce qui rentre et sort du réseau. Si l'on conçoit bien le fait de contrôler ce qui rentre, pour filtrer le trafic ou parer des attaques, contrôler ce qui sort du réseau est tout aussi important. Effectivement, d'après l'article 323-2 du nouveau code pénal : *« le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 300000 francs d'amende »*. Donc, les responsables d'un réseau attaqué peuvent poursuivre en justice les responsables du réseau où l'attaque a pris sa source. Il arrive que des pirates profitent des accès sans fil mal sécurisés des particuliers pour se connecter à Internet et déclencher des attaques . Le particulier, dont le réseau sans fil est la source de l'attaque, se retrouve alors incriminé. De plus, plus le nombre d'utilisateurs augmente et plus il y a de pirates potentiels. Les pirates ne sont pas toujours ceux que l'on croit. On peut prendre comme exemple *Terry Childs* administrateur du réseau MAN de San Francisco. Cet homme, en désaccord avec sa direction, à décider de remplacer les mots de passe des équipements du réseau et de placer un routeur pirate qui n'a toujours pas été localisé à ce jour.

Ce chapitre a abordé sécurité des réseaux informatiques et politique de sécurité. Il a permit d'aborder les spécificités des réseaux ainsi que l'approche PDCA, qui permet d'insérer la politique de sécurité des réseaux dans un mécanisme d'amélioration perpétuelle. Abordons maintenant les différentes étapes de la politique de sécurité réseau à travers l'approche processus.

2. Planification

Nous avons vu, dans la PSSI généraliste, que la phase de planification est composée de quatre phases : la vision, les objectifs de sécurité, les moyens et la stratégie de mise en œuvre. **La vision**, qualifiée dans l'EBT de *« représentation partagée, décrite en termes précis et qui permet de qualifier le futur souhaité »*, nécessite un état des lieux qui permet de recenser tous les biens de l'entreprise et d'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**, qui décomposent la vision, sont élaborés grâce à une échelle de besoin qui va permettre d'associer un objectif à une importance. Cette évaluation se fait grâce à une multitude de paramètres comme la fiabilité, le contrôle ou tous ceux cités au paragraphe 1.3.b (authentification, autorisation, etc...). Une fois les objectifs de sécurité définis, les actions à entreprendre apparaissent clairement et il est temps de leurs associer des moyens. **Les moyens** sont qualifiés dans l'EBT comme *« la partie la plus critique »* car ils arrivent *« à un moment où le projet est souvent embryonnaire et où la visibilité est faible »*. Ils doivent être dimensionnés de manière à atteindre les objectifs de sécurité et définis en 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 vison »* et représente les modes d'actions et d'allocation des moyens. Dans le domaine des réseaux informatiques, cette phase de planification est décomposée en différentes étapes et nous allons commencer par le principe de propriété.

2.1. Principe de propriété

Le principe de propriété qui suit l'état des lieux, exige que la politique de sécurité réseau décrive pour chaque ressource de l'entreprise un propriétaire fonctionnel. Le propriétaire, qui se porte garant de la pérennité et de la protection de la ressource, dicte également les conditions d'accès à sa ressource. Un schéma de responsabilité classique, représenté par la figure 7, fait intervenir un propriétaire, un administrateur et un utilisateur. Le propriétaire définit les règles d'utilisation de la ressource et les donne à l'administrateur qui est en charge de les appliquer à la demande d'un utilisateur. L'administrateur, en cas de besoin, peut demander une dérogation aux droits d'accès au propriétaire. Ce mode de fonctionnement garantit une certaine indépendance de l'administrateur face à l'utilisateur qui n'est jamais en contact direct avec le propriétaire de la ressource.

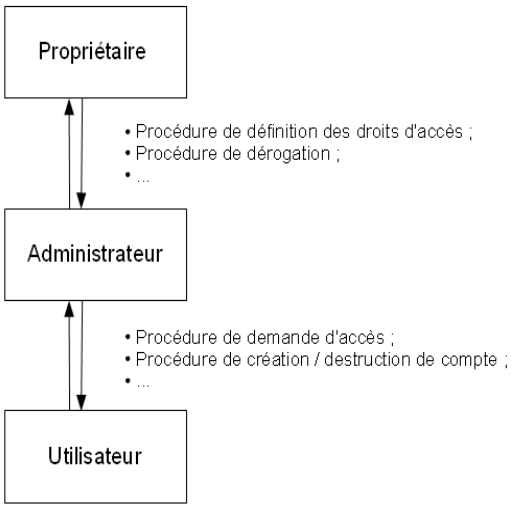

Figure7. Procédure de partage d'une ressource

Maintenant que les ressources sont clairement attribuées, il faut continuer avec le découpage de la politique de sécurité réseau.

2.2. Découpage de la politique de sécurité réseau

La découpage d'une politique de sécurité réseau 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 standard, guides et recommandations de sécurité ;
- de procédure de sécurité.

La politique générale de sécurité de l'entreprise est une politique de haut niveau qui dirige les orientations de toutes les autres. Cette politique, composée de la politique de sécurité de l'intranet et Internet, définit les axes stratégiques de sécurité réseaux de l'entreprise. La politique sécurité de l'intranet précise les règles de sécurité du réseau interne comme, par exemple, l'interdiction de connecter le réseau interne à d'autres réseaux par des connexions non autorisées, de lancer des attaques ou encore de faire circuler des virus au sein du réseau interne. La politique de sécurité Internet énonce les principes de connexion à Internet à partir du réseau interne de l'entreprise. Elle précisera, par exemple, l'interdiction d'installer sur un poste du réseau interne des outils téléchargés sur Internet ou encore d'envoyer des informations non chiffrées sur Internet. **Les standards, guides et recommandations de sécurité** regroupent l'ensemble des recommandations d'ordre technique relatives à l'implémentation de la politique de sécurité et sont également séparés en deux parties : intranet et Internet. Ceux destinés à l'intranet regrouperont, par exemple, comment installer les outils utiles pour administrer les serveurs Unix, comme SSH (*« **S**ecure **SH**ell »*). Ceux destinés à Internet pourront définir comment choisir un pare-feu adapté à une utilisation particulière ou encore comment installer un serveur Web sécurisé. **Les procédures de sécurité** couvrent les éléments critiques définit comme tel dans l'état des lieux. Ces procédures, très détaillées et techniques, sont réparties en trois parties : intranet, Internet et réactives. Les procédures intranet pourront traiter de la sauvegarde des bases de données ou encore de l'accès à distance à l'intranet. Les procédures Internet incluront le paramétrage de la sécurité du navigateur Internet ou encore celui des logiciels antivirus. Les procédures réactives sont utiles pour indiquer la marche à suivre en cas de détection de virus ou en cas d'intrusion.

Le découpage de la politique de sécurité ainsi que les thèmes abordés par les politiques sous-jacentes sont à réfléchir pendant la phase de planification, en revanche, leurs rédactions est à faire pendant la phase de déploiement. La figure 8 se propose de résumer la hiérarchie des différentes politiques de sécurité décrites précédemment.

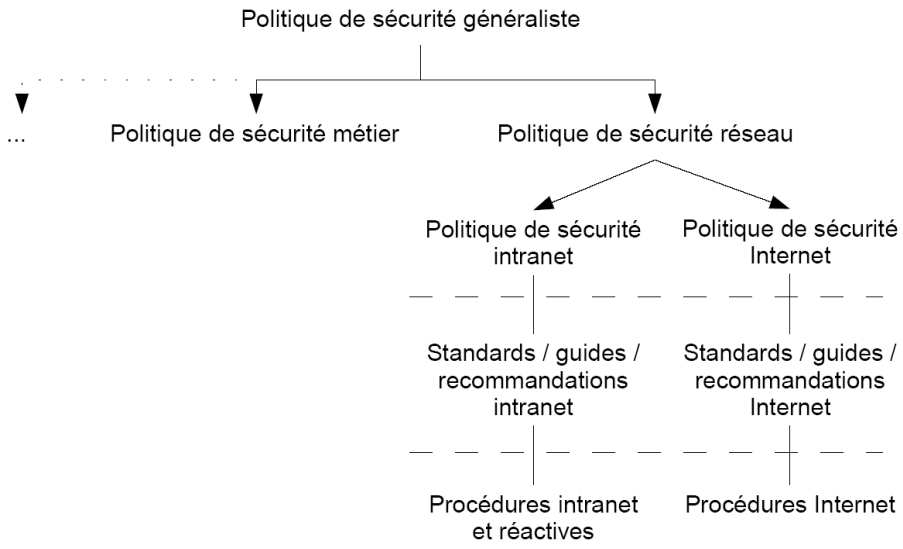

Figure8. Découpage de la politique de sécurité

La planification de la politique de sécurité réseau est essentiellement composée d'un découpage, autant sur le plan des ressources, avec le principe de propriété, que sur le plan de la documentation, avec le découpage de la politique de sécurité en plusieurs niveaux. Maintenant que cette phase de planification est terminée, attardons nous sur l'élaboration de la phase de déploiement.

3. Déploiement

Dans la PSSI généraliste, la phase de déploiement est composée des parties « système documentaire » et « méthode de déploiement ». Le système de documentaire, déjà abordé dans la phase de planification par le paragraphe 2.2, doit être mis en place dans cette phase et pour y arriver, l'utilisation d'un *« framework »* est possible. Ce *« framework »* met en place l'éventail de documents qui composent *« la politique de sécurité « cadre » et le panel opérationnel »*, définit dans l'EBT. Les méthodes de déploiement, appelées stratégies de sécurité, vont permettre d'implémenter les objectifs spécifiés dans la politique de sécurité. Commençons par l'aspect documentaire.

3.1. Définition d'un « framework »

Un *« framework »* est une structure basique permettant la résolution de problèmes complexes. Le *« framework »* de sécurité réseau va permettre de définir un guide de recommandation de haut niveau, d'après la décomposition de la vision en objectifs, qui va ensuite être décliner en plusieurs guides et règles. Il doit tenir compte des spécificités et besoins de sécurité de l'entreprise, mais dans tous les cas il devra traiter des chapitres suivants, essentiels à la partie réseau : organisation et management, ressources humaines, gestion de projet, gestion des accès logiques, exploitation et administration, vérification des configuration, sécurité physique, plan de désastre et vérification de l'application de la politique de sécurité réseau. Les paragraphes qui suivent détaillent un certain nombre de ces guides et règles.

- 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, etc... Il est judicieux de définir un comité, constitué des dirigeants de l'entreprise, et qui a pour mission la définition de la stratégie de sécurité et le support de sa mise en place. Les objectifs de sécurité doivent être inclus dans la stratégie de l'entreprise et définir un plan de sécurité annuel. Une politique de sécurité générale doit être définie avec des objectifs simples et précis, incluant les rôles et responsabilités de chacun des départements de l'entreprise. Une équipe de sécurité, ayant pour mission la vérification de la bonne application de la politique de sécurité réseau, doit être créée. Un ensemble de recommandations, couvrant les domaines ciblés par la politique de sécurité réseau, est défini pour tous les départements de l'entreprise. Enfin, des procédures de sécurité, chargées de garantir la sécurité des ressources critiques, sont établies pour tous les départements.

- Ressources humaines

La politique de sécurité nécessite l'implication des salariés pour être appliquée de façon optimale et c'est pourquoi le facteur humain dépasse souvent les aspects purement techniques. Les procédures de recrutement doivent être clairement définies et les contrats d'embauches doivent inclure un paragraphe relatif à la politique de sécurité de l'entreprise. Les cadres juridiques et réglementaires de la politique de sécurité et des actes de malveillance doivent être connus de tous. Des procédures disciplinaires doivent être définies suite à l'implication d'un salarié dans un acte de malveillance. Les fonctions clés de l'entreprise comme directeur de recherche, des opérations ou expert de la sécurité doivent être identifiées. Les salariés, fournisseurs ou prestataires doivent recevoir une sensibilisation à la sécurité car la connaissance par autrui de toutes informations sensibles risque de faire perdre à l'entreprise un avantage important face à ces concurrents.

- Gestion de projet

La politique de sécurité doit tenir compte des évolutions des produits et services de l'entreprise afin de coller à la réalité. De manière générale la gestion de projet doit tenir compte de la politique de sécurité, le plus en amont possible, afin d'y intégrer les contraintes de sécurité. Les procédures de développement des produits et services doivent être clairement définis et documentés et le développement des produits ou services doivent tenir compte de la politique de sécurité dès la phase de conception. Des tests de non régressions doivent être définis lors du développement et ont pour unique objectif de valider que le niveau de sécurité préalablement défini reste valide. 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 défini. La documentation relatives aux projets informatiques est accessible au personnel de l'entreprise, classée en fonction de la confidentialité et maintenue à jour.

- Gestion des accès

Les accès et droits d'accès aux ressources de l'entreprise composent le volet de la politique de sécurité le plus dure 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 aspect 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 ces droit d'accès. Pour y parvenir, il faut avoir procéder à une classification des ressources de l'entreprise, normalement effectuée pendant la phase de planification. Les responsables, administrateurs et utilisateurs de chacune des ressources sont définis ainsi que les procédures et interactions entre eux, comme stipulé au paragraphe 2.2.a par le principe de propriété. Enfin, 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 du réseau et des services associés de l'entreprise suit un ensemble de procédures opérationnelle afin d'en assurer l'intégrité et la sécurité à moyen terme. Pour cela les procédures opérationnelles doivent être à jour. Elles doivent exister pour la supervision des éléments critiques et il est même souhaitable d'en faire pour la maintenance préventive qui permet de vérifier et corriger toute anomalie. Une sauvegarde des informations critiques doit être effectuée dans un lieu physique distinct de la source. Tout problème doit être détecté et résolu et la mise en place de contre-mesures permet de vérifier qu'aucun problème ne reste sans solution. Ces mêmes problèmes sont 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. Un certain nombre de règles de sécurité génériques doivent être définies afin de garantir la disponibilité et l'intégrité du réseau et de ses services. Il faut vérifier la consistance des plans d'adressage pour éviter les doublons dans le plan d'adressage global du réseau y compris celui des VPN. 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. Cela inclus la vérification de la syntaxe et de la grammaire du langage. Les filtrages réseau, utilisés pour contrôler les flux de données ou de routage, doivent être consistants. Pour cela il faut il faut s'assurer que les règles ne soient ni redondantes ni contradictoires et surtout éliminer les règles inutiles qui ne font qu'allonger le temps de traitement des équipements. Les règles de routages

comme la configuration des services doivent être vérifiée régulièrement pour s'assurer qu'elles sont à jour. Il s'agit, par exemple, de vérifier la topologie de routage interne et externe ou encore de vérifier le périmètre de sécurité d'un VPN MPLS ou IPsec.

- Sécurité physique

La sécurité physique est un facteur de la réussite de la politique de sécurité d'une entreprise et consiste essentiellement à se protéger contre les vols, fuite d'eau, incendies, coupures d'électricité et autres problèmes qui pourrait nuire au fonctionnement du SI. Par exemple, si une pièce qui contient des équipements informatiques peut être vue de l'extérieur, l'installation de rideaux permettra de ne pas susciter le vol ou le vandalisme. De même, une salle informatique n'est jamais installée au rez-de-chaussée pour éviter les risques d'inondation en cas de brusque montée des eaux. Un ou plusieurs périmètres de sécurité physique à accès restreint équipé d'appareil de vidéo surveillance peuvent être définis et les ressources les plus critiques doivent être installées dans le périmètre le plus sécurisé. Les modifications physiques d'infrastructure doivent être reportées et validées. Des contrôles d'accès physiques doivent être mis en place pour l'accès au périmètre de sécurité ainsi que des procédures qui autorisent et révoquent ces accès. Il faut éviter d'installer un site dans un lieu connu pour des catastrophes naturelles et des équipements contre la protection contre le feu, l'humidité et tous les autres problèmes nuisibles au bon fonctionnement du SI doivent être installés. Enfin, des procédures de supervision et de contrôle des équipements de protection doivent être mis en place.

- Plan de contingence

Les éléments critiques, identifiés lors de l'état des lieux de la phase de planification, doivent faire parti d'un plan global de contingence dont le but est de protéger le périmètre de l'entreprise. Le temps de restauration d'un service après désastre devient critique pour l'entreprise s'il vient à se prolonger car les impacts peuvent prendre la forme de perte de revenu ou d'image de marque. Il n'est pas facile d'estimer le temps minimal à partir duquel l'entreprise est mise en difficulté mais il est sûr que l'impact sur celle-ci croît de façon exponentielle en fonction du temps. Pour éviter le pire, les ressources critiques de l'entreprise doivent être identifiées, classées et faire partie du plan de contingence. Ce dernier détaille les priorités, précise les temps de rétablissement de chaque ressource, référence les procédures nécessaires et doit faire l'objet d'une revue régulière qui tient compte des évolutions organisationnelles et techniques.

- Audit de la sécurité

Le fait de définir une politique de sécurité n'implique pas toujours sa correcte implémentation. L'audit interne, par l'équipe de sécurité, ou externe, par une tierce partie est primordiale pour s'assurer du degré d'application ou de déviation de la politique de sécurité réseau. L'audit, véritable état des lieux de la sécurité physique et logique, dégage les dispositions générales prises concernant la sécurité et identifie les vulnérabilités techniques et organisationnelles afin de proposer des recommandations lucides et réalistes. Afin d'éviter de se perdre dans des détails sans intérêt, l'approche classique consiste à définir un plan d'audit détaillé afin de cerner les éléments critiques. Ce plan comprend des contrôles de sécurité réguliers qui se closent par des rapports. Les audits doivent être définis en accord avec l'équipe sécurité qui doit approuver l'utilisation d'outils ou la sauvegarde de données. Les rapports d'audit doivent être présentés au comité de sécurité qui définit les actions à prendre.

Ce *« framework »* permet, à travers l'écriture de ces procédures, d'identifier les processus qui composent l'entreprise, un peu comme le ferait une certification ISO 27001. A l'instar de la certification ISO 27001, l'objectif du *« framework »* n'est pas d'augmenter la satisfaction du client mais bel et bien d'accroître l'efficacité en proposant une approche transversale. Cette approche, qui identifie les différents corps de métiers de l'entreprise engagés dans un processus, garantit voire

accélère le bon déroulement du dit processus. Prenons comme exemple l'embauche d'un nouvel administrateur de serveurs de mails. La **D**irection des **R**essources **H**umaines (**DRH**) définit la procédure avec laquelle le service informatique va pouvoir définir la fiche de poste. Ensuite, une deuxième procédure indique que pour les postes rattachés à la **D**irection du **S**ervice **I**nformatiques (**DSI**), les entretiens d'embauche sont menés avec un employé de la DRH et un autre de la DSI. 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. 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 (cf. *gestion des accès logiques*). Pour terminer, 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...). L'ensemble de ces procédures appartiennent au processus d'embauche, qui utilise de manière transversale trois services de l'entreprise : la DSI, la DRH et les achats. Le processus est représenté sur la figure ci-dessous.

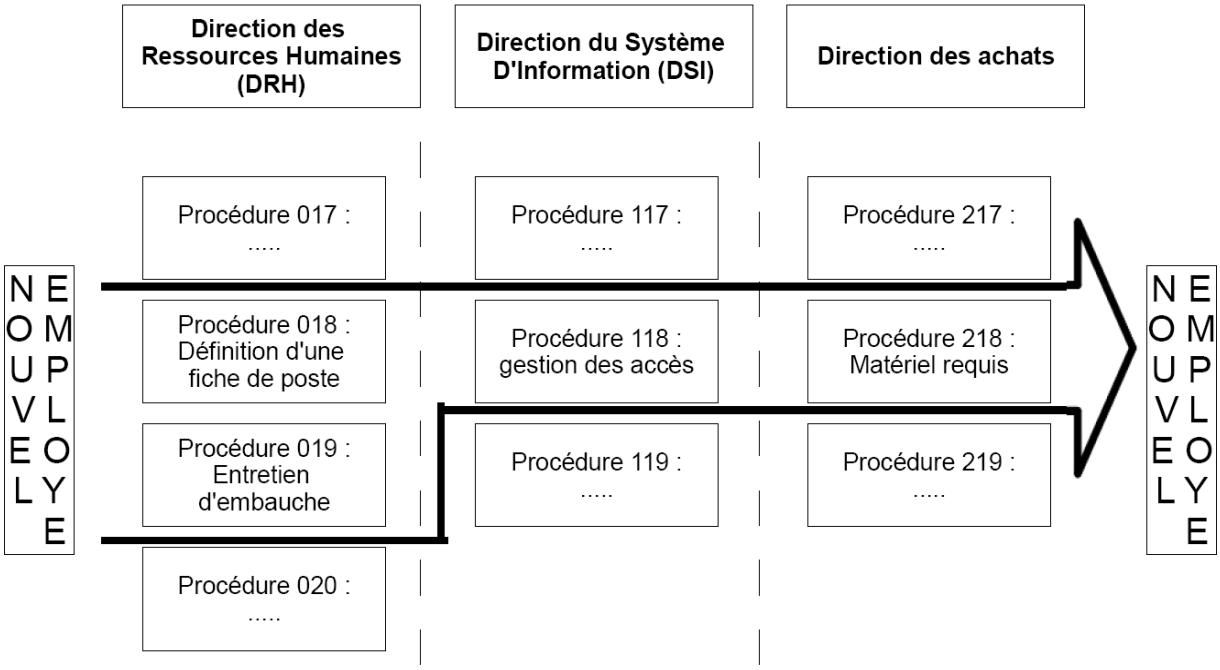

Figure9. Processus d'embauche mis en place grâce au *« framework »*

On pourrait facilement imaginer, de la même façon isoler le processus du contrôle de serveur de mail qui regrouperait des procédures appartenant aux domaines *« exploitation et administration »*, *« vérification des configurations »*, *« sécurité physique »* et *« audit de sécurité »*.

Maintenant que le « framework » est en place, attardons nous sur l'implémentation de la politique de sécurité réseau grâce aux stratégies de sécurité.

3.2. Stratégies de sécurité

L'établissement de stratégies de sécurité exige de prendre en compte l'historique de l'entreprise, l'étendue et l'organisation de son réseau, son nombre d'employés, de prestataires ou encore le nombre de serveurs. Une bonne stratégie de sécurité vise à définir et mettre en œuvre des mécanismes de sécurité, des procédures de surveillance des équipements de sécurité et même des procédures de réponse aux incidents de sécurité et des audits de sécurité. Cette mise en place de la stratégie est débutée par une analyse de risque permettant de pondérer les risques encourus.

a) Gestion des risques

La première étape consiste à déterminer les menaces qui pèsent sur les ressources de l'entreprise, ainsi que leurs impactes si elles devaient se concrétiser. Les risques de sécurité sont déterminés par le triptyque menace / vulnérabilité / conséquence, déjà abordé dans l'EBT, et que nous allons succinctement revoir. Pour commencer, **le risque** est *« la moyenne des conséquences des événements affectés de leur probabilité d'arriver »*. **Une vulnérabilité** est *« une faiblesse de sécurité qui peut être de nature logique, comme par exemple une faille logiciel, ou de nature physique comme une panne de courant »*. La menace représente *« l'exploitation d'une vulnérabilité par une personne tierce »*. Pour terminer, la conséquence est *« l'impacte sur l'entreprise de l'exploitation d'une vulnérabilité »*. Le rôle de la gestion des risquex est de prévenir les menacex car elles ont un impact négatif sur les trois composantes protégées par les objectifs de sécurité que nous avons décrites dans le chapitre 2.1 : l'intégrité, la confidentialité et la disponibilité.

Le risque est évaluable de manière plus qualitatif grâce à la formule communément admise :

Risque = MAX [Confidentialité, Intégrité, Disponibilité] x vraisemblance

Cependant cette formule nécessite d'évaluer les menaces qui pèsent sur chacun des critères précédents, chose qui n'est simple, et d'utiliser la composante la plus menacée.

Maintenant que la gestion des risques est redéfinie, attardons nous sur l'élaboration d'une stratégie de sécurité réseau.

b) Méthodologie pour élaborer une stratégie de sécurité

La première étape de l'élaboration de la stratégie consiste à faire de la gestion des risques pour dégager les ressources critiques de l'entreprise et les menaces qui planent sur elles. Pour protéger les biens critiques des menaces identifiées, il faut analyser les techniques d'attaques utilisées pour tirer partie des vulnérabilités. Ce niveau d'analyse plus poussé permet de définir des stratégies de sécurité pro-actives, visant à diminuer les probabilités d'occurrences des menaces. Les différentes catégories de menaces qui pèsent sur le système d'information ou sur le réseau sont représentées sur la figure 10. Les menaces non intentionnelles ou imprévisibles, comme les catastrophes naturelles, ne mettent pas en œuvre de stratagèmes particuliers et n'ont pas d'objectifs déterminés. A contrario, les attaques intentionnées utilisent pléthores d'outils et de techniques d'attaques. Beaucoup d'études montrent que les trois quart, voire les 80% des attaques, proviennent de l'intérieur de l'entreprise. Faces aux menaces identifiées lors de l'analyse de risque, il faut adopter des stratégies pro-actives et réactives dans tous les cas, chose que nous allons maintenant aborder.

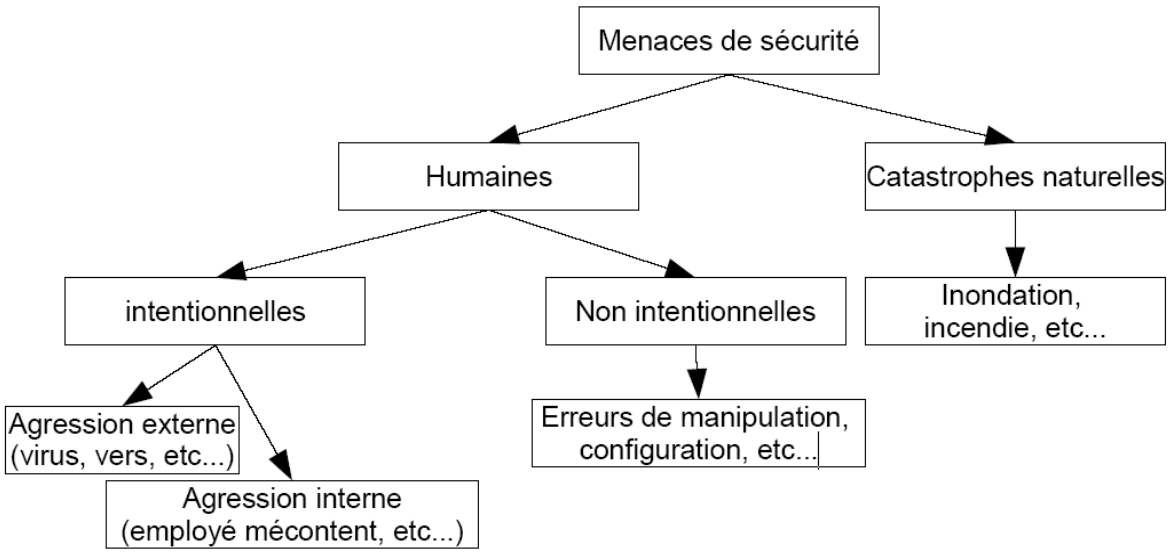

Figure10. Analyse des menaces qui planent sur le SI

- Règles élémentaires

Lors de l'établissement d'une stratégie de sécurité il faut garder à l'esprit quelques règles élémentaires. Tout d'abord, plus une stratégie de sécurité est complexe, plus son implémentation, amélioration et évolution seront difficiles. Simplicité et pragmatisme sont des critères de réussite. La règle du maillon le plus faible est également à garder à l'esprit. Par exemple, intéressons-nous au périmètre d'une l'entreprise qui aurais trois moyens d'accéder à son réseau interne. Deux moyens sont des équipements implémentant de la sécurité comme un pare-feu et une passerelle VPN et le troisième moyen est un routeur sans aucune couche de sécurité. Le troisième moyen d'accès constitue une faiblesse qui sera privilégié par le pirate pour effectuer son attaque. La variété des protections mise en place est également importante. Dans l'exemple précédent on s'intéressera à un seul moyen d'accès composé de deux pare-feu identiques (même équipementier et même technologie). Si le pirate réussit à utiliser une vulnérabilité sur l'un des pare-feu pour pouvoir le contourner, il y a de grande chance pour qu'il puisse l'utiliser également sur l'autre. Si les pare-feu sont de marques différentes, les vulnérabilités sont différentes, et il aura alors plus de mal à pénétrer dans l'intranet de l'entreprise. La sécurité ne doit jamais reposer sur un seul mécanisme de sécurité et une imbrication de mécanisme offre un degré de protection supérieur face à la défaillance de ceux-ci. Par exemple, pour accéder à un serveur sur un réseau distant, il est possible de fournir un premier mécanisme de sécurité d'authentification comme une passerelle VPN (avec IPsec ou SSL). Une fois l'individu authentifié sur le réseau, il faut encore qu'il se connecte au serveur, et pour cela on peut utiliser un mécanisme de chiffrement de session comme SSH. Cette imbrication, impose au pirate de contourner deux barrières au lieu d'une et de natures différentes (authentification et connexion). La séparation logique et physique des protections de sécurité permet de ne pas concentrer la sécurité en un seul point qui devient alors un point de faiblesse. Cette séparation engendre des compartiments étanches de sécurité ainsi qu'une meilleure implémentation des fonctions de sécurité sur des matériels dédiés. En effet, sur des équipements UTM (*« **U**nified **T**hreat **M**anagment »*), qui remplissent plusieurs fonctions de sécurité comme celle de passerelle VPN, routeur, pare-feu ou encore anti-virus, comment savoir dans quel ordre ces fonctions seront exécutées. De plus, plus l'équipement assure de fonctions et plus sa configuration est complexe et difficile à maintenir. Cependant, la solution de séparation est très souvent beaucoup plus onéreuse que l'achat d'un UTM. Les différentes simulations sont l'occasion d'améliorer les contre-mesures de sécurité, voire de les remettre en question. Effectivement, si on constate que certains types d'attaques ne sont pas détectés par un pare-feu, soit les règles de filtrages soit le pare-feu ne sont pas adaptés. Il est également important de valider l'efficacité des stratégies de sécurité mise en place

face aux simulations utilisées. Si la stratégie existante n'a pas apporté de bons résultats, il faut soit la modifier soit en implémenter une nouvelle.

- Stratégie pro-active (dite de prévention)

Une stratégie pro-active comporte plusieurs étapes prédéfinies qui doivent être exécutées afin de se prémunir d'attaques identifiées. Elle doit évaluer les dommages causés par une attaque et mesurer les impactes qui peuvent aller de la perte mineur, comme le redémarrage de la machine, jusqu'à la perte totale du bien attaqué (réinstallation de la machine). Elle évalue ensuite le degré de vulnérabilité et les faiblesses exploitées par une attaque pour en définir les contre-mesures à mettre en place. L'objectif est de réduire les risques liés à cette attaque. La dernière étape de cette stratégie consiste à la mise en place d'un plan de contingence ou *« Business Continuity Plan »*, visant à définir les actions à mettre en place. Ce plan définit pour chaque tâche à exécuter, la personne et le moment de l'exécution. Pour finir, il doit adresser le problème de restauration des données. Le plan doit faire l'objet d'exercices réguliers pour que, le jour de son application réelle, le personnel soit prêt.

- Stratégie réactive

La stratégie réactive définit les étapes à mettre en œuvre après ou pendant un incident et suppose que la stratégie pro-active a échouée. Elle analyse l'incident de sécurité afin de déterminer le périmètre des dommages causés ainsi que les stratagèmes utilisés pour mener l'attaque, pour décider des actions à prendre. Le plus important est de déterminer la cause de l'incident par tous les moyens possibles comme les événements de journalisation (*« logs »*) des équipements réseaux ou encore par la détection de signature de programme comme les virus, vers ou chevaux de Troie sur les systèmes attaqués. Un test de pénétration doit être réalisé pour confirmer la vulnérabilité exploitée par l'intrus. L'étape suivante consiste à réparer les dommages causés par l'attaque et vient naturellement à la fin de l'analyse *post-mortem* de façon à ne pas écraser les traces de l'incident de sécurité. Les leçons tirées de cet incident doivent faire l'objet d'un rapport qui détaille les aspects techniques, comme les dommages causés ou les moyens mis en œuvre, et analyse l'impact de l'incident sur l'entreprise comme la baisse de productivité, la fuite d'information ou encore les données perdues. Ce rapport permet dévaluer l'aspect financier de l'incident de sécurité et d'améliorer les stratégies de réduction des risques. La mise en œuvre d'un plan de contingence peut être envisagé selon la criticité du bien impacté ou si l'analyse *post-mortem* prend trop de temps. Il permettra de résoudre la crise plus rapidement, même en mode dégradé.

Maintenant que nous avons fait le tour des règles élémentaires ainsi que de la méthodologie pour aborder les stratégie de sécurité, intéressons nous aux différentes stratégies de sécurité qui existent.

c) Quelques stratégies de sécurité réseau

Les stratégies de sécurité doivent être considérées comme des briques à adapter afin de construire une stratégie personnalisée. Les stratégies suivantes seront abordées avec comme exemple le réseau d'une entreprise connectée à Internet et qui comporte trois sous-réseaux, un de production, un de **R**echerche et **D**éveloppement (**R&D**) et un de bureautique.

- Stratégie des périmètres de sécurité

L'objectif est de découper le réseau d'entreprise en périmètres de sécurité logiques regroupant des entités ou fonctions afin de mettre en place des niveaux de sécurité à la fois imbriqués et séparés. La première étape est la définition d'un périmètre de sécurité autour du réseau d'entreprise face au réseau Internet. Il faut également définir un périmètre de sécurité autour de chacun de ces réseaux inclut dans le réseau intranet. Cette compartimentation du réseau intranet rend plus difficile une éventuelle pénétration. Cependant cette stratégie n'est pas suffisante est doit être couplée avec celle des goulets d'étranglement.

- Stratégie des goulets d'étranglement

L'objectif est de définir des contrôles d'accès différenciés et en nombre limités pour permettre l'accès à chaque périmètre de sécurité du réseau intranet. Les contrôles d'accès définissent ce qu'il est autorisé de faire pour entrer dans un périmètre de sécurité du réseau. Tout ce qui n'est pas autorisé doit être interdit et les contrôles d'accès définissent les conditions à respecter pour avoir le droit d'entrer dans un périmètre donné. Les contrôles d'accès s'accompagnent des quelques règles évidentes suivantes :

- chaque système ne dispose que d'une seule connexion au réseau d'entreprise pour éviter les attaques par rebonds. Effectivement, si un ordinateur est connecté au réseau de l'entreprise d'un côté et de l'autre à Internet, un pirate pourrait, depuis Internet rebondir dans le réseau intranet ;
- Internet est un outil de travail et ne doit être utilisé que dans un cadre professionnel ;
- des contraintes sont installées sur les stations de travail pour éviter les installations de programmes non validées par l'équipe technique ;
- les logiciels de sécurité installés sur le poste doivent être mis à jour régulièrement ;
- interdiction d'utiliser un outil qui permettrait d'obtenir des informations sur le réseau de l'entreprise (scanner de vulnérabilité, outil de découverte de réseau, etc...).

Les communications entre le réseau intranet et d'autres réseaux doivent être contrôlées et les services réseau accessibles sur Internet définis. Ces flux doivent être également contrôlés pour vérifier qu'il ne véhiculent pas de virus. Une solution de filtrage de contenu pourra être mise en place pour s'assurer que les employés ne naviguent pas sur des sites interdits par la loi (pédophiles, pornographiques, pirates, etc...). Des mécanismes de surveillance doivent être appliqués aux périmètres de sécurité et toucher les domaines suivants : collecte et stockage des logs, analyse des attaques (comme les sondes d'intrusion) ou encore l'analyse de trafic.

Maintenant que les périmètres sont définis ainsi que les goulets d'étranglement, attelons nous à authentifier les utilisateurs du réseau.

- Stratégie d'authentification en profondeur

L'objectif est de mettre en place des contrôles d'authentification pour authentifier les accès aux périmètres de sécurité. Pour faire cela, il est recommandé d'installer des systèmes de contrôle d'authentification au sein d'un périmètre qui leur est réservé. Ces contrôles peuvent avoir lieu au moment de la sortie sur Internet mais également au niveau de chaque serveur pour accéder au réseau interne. Chaque fois qu'un utilisateur s'authentifie, un ticket est créé sur un système chargé de stocker les logs afin que le parcours de l'utilisateur soit connu à tout moment. Cette logique peut être étendue à chaque action de l'utilisateur comme la création, suppression ou impression d'un document ou encore les adresses Web visitées. Lorsqu'un tel système est mis en place on parle de modèle AAA (*« Authentication, Authorization, Accounting »*) ou authentification, autorisation et comptabilité d'événements. Cependant la mis en place de ce type de système est lourde et souvent très coûteuse.

Voici un aperçu de notre réseau après la mise en place de ces trois stratégies de sécurité.

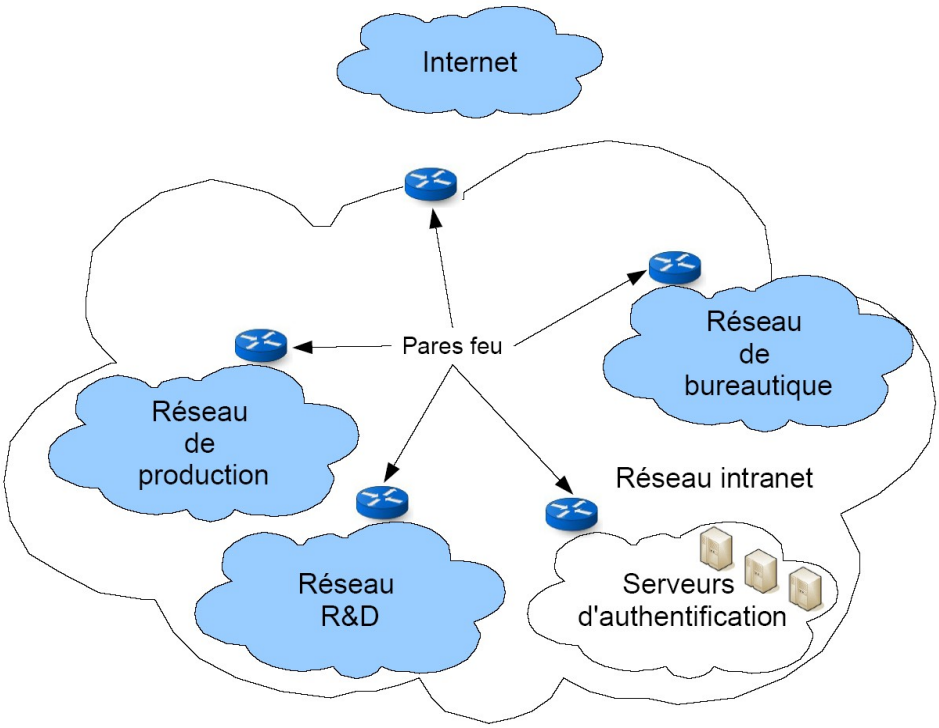

Figure11. Obtention d'une stratégie personnalisée

On peut voir les zones qui ont été définies par la stratégie des périmètres de sécurité, les pare-feu qui constituent l'unique point d'entrée pour chaque zone, comme spécifié dans la stratégie par goulets d'étranglement. Enfin, on voit également les serveurs d'authentifications qui servent à authentifier les accès aux périmètres de sécurité, comme spécifié dans la stratégie d'authentification en profondeur.

- Stratégie du moindre privilège

Cette stratégie a pour objectif d'assurer que chacun dispose uniquement des privilèges dont il a besoin. La porté de tout acte de malveillance s'en retrouve réduite aux privilèges dont dispose la personne qui le commet et il faudra une complicité de plusieurs personnes pour pouvoir mettre en péril le réseau intranet. Un moyen facile de renforcer cette stratégie est d'augmenter les autorisations nécessaires pour accéder à une ressource. Par exemple, pour accéder aux données comptable, la comptable a besoin de son code et de celui de sa responsable. Cependant, ce

mécanisme implique des contraintes supplémentaires de disponibilité, qui font qu'une comptable ne pourra accéder aux données comptables si sa responsable est en vacances. L'application stricte de cette stratégie est difficile à réaliser et souvent possible qu'avec la mise en place d'un système SSO (*« **S**ingle **S**ign **O**n »*), qui permet d'authentifier un utilisateur quelle que soit son adresse réseau et de lui appliquer un profil à droit d'accès spécifique.

- Stratégie de confidentialité des flux réseau

L'objectif de cette stratégie est de protéger tout message qui doit être émis vers un autre réseau ou Internet. Cette stratégie est généralement utilisée lorsqu'une entreprise a plusieurs sites qui sont reliés par le biais de réseau public comme Internet, X25 ou encore de **L**igne **S**pécialisées (**LS**). Lorsqu'une entreprise créé un réseau de type WAN, elle construit un réseau centrale (*« backbone »*) et relie ces sites à ce réseau. Des boîtier de chiffrement, telles que des passerelles IPsec, peuvent être installés entre les routeurs et les pare-feu pour garantir la confidentialité des communication inter-sites. Ainsi, tous les flux qui sortent de chaque site sont chiffrés à la volée par le boîtier de chiffrement placé en goulet d'étranglement sur les connexions inter-sites. Il existe d'autres moyens de chiffrer les communications comme SSL, qui est très utilisé pour chiffrer les flux des serveur Web.

- Stratégie de séparation de pouvoir

L'objectif est de créer des entités séparées chacune responsable de zones de sécurité distinctes du réseau intranet. Cette stratégie s'adresse particulièrement aux entreprises de grande taille. En effet, les petites entreprises, qui n'ont pas beaucoup de ressources à protéger, se contentent souvent d'un seul département chargé de leurs maintenance. En revanche, dans des entreprises plus grandes il est nécessaire de séparer ou limiter les pouvoirs de chaque entité afin de limiter les conséquences d'un acte de malveillance. On peut prendre comme exemple une entité qui serait en charge d'assurer une fonction opérationnelle et d'en assurer le contrôle. S'il n'y a pas de séparation, il est pratiquement certain que les procédures de contrôle les plus contraignantes seront ignorées, créant ainsi une faiblesse de sécurité.

Maintenant que des responsables sont définis pour chaque périmètre, il s'agit de contrôler tous les accès à ces périmètres.

- Stratégie d'accès au réseau local

L'objectif de cette stratégie est d'assurer qu'aucune porte dérobée interne ne permettent d'accéder au cœur du réseau. Pour contourner ce risque, il faut créer un contrôle d'accès à toutes les portes d'entrée du périmètre de sécurité. Ce contrôle sera sous la responsabilité du périmètre de sécurité qui déterminera la politique d'accès à mettre en œuvre. Pour y parvenir, il faut que tous les premiers éléments intelligents d'accès au réseau (commutateurs ou routeurs) fasse un contrôle d'accès. La technologie AAA, vue précédemment est particulièrement adaptée.

Maintenant que les postes et responsables sont définis il s'agit d'assurer une gestion ou administration sécurisée de chaque périmètre de sécurité.

- Stratégie d'administration sécurisée

L'objectif de cette stratégie est de créer une zone d'administration, dédiée et séparée du réseau afin d'assurer une isolation des systèmes chargés de l'administration de chaque périmètre de sécurité. Une zone d'administration est en charge de vérifier le bon fonctionnement de tous les composants d'un périmètre de sécurité donné. Cette zone est donc particulièrement sensible et doit être protégée de manière adéquate. Cette stratégie est à mettre en place avec celle des goulets d'étranglement qui visent ici à réduire le nombre de point d'entrée dans les zones d'administration.

Toute politique de sécurité réseau s'accompagne de stratégie ayant pour objectif d'établir un premier niveau de règles de sécurité et, dans un deuxième temps, de mettre en œuvre des solutions techniques. Les architectures réseau et les services offerts deviennent tellement complexes qu'il faut remettre en cause les mécanismes de sécurité préalablement définis le plus souvent possible. Cette adaptabilité et cette réactivité vont permettre à l'entreprise de protéger au mieux ces périmètres de sécurité.

Cette phase de déploiement a permit de mettre en place un *« framework »* pour permettre d'utiliser la documentation afin d'identifier les différents processus qui gravitent autour de la sécurité des réseaux. Elle a également permit d'aborder les différentes stratégies de sécurité réseau, qui permettent l'application des objectifs de sécurité vus dans la phase de planification. Ces stratégies doivent être couplées entre elles pour produire une nouvelle stratégie de sécurité réseau parfaitement adaptée à l'entreprise. Attardons nous maintenant sur le contrôle et l'amélioration de ces entités nouvellement mise en place.

4. Contrôle et amélioration

Dans la PSSI généraliste, les phases de contrôle et d'amélioration sont constituées de la mise en place de tableaux de bord et d'audit de sécurité. Le tableau de bord, composé d'indicateurs de fonctionnement, *« permet aux responsables de la sécurité de l'entreprise de s'assurer de la performance du système et de l'avancement des travaux qui soutiennent la vision et la stratégie de l'entreprise »*. Quant à l'audit de sécurité, il constitue *« un outil central pour détecter les écarts de conformité et ainsi déclencher les corrections nécessaires »*. Ces deux entités sont également présentes dans la phase de contrôle et d'amélioration de la politique de sécurité réseau, et nous allons commencer par aborder les audits

4.1. Les audits de sécurité

a) Contrôle externe

Les contrôles externes de la sécurité consistent à vérifier, de l'extérieur et sans droit d'accès aux systèmes composant le réseau de l'entreprise, que les règles de sécurité, définies dans la phase de planification et mises en place dans la phase de déploiement, sont fonctionnelles. Ce contrôle externe porte en priorité sur l'analyse des systèmes de l'entreprise, en se plaçant à des endroits stratégiques du réseau, et sur l'analyse externe des systèmes de l'entreprise. Ces contrôles doivent être réguliers et automatisés au maximum afin de gagner du temps pour l'analyse. Ils doivent également tenir compte de la politique de sécurité et de l'évolution des architectures et des services réseau. Ces contrôles 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.

- Système d'auditeurs distribués

Pour des raisons d'optimisation, le système en charge d'assurer les contrôles peut être une infrastructure distribuée contenant plusieurs systèmes de contrôle. Un système maître dispose d'une base de données associant à chaque sous-réseau de l'entreprise une machine d'audit dédiée qui lancera les contrôles. Cette distribution permet d'optimiser la bande passante disponible et donc d'effectuer plus rapidement les contrôles. On peut voir plusieurs avantages à une architecture d'auditeurs distribuée par rapport à une architecture centralisée. Le premier est la décentralisation de la gestion qui permet de créer des sous-réseaux logiques, gérés localement tout en restant dépendant d'une administration centrale. Le mode distribué permet également de tester les mécanismes de sécurité à l'intérieur de chaque zone sans avoir à désactiver les équipements de sécurité qui se trouvent à la périphérie. La performance des vérifications est induite par une charge réseau partagée et non localisée en un seul point de test. La création des rapports est effectuée sur les machines distantes et remontés à l'administration centrale. Pour terminer, chaque zone d'autorité a ses propres paramétrages de vérification et listes d'exception, ce qui permet d'adapter les tests aux contraintes locales des zones.

Attardons nous maintenant sur les différentes techniques de contrôle.

- Contrôle par balayage réseau

Dans la plupart des cas 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 offre des services réseaux tel que le Web ou encore la messagerie. Malheureusement, la plupart des systèmes d'exploitation ne proposent que des logiciels d'administration à distance fonctionnant en flux non chiffré. La politique de sécurité exige que, pour chaque système, le service utilisé pour accéder à distance soit authentifié et que les flux entre le client et le serveur soient chiffrés. Cette politique de sécurité peut être déclinée en guide détaillant la liste des logiciels à utiliser à des fin d'administration :

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

Pour la mise en œuvre du plan de contrôle externe, il importe de choisir un outil susceptible de couvrir le besoin de balayage de port, comme Nmap. Cet outil est la référence en matière de balayage de port et, de plus, il fonctionne en ligne de commande, ce qui va permettre de créer un script de lancement automatique. Cependant, l'automatisation ne se résume pas au seul lancement de l'outil mais comprend également la collecte des résultats et de la comparer à un modèle afin de déterminer les écarts.

Le processus de contrôle externe par un scanning réseau se déroulerait comme indiqué sur la figure ci-dessous.

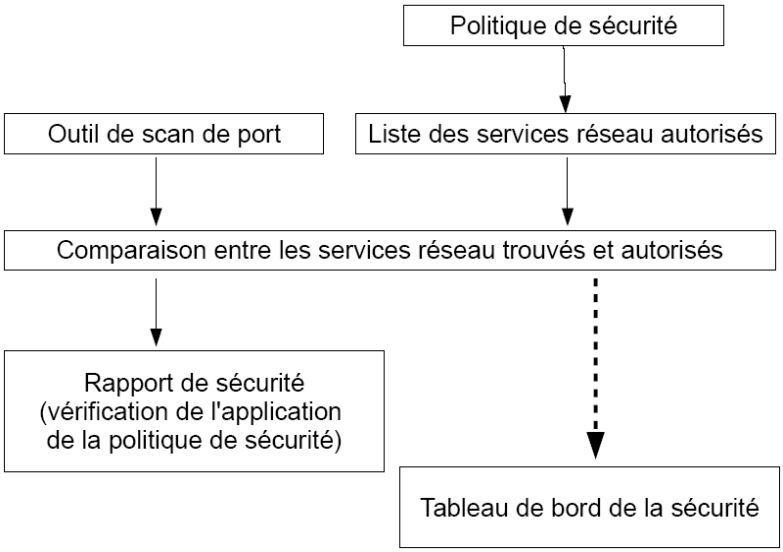

Figure12. Déroulement du processus de contrôle externe de balayage de ports

- Contrôle par analyse des applications

Le balayage des ports permet de se faire une idée de la sécurité d'une plate-forme mais n'est pas suffisant pour déterminer si un service réseau est sécurisé. Pour affiner la qualité des contrôles de sécurité, il faut que ces derniers s'intéressent à la couche application (niveau 7 OSI). Le contrôle doit inclure des échanges de données avec le protocole applicatif pour s'assurer du service réseau et détecter d'éventuelle vulnérabilités. Des outils comme Nessus permettent de mettre en place de tels contrôles. Ils sont généralement composés d'un client, qui peut être en mode texte (toujours pour l'automatisation), et d'une partie serveur chargée de lancer les vérifications sur la machine cible.

Certains systèmes sont plus exposés que d'autres à des attaques, comme ceux accessibles depuis Internet, ou contiennent des données critiques pour l'entreprise. Pour ces systèmes plus sensibles, il n'existe pas d'outil miracle qui permettrait de trouver l'ensemble des faiblesses possibles. Seule l'expérience et la compétence d'un auditeur permettent d'approcher ce « Graal » de la sécurité. Il s'agit là de la frontière entre l'outil et l'expertise en matière de sécurité.

- Cas particulier des réseaux sans fil

Les réseaux sans fil échappent aux solutions de contrôle précédemment citées, qui partaient sur le postulat que l'auditeur et la machine cible étaient connectes à un réseau leurs permettant de communiquer via TCP/IP. Dans le cas des réseaux sans fil, le contrôle de la politique de sécurité doit s'effectuer avant l'attribution d'une quelconque adresse. Effectivement, la technologie sans fil repose sur des communications hertziennes, qui permettent d'interagir avec les machines connectées au réseau sans pour autant disposer d'une adresse légitime. Les premiers visés par les contrôles sont les points d'accès.

Un point d'accès est par nature hautement exposé, puisque les données transitent par le biais d'ondes radio qui peuvent être capturées par n'importe quelle machine se trouvant à porté du signal. De plus un ordinateur désirant se connecter à un point d'accès sans fil doit savoir que celui-ci existe; alors, soit le point d'accès s'annonce, soit l'utilisateur dispose d'une information permettant de se connecter sans que cette annonce soit nécessaire.

Une distribution Linux, appelé Whax [W2], est particulièrement pratique car elle est composée d'une multitude d'outils de contrôle.

La réalisation et l'automatisation de contrôles externes permettent de vérifier de l'extérieur qu'un système implémente les règles de sécurité issues de la politique de sécurité réseau. Si dans certains cas les outils suffisent à démontrer les vulnérabilités et non conformités d'un système, dans d'autres l'avis d'un expert de la sécurité est indispensable. Penchons nous maintenant sur les contrôles internes qui visent à vérifier qu'un système respecte bien la politique de sécurité mais, cette fois-ci, de l'intérieur.

b) Contrôle interne

Le contrôle interne de sécurité porte en priorité sur l'analyse de la configuration des équipements comme les routeurs ou commutateurs ainsi que des services réseau comme le DNS (*« **D**omain **N**ame **S**ystem »*) ou encore NTP (*« **N**etwork **T**ime **P**rotocol »*). La configuration des systèmes d'information est également à prendre en compte comme les serveurs ou les stations de travail. Enfin, il est important d'installer des équipements de sécurité chargés de faire de l'écoute passive du réseau et d'analyser leurs journaux d'activité. Les contrôles internes doivent être effectués de manière régulière et doivent prendre en compte les évolutions de la politique de sécurité, des architectures, des services ou plus généralement du SI.

- Analyse de la configuration des équipements réseau

La configuration des équipements réseau représente la sécurité logique du réseau et se traduit par des règles de configuration précises, telles que la configuration des règles de filtrage d'un pare-feu ou d'un routeur. Toutes ces règles représentent l'implémentation de la politique de sécurité réseau. Des problèmes de consistance ou des erreurs dans la configuration de ces équipement réseau, volontaires ou non, peuvent mettre en danger les équipements attachés au réseau puis le réseau lui même. Ces problèmes de consistance peuvent venir de règles de filtrage, ou d'ACL (*« **A**ccess **C**ontrol **L**ist »*) définies mais jamais appliquées voire, d'ACE (*« **A**cess **C**ontrol **E**ntry »*) redondantes ou contradictoires au sein même d'une ACL.

Imaginons qu'une personne mal intentionnée prenne pied sur un routeur de l'intranet suite à une faiblesse de configuration des accès en administration. Cette personnes peut modifier des filtres, les mots de passe de l'équipement, écouter le réseau au travers d'un tunnel GRE (*« **G**eneric **R**outing **E**ncapsulation »*) ou même faire chuter le réseau en altérant les tables de routages. Altérer un processus de routage est simple, rapide et généralement très efficace : plus de routage, plus de trafic et donc plus de réseau. L'analyse de la configuration des équipements réseau est donc un axe majeur de la sécurité du réseau. L'outil RAT (*« **R**outer **A**udit **T**ool »*) peut être utiliser pour contrôler la consistance de sa configuration.

- Analyse de la configuration des équipements de sécurité passifs

Les équipements de sécurité passifs, tels que sondes de détection d'intrusion IDS (*« **I**ntrusion **D**etection **S**ystem »*), table d'écoute, pots de miel *« honeypots »* ou sonde de prévention d'intrusion IPS (*« **I**ntrusion **P**revention **S**ystem »*), n'ont pas pour fonction de protéger le réseau ou le SI. Ils sont chargés d'effectuer des contrôles pro-actifs ou réactifs, selon la manière dont ils sont paramétrés et contrôlés. Ces équipements n'ont pas un rôle actif dans le réseau mais c'est l'analyse de leurs logs qui apporte l'information importante et font pleinement partie des contrôles internes de sécurité. La vérification de l'application de la politique de sécurité consiste à définir un contrôle interne de sécurité sur les fichiers de configuration des ces équipements, mais également de contrôler leurs logs. Les étapes pour y parvenir sont illustrées par la figure 13.

Une sonde IDS ne sert pas à détecter une intrusion à proprement parler mais signale tout comportement anormal du réseau que ce soit sous forme d'un paquet de données mal formé ou d'un flux réseau non autorisé par la politique de sécurité. De même, une sonde IPS ne sert pas à détecter un intrus avant qu'il ne commence à agir mais analyse le trafic réseau et produit une matrice statistique de flux qui indique quels flux sont en transit (adresse IP source et destination, port et protocoles) et la bande passante que chacun d'eux consomme. La configuration de la sonde a pour but de lui indiquer le critère à partir duquel le comportement réseau est anormal. Par exemple, un réseau constitué de station de travail Windows s'échange normalement des flux sur les port 139/TCP (Netbios Session), 137/UDP (Netbios Name) et 138/UDP (Netbios Datagram). En présence d'un ver (ce que les IPS savent le mieux détecter) s'appuyant sur le port « Netbios Session » pour se

dupliquer, la bande passante habituelle du flux 139/TCP commence à augmenter sans motif apparent. La sonde remonte alors une alerte qui permet à l'équipe de sécurité de mener une enquête en soupçonnant sans difficulté la présence d'un nouveau ver *Microsoft* et l'éradique avant que sa propagation devienne incontrôlable. Ces sondes peuvent aussi être actives et déclencher des actions en fonction de critères. On dit que la sonde est pro-active, car elle réagit à la détection de l'événement au lieu de se contenter de la signaler. Cependant il est déconseillé de les configurer dans ce mode car elles peuvent être utilisées par des pirates contre le réseau.

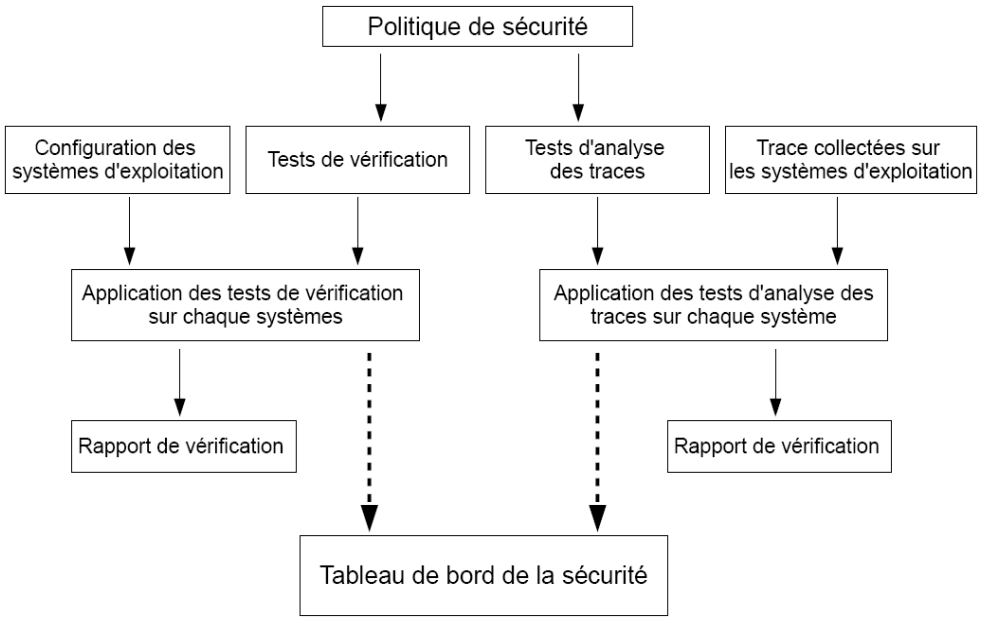

Figure13. Processus de vérification des configuration et traces des systèmes

- Les pots de miel ou « *honeypot* »

Les pots de miel ont pour fonction d'attirer les personnes malveillantes par leur prestations alléchantes, afin que celles-ci tentent de nuire au système. Cependant, l'accès au pot de miel peut être fait de manière non intentionnel par une personne se trompant de machine. S'il s'agit d'une erreur, l'incident est rapidement clos par l'utilisateur qui réalise son erreur ou appelle au secours un centre d'appel utilisateur. A l'inverse, la personne malveillante reste collé au pot de miel et tente différentes approches afin de trouver le point le plus faible. Le pot de miel permet ainsi aux équipes de sécurité de commencer leur enquête visant à déterminer l'origine de l'attaque ou de trouver son véritable point de départ ainsi que les moyens utilisés. L'intrus peut effectivement avoir pris le contrôle de plusieurs machines et rebondir sur celles-ci avant de tomber sur le pot de miel. D'ordre général, dès qu'un pot de miel est attaqué par des méthodes comme le balayage de port, la prise d'empreinte ou encore la tentative de débordement de tampon sur un des services réseau, il faut au plus vite remonter une alerte.

- Corrélation d'événements

L'inconvénient majeur des sondes d'intrusion et du pot de miel, est que chacun d'eux est indépendant de l'analyse des autres. Par conséquent, chaque sonde ou pot de miel rapporte une anomalie en fonction de sa connaissance limité du réseau. Afin de réduire le nombre de faux positifs (alertes sur des incidents qui n'existent pas), il est nécessaire de corréler l'information avec d'autres sondes mais également avec les traces des équipements filtrant comme les pare-feu, voire des traces associées aux systèmes d'exploitation. Certaines solutions permettent de corréler les événements

avec plus ou moins d'efficacité. *Snort*, une sonde d'intrusion gratuite, propose sa console *Demarc* pour corréler les événements de plusieurs sondes *Snort*.

Cependant, lorsque les sources d'information sont de natures différentes, il faut mettre en œuvre des solutions à la fois plus robustes et plus flexibles, permettant en premier lieu de transformer les différents formats d'alertes en un format uniforme, mais également d'offrir la possibilité de créer des alertes en fonction de différents types d'événements, soit de manière simplifiée, soit par l'utilisation d'un macro langage. Dans tous les cas une architecture doit être crée pour permettre la collecte des alertes et l'élimination des faux positifs, afin que seuls les événements véritablement significatifs soient rapportés. Des logiciels comme *OSSIM (« **O**pen **S**ource **S**ecurity **I**nformation **M**anagement »)* ou *OSSEC* proposent des outils pour traiter les fichiers de logs mais leurs configurations restent fastidieuses et sans mécanisme automatique de remonter des fichiers logs ils sont inutiles. De plus, les équipementiers ont des formats de logs différents, comme on peut le voir sur la figure ci-dessous, ce qui complique d'avantage le travail de corrélation.

Cisco	<190><session_number>: <value_hostname>: <value_date>: %SEC-6-IPACCESSLOGNP: list <value_ACL_id> permitted <value_ACL_number> <source_ip_address> -> <destination_ip_address>, <value_number_of_packets> packet
Fortinet	SN=<session_number> duration=<value_seconds> user=<username> group=<groupname> rule=<value_webtrend> policyid=<value_policyid> proto=<protocol> service=<network_service> status=accept src=<source_ip_address> srcname={<ip_address> | <domain_name>} dst=<ip_address> dstname={<ip_address> | <domain_name>} src_int=<interface_name> dst_int=<interface_name> sent=<value_bytes> rcvd=<value_bytes> sent_pkt=<value_packets> rcvd_pkt=<value_packets> src_port=<port_num> dst_port=<port_num> vpn={<vpn_name> | n/a} tran_ip=<ip_address> tran_port=<port_num> dir_disp={org | replay} tran_disp={noop |snat | dnat}

Figure14. Format de log pare-feu chez Cisco et Fortinet

La corrélation demande donc une solution de contrôle fondée sur l'analyse des traces des sondes d'intrusion, des routeurs, des commutateurs, des pare-feu et même des ordinateurs du réseau. Les traces doivent être envoyées à un collecteur local, pour des raisons de bande passante, lequel est chargé de transformé l'information dans un format standard et surtout de fournir un premier niveau d'agrégation. Pour tout événement significatif, définit comme tel dans la configuration du collecteur, l'alerte doit être réacheminée vers le collecteur centrale. Il peut y avoir plusieurs niveaux de collecteurs en fonction de la taille de l'entreprise. Au niveau du collecteur central, différents processus automatisés effectuent des analyses standards et les comportement types, comme des paquets mal formés, peuvent être rapportés sans que cela nécessite de développer un code spécifique. Le collecteur centrale valide ou non les alertes remontées par les collecteurs locaux. Cette architecture est représentée figure 15.

Imaginons un scénario d'attaque, représenté sur la figure 15. Le chemin 1, par lequel le paquet mal formé va d'un point A vers un point B, traverse différents équipements qui notent son passage et renvoient cette information à leur collecteur. Les collecteurs locaux renvoient l'information au collecteur central qui est en mesure, avant de valider l'alerte, de s'assurer que le paquet est bien partie du A au point B en empruntant le chemin 1. En effet, si les équipements du chemin 1 ne

notent rien, le collecteur central peut estimer que l'adresse IP source du paquet est en réalité usurpée et peut même déterminer quel est le véritable point de départ du paquet (A' sur la figure) et le chemin (2 sur la figure) si un autre équipement a noté le passage du paquet. Une fois que le collecteur central a validé toutes les hypothèses associées à cette série d'événement, il peut générer une alerte selon la politique de sécurité définie.

L'avantage d'une solution centralisée de collecte des alertes est qu'une corrélation supplémentaire est faite, fournissant une vision plus globale de l'incident potentiel. Sans cette centralisation, les sondes généreraient une forte quantité de faux positifs, contraignant pour l'équipe sécurité. Cependant, lorsque l'on combine des sondes de détection, chargées de détecter une signature, avec des sondes de prévention, fonctionnant sur l'analyse comportementale, on constate qu'il est possible de déterminer le nombre de faux positifs. De la sorte si on reprend l'exemple du ver *Windows*, une augmentation des flux 139/TCP ne signifie pas nécessairement une menace sauf si les paquets véhiculent le ver *Nachi*.

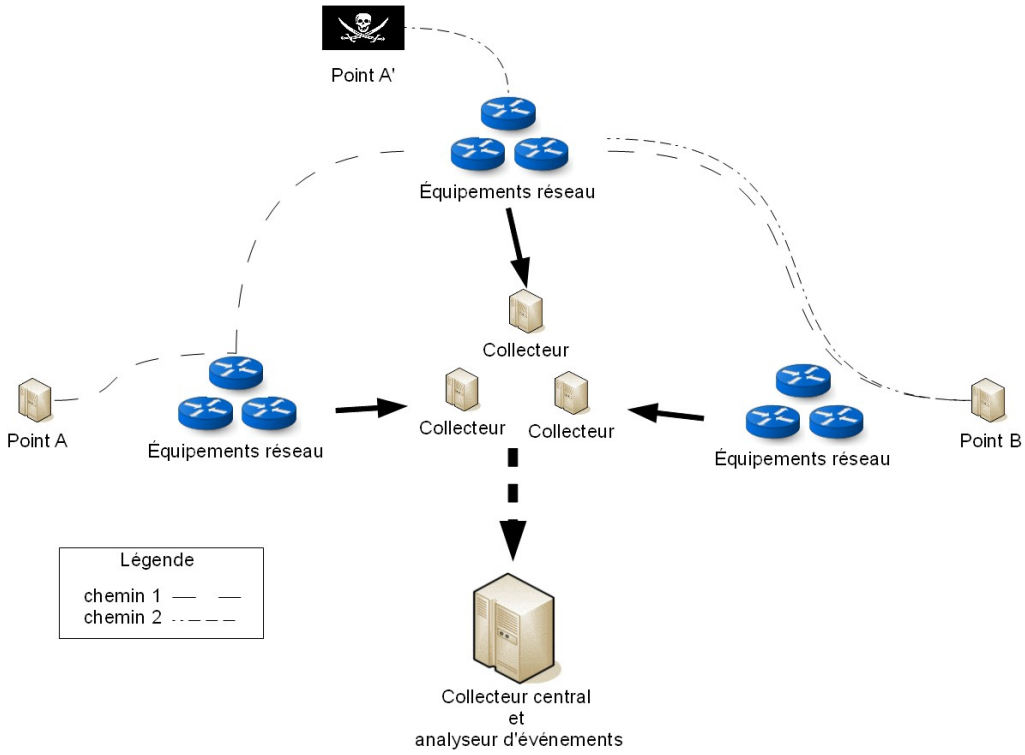

Figure15. Scénario d'attaque par usurpation d'identité et paquet mal formé

Dans les analyses internes rentrent encore l'analyse de la configuration des systèmes réseaux, du système d'exploitation ou encore des fichiers de configuration des services réseaux. Finalement, peut importe le nombre d'analyses faites, si ces événements sont pris de manière indépendants, ils risqueront d'être faux positifs. En effet, l'important est de corréler ces événements entre eux pour s'assurer de la véracité de l'alerte et surtout avoir une vision globale du réseau. Cette vision globale très importante est affichée grâce au tableau de bord, moniteur de l'état du réseau.

4.2. Les tableaux de bord

Comme nous avons pu le voir, les contrôles externes et internes de sécurité apportent un grand nombre d'informations qui doivent être analysées afin de tenter de détecter des failles de sécurité et de dresser un tableau de bord de la sécurité réseau. Pour analyser ces informations et établir des corrélations entre les différents événements, il est nécessaire de centraliser ces informations mais aussi de disposer d'outils efficaces d'aide à la décision. Bien que les événement réseaux soient cruciaux dans la détection de failles de sécurité, il convient de rester prudent dans leurs analyse ainsi que dans les conclusions déduites. La problématique majeure de l'analyse des événements de sécurité est que les informations ou événements disponibles sur un système donné couvrent des domaines très larges et il faut sélectionner ceux qui doivent être émis vers une plate-forme centrale d'analyse et de corrélation. Cette sélection est d'autant plus importante que le trafic des événements tend à croître de manière considérable dès que le nombre d'équipements supervisés augmente. Il faut prévoir les trafics de pointe associés à la remonté des événements et envisager une plate-forme centrale capable d'absorber et de traiter la quantité d'événements reçus.

a) Objectifs d'un tableau de bord de la sécurité réseau

L'établissement d'un tableau de bord de la sécurité réseau se réfère de manière fondamentale à la notion de mesure. De manière théorique, une mesure est définie comme le processus par lequel on affecte des nombres ou des symboles aux attributs d'entités appartenant au monde réel, de manière à les décrire par rapport à des règles clairement définies. Les mesures directes permettent d'attribuer une valeur à l'attribut d'une entité comme par exemple la taille d'un programme sera déterminé en fonction du nombre de ligne ou de lexèmes. En revanche, les mesures indirectes ne permettent pas d'attribuer une valeur à l'attribut d'une entité comme, par exemple, la facilité de maintenance ne peut se mesurer directement (par opposition au coût). La théorie de la mesure montre bien toute la difficulté de définir de manière cohérente et consistante un tableau de bord de la sécurité et on ne peut réduire un tableau de bord à un indicateur entre 0 et 100%, pour un système complexe, sans perte d'informations vitales.

Malgré ces difficultés il est essentiel d'initier la démarche d'établissement du tableau de bord pour répondre aux besoins de sécurité réseau de l'entreprise. Ce tableau doit comporter les éléments les plus critiques, définis lors de l'état des lieu de la phase de planification, ainsi que les menaces qui pèsent sur eux, définies lors de la phase de déploiement. Il doit définir la politique de sécurité permettant de se prémunir contre les menaces et les conséquences les plus critiques, également abordées dans la phase de déploiement avec le plan de contingence. Il doit mettre en œuvre les technologies répondant aux objectifs de sécurité définit dans la phase de planification. Il doit permettre de contrôle l'application de la politique de sécurité par le biais des contrôles internes et externes récurrents qui peuvent être automatiques ou non. Enfin, il doit consolider et corréler les informations des contrôle afin de bâtir un tableau de bord de bord en cohérence avec les objectifs de sécurité.

Pour atteindre les objectifs précédemment cités, le tableau de bord doit refléter régulièrement le niveau de sécurité d'un système et l'historique doit être conservé pour des analyses statistiques ultérieures. Il doit permettre de déclencher des actions ou alertes préventives qui prennent en considération l'historique des données collectées. Il doit être multidimensionnel, dans le sens ou il doit permettre de prendre des décisions en fonction de critères de natures différentes. Il doit constituer des rapports préventifs afin d'éviter, à priori, des incidents de sécurité et non des rapports post-mortem d'incidents de sécurité.

b) Mise en place

La première chose à faire dans la mise en place du tableau de bord est de définir une échelle de mesure. Il réside toujours une ambiguïté entre le terme « métrique » et « mesure » qu'il convient de lever. Le *NIST(« **N**ational **I**nstitute for **S**tandard and **T**echnology »)* précise que le terme « métrique » devrait être utilisé dans la définition mathématique et algorithmique et que le terme « mesure » devrait désigner la valeur numérique obtenue. Le jugement de l'adéquation d'une mesure est fondé sur le choix des attributs qui caractérisent une entité, mais aussi sur le faite que l'association de valeurs numériques aux attributs doit préserver certaines propriétés. De manière plus simple, toutes les relations définies du système empirique doivent être préservées dans le système numérique. Un énoncé est signifiant si sa vérité ou sa fausseté reste inchangée quand on passe d'une échelle à une autre échelle admissible. Il est important de toujours utiliser des opérations définies sur l'échelle choisie. Par exemple, si la criticité des vulnérabilités réseau est sur une échelle ordinale (basse, moyenne ou haute), il est impossible de calculer la moyenne des criticités observées.

La prochaine étape est certainement l'évaluation de la sécurité du réseau. Elle consiste à calculer les scenarii d'événements possibles par le biais d'un arbre probabiliste fondé sur les vulnérabilités préalablement détectées. En plus des vulnérabilités, deux autres facteurs sont nécessaires au moteur de calcul des scenarii pour construire un tel arbre. Le premier correspond aux règles de propagation des événements exploitants les vulnérabilités détectées et le second correspond à la topologie du réseau. La topologie est nécessaire pour valider l'existence d'un chemin réseau dans le déclenchement d'un événement conditionné par un autre événement. La figure ci-dessous illustre le calcul probabiliste.

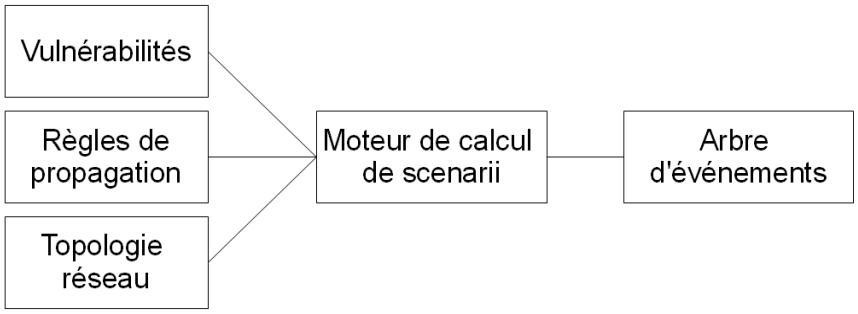

Figure16. Calcul d'un arbre probabiliste

Une fois les probabilités des impacts réseau calculées, la prochaine étape est la mesure du risque. Pour cela, il suffit de quantifier les conséquences associées à ces impacts réseau pour calculer le risque associé à la non-application de la politique de sécurité. Ce risque est calculé comme une espérance mathématique en multipliant les probabilités par les conséquences associées aux impacts réseau. La prochaine étape va être la pondération de ces impacts. Si l'on reprend les vulnérabilités précédemment citées, il est possible d'attribuer à chaque niveau de criticité un score qui va permettre d'utiliser une moyenne pondérée ($\bar{x} = \frac{\sum_{i=1}^{n} w_i x_i}{\sum_{i=1}^{n} w_i}$) pour faire un calcul statistique.

Ensuite, il faut encore considérer des valeurs du risque pour lesquels il est fort, moyen ou faible. Par exemple, un risque comprit entre 100 et 50 est fort, un risque compris entre 50 et 20 est moyen et un risque compris entre 20 et 0 est faible.

c) Les outil de SIM (*« Security Information Management »)*

Pour analyser et corréler les événements de manière efficace, de nouveaux outils sont apparus sur le marché sous le nom de SIM. Par opposition à l'approche précédente, ces outils aident à estimer le risque actuel, fondé sur des événements en temps réel. Ces outils permettent de centraliser les événements ou messages émis par les équipements de sécurité (pare-feu, système de détection d'intrusion, etc...) ou les systèmes et équipements réseau (routeur, serveur, etc...). Les messages reçus peuvent s'appuyer sur différents protocoles comme *syslog*, qui permet de véhiculer des messages systèmes.

Les corrélations entre les événements sont définies à l'aide de règles précises dont la forme générique est la suivante : si un événement peut être associé (*« match »*) à une suite de données de corrélation (*« pattern »*), une action est exécutée. Il ne faut pas s'imaginer que ces outils trouvent par eux même les règles et failles de sécurité. Ils se content de bien appliquer les paramétrages décidés par l'administrateur qui doit les faire évoluer avec les architectures et les services réseau, faute de quoi les règles risquent de devenir obsolètes et les corrélations de perdre leur sens. Les règles de corrélation doivent tenir compte des séquences possibles associées à des attaques ou arbre d'attaques.

L'intervention humaine est primordiale dans le processus de contrôle et d'analyse des incidents de sécurité . La figure ci-dessous illustre un *« workflow »,* assimilé à flux d'information au sein d'une organisation, détaillant les étapes à suivre pour la résolution d'un problème de sécurité, quel que soit l'outil mis en place.

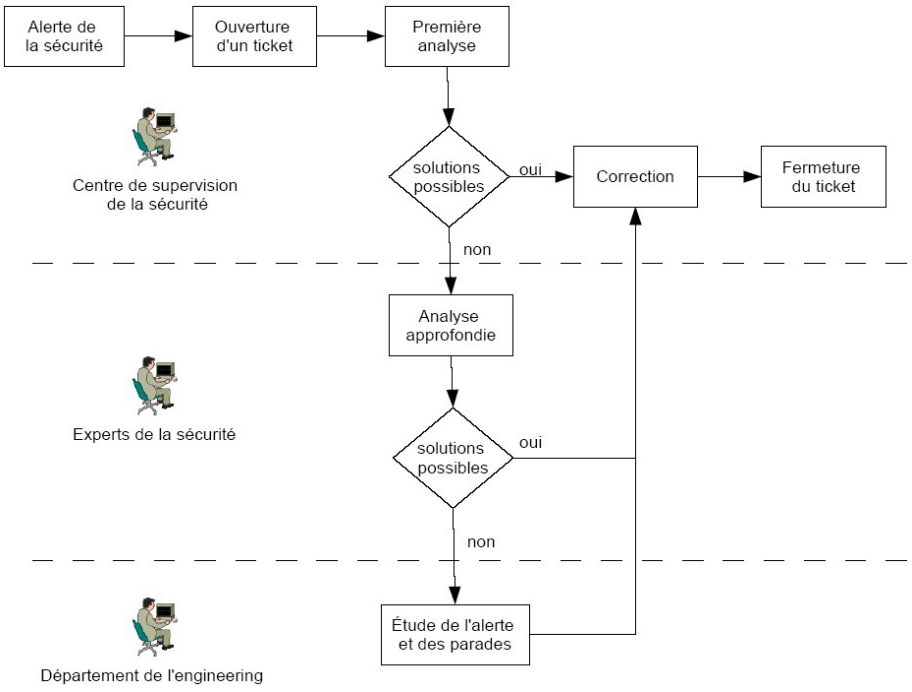

Figure17. « workflow » de gestion d'incident de sécurité

On remarque que ce *« workflow »* de gestion des incidents de sécurité fait intervenir trois acteurs. Le centre de sécurité a en charge la supervision et la résolution des alertes remontées. Les experts de la sécurité prennent la main si l'alerte s'avère plus complexe ou inconnue et analyse de manière approfondie les risques et solutions possibles. Enfin, le département de l'engineering prend le relais si l'alerte nécessite de mener des test complémentaires et poursuit la résolution du problème avec les experts de la sécurité en salle ou laboratoire de test afin de ne pas impacter le réseau.

Le contrôle de la sécurité réseau (interne et externe) fait partie intégrante de la démarche sécuritaire d'une entreprise et, comme détaillé dans ce chapitre, ce contrôle devient aussi complexe que les techniques mises en place contre les attaques. L'un des objectifs majeurs des contrôles de sécurité est de pouvoir établir des tableaux de bord reflétant l'application de la politique de sécurité réseau de l'entreprise. Il faut garder à l'esprit que les informations du tableau de bord sont additionnelles et ne représentent en aucun cas un niveau de sécurité réel. Maintenant que l'ensemble de la mise en place de la politique de sécurité réseau est faite, parcourons le marché pour voir ce qui va nous permettre, concrètement, d'implémenter la sécurité.

5. Implémentation concrète de la sécurité

Cette troisième partie est l'occasion d'appuyer sur l'aspect un peu plus technique de la sécurité des réseaux informatiques. En effet, nous avons abordé dans la partie précédente la mise en place de la politique de sécurité et on peut poursuivre en regardant les outils et technologies qui sont à notre disposition pour le faire. Ces différents outils sont abordés de manière chronologique ce qui permet de comprendre leurs évolutions et donc leurs apports au niveau de la sécurité. Nous continuerons cette analyse en abordant les produits considérés comme périphériques et qui permettent le management de la sécurité des réseaux. Enfin, nous terminerons sur le point de vue de différents équipementiers ce qui permettra d'analyser les tendances actuelles et l'implémentation qui en est réellement faite dans les entreprises.

5.1. Les outils et technologies

a) Le pare-feu

Le pare-feu est un composant réseau qui permet non seulement de concentrer l'administration de la sécurité en des points d'accès limités au réseau d'entreprise mais aussi de créer un périmètre de sécurité, par exemple entre l'intranet et Internet. Une architecture à base de pare-feu offre l'avantage de concentrer les efforts de sécurité en un unique point d'entrée. Grâce à des mécanismes de filtrage en profondeur ainsi qu'à des fonctions de journalisation des événements, les pare-feu fournissent des informations de premier choix quand des investigations de sécurité doivent être menées. Les principaux concepts du pare-feu sont le filtrage de paquets, le filtrage à mémoire, la passerelle de niveau circuit et la passerelle de niveau applicative.

- Filtrage de paquets

La première technologie de pare-feu réalise le filtrage au niveau des protocoles de la couche 3 du modèle OSI, sans mémoire des états des sessions. Aucune information n'est conservée de l'analyse de chaque paquet et aucune corrélation entre les paquets n'est faite. Le pare-feu agit comme une sonde placée sur le trafic réseau qui n'intervient pas sur les connexions TCP établit. Le filtrage est généralement effectué selon les critères suivants : adresse IP de l'émetteur et du destinataire, port source et destination et type de protocole (GRE, ICMP, IP, etc...).

La mise en œuvre de tels mécanismes de filtrage est relativement aisée, notamment au travers d'ACL comme sur les routeurs et les commutateurs de la marque *Cisco*. Cependant la puissance de traitement dépend directement du nombre d'entrées et de règles prises en compte par le filtrage et du niveau d'optimisation du filtre. Une ACL est généralement appliquée au trafic entrant (*« ingress »*) ou sortant (*« egress »*) et s'applique sur un équipement *Cisco* en respectant la syntaxe suivante :

access-list {numéro id} {deny | permit} {source} [masque inverse]

Une variante plus performante de l'ACL, appelé Turbo ACL, permet de limiter le temps perdu dans la lecture des règles de filtrage. Cependant, cette variante présente des inconvénients comme le faite de devoir compiler les ACL classiques avant de les copier sur l'équipement. Elles ne sont plus lisibles sur l'équipement et, de plus, elles nécessitent de la part de l'équipement un processeur particulier : l'ASIC *(« **A**pplication-**S**pecific **I**ntegrated **C**ircuit »*).

- Filtrage dynamique

Les applications utilisent des ports sources dont on ne peut connaître la valeur à l'avance (valeur prise aléatoirement entre 1024 et 65535). Le filtrage dynamique, ou *« stateful »*, de paquet permet de suivre les sessions et d'adapter de manière dynamique les règles du pare-feu.

Les performances de ce type de pare-feu sont bonnes, puisque le filtrage consiste en une simple inspection du trafic de données. Cependant, la configuration de tels équipements est complexe du fait du grand nombre d'options de filtrages disponibles. Ils sont généralement couplés à des solutions de translation d'adresse et de translation de port qui permettent de masquer le plan d'adressage internet du réseau d'entreprise.

Certains pare-feu bénéficient de technologie propriétaire comme ceux de la marque *Checkpoint* qui peuvent, grâce à leur technique de hachage du trafic, pointer directement sur la bonne règle de filtrage sans avoir à parcourir l'ensemble de l'ACL. Les routeurs de la marque Cisco avec leur technologie CBAC (*« Context-Based Access Control »*) peuvent, quant à eux, réaliser des filtrages sur l'état des connexions des couches 3 et 4 du modèle OSI pour déterminer d'éventuelles attaques.

- Passerelle de niveau circuit

Une passerelle de niveau circuit est un pare-feu qui agit comme intermédiaire, ou passerelle, au niveau du périmètre de sécurité du réseau. Chaque connexion qui traverse le périmètre de sécurité correspond à deux connexions réalisées par la passerelle, l'une entre l'utilisateur et la passerelle, l'autre entre la passerelle et le système visé par l'utilisateur.

Bien que cette technologie de translation d'adresse NAT (*« **N**etwork **A**ddress **T**ranslation »*) ait été initialement mise en place pour faire face à la pénurie d'adresse Ipv4, elle permet de « cacher » un grand nombre de systèmes derrière une seule adresse IP, améliorant ainsi la sécurité du réseau interne.

- Passerelle de niveau applicatif

Dans le filtrage de niveau applicatif, également appelé *proxy*, le pare-feu agit comme un filtre au niveau 7 du modèle OSI. Pour y parvenir, chaque application est implémentée sur le pare-feu par l'intermédiaire d'un agent agissant comme un relais applicatif. Chaque connexion qui traverse le périmètre de sécurité correspond donc à deux connexions par le proxy applicatif, comme expliqué pour la passerelle de niveau circuit.

Ce genre de pare-feu autorisent une authentification des utilisateurs beaucoup plus grande qu'avec les adresses IP. Ils cachent le réseau interne de l'entreprise et offrent des informations de journalisation d'événements très détaillées.

- Les produits du marché

Beaucoup de produit disponibles sur le marché cumulent les possibilités de filtrage, en offrant à la fois des fonctions de filtrage de paquets et de passerelle applicatives. Un pare-feu composite reste cependant plus performant dans le filtrage pour lequel il est initialement prévu. Par exemple, les pare-feu *Checkpoint* sont conçus au départ pour faire du filtrage *« statrful »* alors que les pare-feu *Gauntlet* de *Trusted Information Systems* ont été conçus pour faire du filtrage applicatif. Même si ces deux produits peuvent réaliser les deux filtrages applicatif et de paquet, ils restent avant tout des références dans leur domaine de prédilection. Le choix d'un pare-feu n'est pas simple si l'on n'a pas identifié avec soin les besoins de sécurité de l'entreprise.

Les critères pour choisir un pare-feu sont nombreux et en voici quelques-uns :

- les moyens d'administration (gestion, interface utilisateur, accès distant, rôles, etc...) ;
- les possibilités d'audit des règles de filtrage et des journaux d'activité (vérification de la consistance des règles, sauvegarde des journaux, etc...) ;
- le niveau de détail des règles de filtrage ;
- les réaction du pare-feu en cas de problème (blocage du trafic ou au contraire tout passe) ;
- la haute disponibilité ;
- la fréquences des correctifs de mise à jour ;

Le choix d'un pare-feu doit être dicté par des objectifs de sécurité précis et le tableau ci-dessous recense les principales fonctions offertes par quelque pare-feu du marché.

	Filtre hors contexte	Filtre contextuel	Proxy circuit	Proxy applicatif
Produit typique	ACL (*Cisco*)	pare-feu 1 (*CheckPoint*)	ASA (*Cisco*)	Gauntlet (*Trusted Information Systems*)
Modèle d'implémentation	Automate sans mémoire secondaire	Automate à mémoire	Automate à mémoire	Automate à mémoire
NAT / PAT	Non	Oui	Oui	Oui
Performant	Oui	Oui	Oui	Non
Universalité	Élémentaire	Moyenne	Moyenne	Forte
Puissance d'expression	Couches 3 et 4	Couches 3 et 4	Couches 3 et 4	Couches 7
Nombre de règles de filtrage	Faible, compte tenu des impacts possibles	Important	Important	Faible, compte tenu des impacts possibles

Figure18. Quelques solutions de pare-feu

b) Assurer la confidentialité des connexions

La confidentialité des informations transitant sur un réseau ne peut être assurée que par le chiffrement des données avant leur émission. Le réseau ne peut garantir par lui-même la confidentialité des données si elles ne sont pas chiffrées par un quelconque processus. Le chiffrement des données doit avoir un sens et se référer à une politique de classification des informations dans l'entreprise. Cette classification a pour objectif d'établir clairement des niveaux de confidentialité, comme défini lors de la phase de planification, et de définir les moyens pour les mettre en œuvre.

La confidentialité des connexions permet de prémunir d'un grand nombre d'attaques comme Les attaques à l'aide de programmes d'écoute, ou *« sniffer »*, qui permettent de reconstruire une transaction réseau de manière invisible pour les acteurs de la connexion. Pour garantir une isolation des fonctions de sécurité d'un réseau, il est préférable de dédier le chiffrement des données à un équipement spécifique plutôt que d'ajouter cette fonction à un routeur ou pare-feu.

Comme pour les pare-feu, le choix d'un protocole implémentant des fonctions de chiffrement doit tenir compte du type d'application qui sera utilisé ainsi que du besoin de sécurité désirée. Le tableau ci-dessous recense les principaux protocoles de chiffrement.

	IPsec	SSH	SSL
Administration système	Possible	Oui	Possible
Administration réseau	Oui	Oui	Possible
Accès distant au réseau de l'entreprise	Oui	Possible	Possible
Réseau privé virtuel	Oui	Possible	Possible
Connexion système	Oui	Oui	Oui
Connexion à une application	Possible	Oui	Oui
Facilité de mise en œuvre	+	+++	++++
Mise en œuvre d'un tunnel IP	Oui	Oui injection de paquet PPP dans SSH	Oui injection de paquet PPP dans SSL

Figure19. Solutions permettant d'assurer la confidentialité

c) Les AntiX

L'appellation *antiX* regroupe tous les logiciels dont le rôle est de filtrer les *« malwares »* ou d'éviter la baisse de productivité. On regroupe donc antivirus, anti-spam et filtrage d'URL.

- L'antivirus

Les antivirus sont conçus pour identifier, neutraliser et éliminer les logiciels malveillants comme les virus. Les principaux antivirus utilisent des fichiers de signatures pour comparer les objets à vérifier avec des signatures virales. Certains fonctionnent de manière heuristique, c'est à dire qu'ils recherchent des virus en fonction de leurs comportement, ou alors utilisent l'analyse de forme basée sur des expressions régulières (*regexp*). Les zones parcourues peuvent changer d'un antivirus à l'autre. Effectivement, si les plus anciens savent uniquement rechercher des virus sur ordre de l'utilisateur, la dernière génération d'antivirus sait faire des recherches dites « à l'accès » et d'autres peuvent même scanner la mémoire.

Si la majorité des antivirus sont applicatifs, dans le sens où ils sont livrés sous forme d'applications à installer sur un système d'exploitation, d'autres fonctionnent en tant que service embarqué. Cette dernière génération d'antivirus est particulièrement intéressante car elle effectue des scannes dits « à la volé ». Ils sont généralement embarqués sur des boîtiers UTM et ont l'avantage de scanner le trafic réseau qui passe à travers le boîtier. De la sorte ils ne protègent plus un seul ordinateur mais tous les ordinateurs qui sont sur le réseau. Cependant, il ne permettent pas de protéger des virus ou *« malware »* déjà présents sur le réseau par le biais de clé USB, disques durs ou encore CDROM et dégradent les performances du boîtier UTM. Pour faire un tour d'horizon des équipementiers, *Cisco* utilise une solution développée par *Trend Micro* dans son *ASA* (avec la carte CSC-SSM), *Fortinet* utilise une solution propriétaire qu'il réutilise dans son client VPN et *Juniper* utilise une solution développée par *Kaspersky.*

- L'anti-spam

Aujourd'hui plus de 75% du courrier représente des spams, c'est à dire de la publicité non sollicitée. Ce fléau, responsable d'une sérieuse baisse de la productivité dans les entreprises, représente une activité florissante où il est possible de gagner beaucoup d'argent en peu de temps. L'objectif de l'anti-spam va être de faire le tri dans la multitude de messages reçus pour trier les non désirés des légitimes. Il existe plusieurs filtrages pour rechercher des spams comme le filtrage d'enveloppe, de contenu, par mot clé ou adresses ou encore par expressions rationnelles. La méthode la plus efficace reste le filtrage heuristique qui filtre en fonction de comptage établi grâce aux mots présents dans le corps du message.

L'anti-spam peut être installé directement sur le serveur de mail ou utilisé sur un boîtier UTM. Il existe des solutions logiciels gratuites comme *SpamAssassin* ou des solutions payantes comme celle de *Microsoft* pour son serveur de mail *Exchange*. La solution embarquée sur les UTM est certainement la plus simple à déployer. Il suffit généralement d'activer le filtrage de contenu et de spécifier une règle de filtrage à destination du serveur de mail où l'on activera un profil de contenu utilisant l'anti-spam. Ces profil peuvent contenir des listes blanches, spécifiant les domaines autorisés, ou noires, spécifiant les spammeur.

- Le filtrage d'URL

L'objectif du filtrage d'URL est d'empêcher le surf sur des sites Web non autorisés. Cette limitation peut avoir différentes origines comme le contrôle parental, les restriction d'usage professionnel ou encore la protection des libertés individuelles. Il existe plusieurs techniques de filtrage comme le filtrage par mots clés, par listes blanches, listes noires ou encore par catégories.

Ce filtrage peut se faire par le biais d'un logiciel installé sur le poste client ou directement sur le boîtier UTM. L'avantage de le faire directement sur l'UTM est de concentrer toute la politique de filtrage en un seul endroit. Les modifications et mises à jour s'en retrouvent grandement simplifiées.

d) Les outils de management de la sécurité

Les outils de managements de la sécurité sont obligatoires pour les réseaux de grande étendues géographiques possédant de nombreux équipements réseau. Ils permettent de manière centralisée d'assurer, en plus de la remonté des événements comme les SIM, la gestion des équipements réseau, c'est à dire la modification de la configuration. Ces outils sont généralement composés d'une interface graphique permettant de visualiser le réseau et l'état des équipements qui s'y trouvent. C'est le cas de l'outil UBIqube, qui propose une interface de gestion unifiée et multi-vendeurs. Par le biais de la console de l'outil, l'utilisateur peut visualiser des informations d'ordre réseau, comme les adresses IP des équipements, mais également des informations dites *« d'asset »,* comme les dates d'expiration des licences des antiX ou encore la version du système installé.

Ces outils intègrent également des solutions de gestion d'incident, comme avec les SIM, et permettent de fonctionner dans un mode indirecte. Par exemple, prenons le cas d'une nouvelle filiale qui veut se connecter à sa holding. La première étapes, réalisées par l'équipe technique présente à la *holding*, consistent à *« stager »* l'équipement réseau qui sera ensuite envoyé à la filiale. Le *« staging »* représente la configuration minimale qui permet à l'équipement, une fois branché, d'être accessible depuis internet. Une fois l'équipement reçu et branché, par une personne pas nécessairement qualifiée en informatique, vient l'étape du *« provisionning »*. Lors de cette étape, l'outil de gestion du management de la sécurité, se connecte à l'équipement et le configure en fonction des profils de sécurité auxquels il appartient. Une fois *« provissionner »* l'équipement envoie ces logs à l'outil de management de la sécurité qui peut, de son côté, générer des rapports d'activités.

5.2. La position des équipementiers

Les équipementier sont des vendeurs de solutions réseau et peuvent être classés en fonction de leurs implantations sur le marché, leurs clientèles et leurs produits. Dans le multitude d'équipementiers qui existent, seuls quelques-uns ressortent dont *Cisco*, *Fortinet*, *Juniper*, *NetASQ*, *CheckPoint* ou encore *HP*.

En France, la marché est principalement occupé par *Cisco* et *NetASQ*. *Cisco* bénéficie d'une grande renommé ainsi que d'une implémentation dans le milieu scolaire de la sécurité qui en fait un produit apprécié des nouveaux administrateurs réseau. Effectivement, beaucoup de formations comme R&T (**R**éseau & **T**élécommunication) anciennement GTR (**G**énie des **T**élécommunication et des **R**éseaux) ou encore la licence professionnelle RSFS (**R**éseau **S**ans **F**il et **S**écurité) proposent des cours utilisant du matériel Cisco, voire des formations gratuites pour passer les certifications CCNA (*« **C**isco **C**ertified **N**etwork **A**ssociate »*). *NetASQ*, n'est pas en reste et se partage cette implantation dans le secteur de l'éducation nationale avec *Cisco*. Effectivement, le constructeur français, plus attractif au niveau économique, a fourni beaucoup d'écoles primaires et de mairies. Cependant, le constructeur Américain ne possède pas que le secteur public, il est également bien implanté dans le secteur privé, comme *Fortinet*, *Juniper* et *CheckPoint*.

Dans le domaine bancaire, *Cisco* remporte de larges parts de marché du à sa grande renommée. Cependant, si cette affirmation est vraie au État-Unis, on ne peut pas en dire autant dans les pays de l'Europe de l'est et au Maghreb. Dans ces régions *Fortinet* et *Juniper* sont beaucoup mieux implantés. Si l'Europe de l'est est partagée entre les deux constructeurs *Fortinet* et *Juniper*, les pays du Maghreb sont largement conquis par *Fortinet*. La principale raison que l'on peut trouver, vient du faite que la politique de prix pratiquée par *Fortinet* est plus abordable que celle de *Juniper* et *Cisco*. Cela s'explique principalement par le faite que Fortinet utilise des solutions « maison » pour ces applications embarquées comme l'antivirus, alors que *Juniper* et *Cisco* utilise des solutions propriétaires.

Pour finir, les équipementier se différencient de par les types de produits vendus. *Cisco* ne possède pas d'UTM à proprement parlé et ce n'est que récemment que le constructeur Américain se lance dans le marché de l'embarqué en proposant l'*ASA*. *Cisco*, reconnu pour ces routeurs, a toujours fonctionné par le rachat d'entreprise, en commençant par *PIX* pour ces solutions pare-feu, et maintenant avec *ASA* pour ces solutions UTM. Ce produit, à l'origine un pare-feu, accepte une carte embarquée SSM qui peut délivrer soit un service antivirus, soit un service de détection d'intrusion. Cela apparaît comme pauvre à côté de *Juniper* et *Fortinet* qui proposent depuis déjà longtemps des gammes complètes d'UTM. Que ce soit *Fortinet*, avec ses *Fortigate*, ou *Juniper*, avec ces *NetScreen*, le marché de l'UTM est incontestablement dominé par ces deux constructeurs. *CheckPoint* suit le même chemin que *Cisco* en se spécialisant dans les solutions de pare-feu et de VPN. Il faut dire que l'interface proposée pour le pilotage des pare-feu est unique et permet un niveau de granularité important.

Conclusion

Ce mémoire nous a permis d'aborder le thème de la politique de sécurité des réseaux informatiques. Dans une première partie, nous avons abordé la notion de réseaux informatiques. Cette partie a permis de mieux cerner les réseaux informatiques en les discriminant, notamment géographiquement, en les opposant aux systèmes répartis et en les abordant à travers le modèle OSI. Ces différentes approches mettent en avant l'aspect multidimensionnel des réseaux informatiques et laisse entrevoir le faite qu'assurer leurs sécurité n'est pas chose facile. La dernière section de ce chapitre rappelle l'approche processus et traite de la politique de sécurité réseau. Elle met en avant les spécificités et différences de la politique de sécurité réseau par rapport à la PSSI généraliste, abordée dans l'épreuve bibliographique tutorée.

Ce mémoire poursuit la mise en place de la politique de sécurité réseau à travers les quatre phases composants l'approche PDCA : **P**lanification, **D**éploiement, **C**ontrôle et **A**mélioration. La planification permet la répartition des ressources entre différentes personnes en suivant le « principe de propriété ». Ce principe permet de désigner un « propriétaire » qui se porte garant de la pérennité et de la protection de la ressource. Une fois ce découpage des ressources terminée, nous avons abordé le découpage de la politique de sécurité réseau en plusieurs niveaux. Ce découpage permet de ne retenir que les éléments essentiels pour le fonctionnement du système d'information et de répartir la politique de sécurité réseau en politique générale, en standard guide et recommandations et en procédures. Cette phase est poursuivie du déploiement qui permet de mettre en place le système documentaire ainsi qu'élaborer une stratégie de sécurité personnalisée. Le système documentaire, mis en place au travers d'un *« framework »* permet, un peu comme les normes ISO 9001 ou 27001, d'avoir une approche transversale qui permet d'identifier les différents processus qui gravitent autour de la sécurité des réseaux informatiques. Les stratégies de sécurité, qui permettent le déploiement de l'architecture réseau, sont nombreuses et doivent être combinées pour obtenir la stratégie de sécurité personnalisée qui convient à l'entreprise. Les phases de contrôle et d'amélioration qui suivent sont composées de la mise en place d'audits de sécurité ainsi que d'un tableau de bord de la sécurité réseau. Ces audits, qui peuvent être internes ou externes, permettent de vérifier l'application correcte de la politique de sécurité. Ils génèrent des informations qui permettent de caractériser le fonctionnement des réseaux informatiques et qui doivent être réutilisées dans l'élaboration du tableau de bord de la sécurité.

Enfin, ce mémoire se termine en abordant l'implémentation concrète de la sécurité des réseaux. Cette partie balaye les outils et les technologies disponibles pour assurer la sécurité des réseaux, comme les pares feu, les outils de management de la sécurité, ou encore les technologies AntiX comme les antivirus ou anti-spam. La dernière section aborde la position des équipementiers comme *Cisco*, *Fortinet* ou encore *Juniper* et met en évidence leurs répartitions géographiques, leurs différentes gammes de produits et leurs différentes implantations.

On retiendra de ce mémoire que la sécurité des réseaux est multidimensionnelle et que la politique de sécurité doit tenir compte de cet aspect. La mise en place d'un *« framework »*, de part son approche transversale des processus qui gravitent autour de la sécurité des réseaux, est une manière de prendre en compte cet aspect. Les stratégies de sécurité et les équipementiers fournissent les méthodes et le matériel nécessaire à la mise en place de la sécurité. Les audits ainsi que le tableau de bord permettent de s'assurer de la bonne application de la politique de sécurité. Cependant, cette politique de sécurité réseau a un coût que les décideurs commencent seulement à accepter, suite aux obligations induites par les diverses réglementations financières.

Bibliographie

[B1]

C. Llorens, L. Levier, D. Valois. Août 2006. *Tableaux de bord de la sécurité réseau* . Eyrolles

[B2]

A. Tanenbaum . 2003 . *Réseaux 4éme édition* . Pearson Education

[B3]

Direction Centrale de la Sécurité des Systèmes d'Information . Mars 2004 . *Guide pour l'élaboration d'une politique de sécurité de système d'information (PSSI), Section 2 Méthodologie* . [en ligne] : http://www.ssi.gouv.fr/fr/confiance/documents/methodes/pssi-section2-methodologie-2004-03-03.pdf

[W1]

Robert Jaques . Octobre 2007 . IT security spending steadily increasing . [en ligne] : http://www.vnunet.com/vnunet/news/2200795/security-spending-steadily . Visité le 17/06/2009

[W2]

Distribution Linux Whax . [en ligne] http://www.billyboylindien.com/tutos/whax-auditor-backtrack.html . Visité le 20/06/2009

Glossaire

- EBT : épreuve bibliographique tutorée
- PSSI : Politique de Sécurité du Système d'Information
- RSSI : Responsable de la Sécurité du Système d'Information
- SI : Système d'Information
- PDCA : Planification, Déploiement, contrôle et Amélioration
- LSF : Loi sur la Sécurité Financière
- OSI : Open System Interconnection
- ISO : International Organization for Standardization
- UTM : Unified Threat Managment

Titre : Les réseaux informatiques et la politique de sécurité

Résumé : Ce mémoire, adressée au RSSI ou DSI, aborde le domaine de la politique de sécurité des réseaux. Cette politique de sécurité est abordée à travers l'approche processus qui est décomposée en quatre phases : la planification, le déploiement, le contrôle et l'amélioration. Pour terminer, elle passe en revue les technologies disponibles pour implémenter la politique de sécurité des réseaux.

Mots clés : sécurité, système, information, politique, planification, déploiement, contrôle, amélioration.

Title : Networks and security policy

Abstract : This study, design for the ISSR or ISD, is about the network security policy. This policy is detailled from a process point of view which is composed of four parts : scheduling, deployment, control and improvement. To finish, this study shows the technologies available to implement the network security.

Keywords : security, system, information, policy, scheduling, deployment, control, improvement.