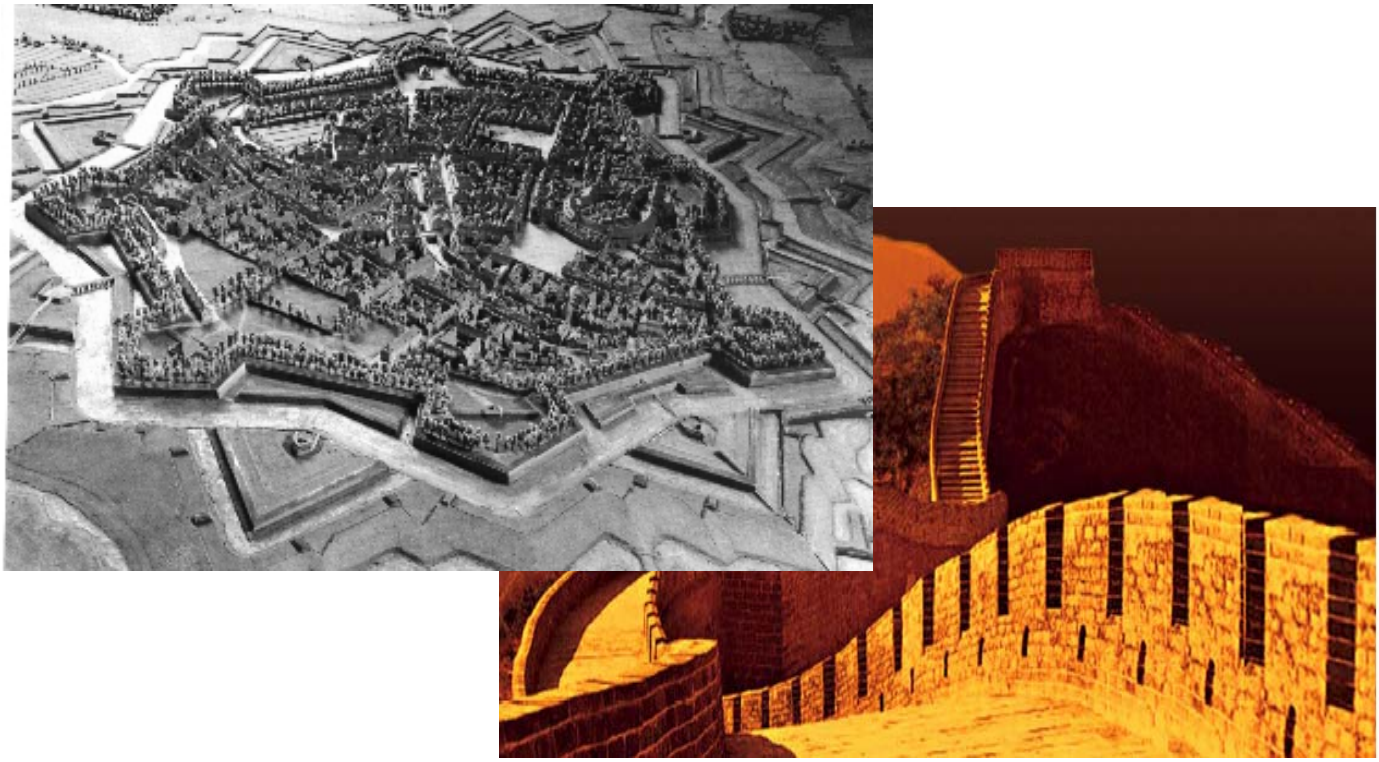
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

La défense en profondeur appliquée aux systèmes d'information

MÉMENTO



Version 1.1 – 19 juillet 2004

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01 71 75 84 15 - Fax 01 71 75 84 00

Ce document a été réalisé par le bureau conseil de la DCSSI
(SGDN / DCSSI / SDO / BCS)

Les commentaires et suggestions sont encouragés et peuvent être adressés à l'adresse suivante
(voir formulaire de recueil de commentaires en fin de guide) :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau Conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP

conseil.dcssi@sgdn.pm.gouv.fr

Sommaire

Tables des figures

Tables des tableaux

Introduction

1.1 Présentation de l'étude

En matière de sécurité, dans le domaine des systèmes d'information comme ailleurs, le plus dangereux est bien souvent de se reposer, consciemment ou non, sur une fausse assurance. Une démarche saine serait de gérer l'incertitude, de maintenir une inquiétude raisonnée et d'entretenir une véritable vigilance. Dans ce cadre, le bureau conseil de la DCSSI a mené une étude consacrée à la définition et la formalisation du concept de défense en profondeur appliquée au domaine de la sécurité des systèmes d'information. L'objet de l'étude est de permettre de dégager des conclusions pratiques et opérationnelles en matière d'architecture de SI et de gestion des risques. Pour atteindre ces objectifs, un grand nombre d'experts et d'acteurs français industriels ont été consultés.

1.2 Plan du document

Ce document comprend trois parties principales qui sont le reflet de la démarche :

- la première partie dresse un point de situation bibliographique exhaustif sur les pratiques des mondes industriel et militaire afin de tenter de déterminer les grands principes de la défense en profondeur ;
- la seconde pose les concepts et les définitions de la défense en profondeur appliquée à la SSI ;
- la troisième expose la méthode issue des principes définis précédemment et applicable à la sécurité des systèmes d'information ;
- une annexe illustre la méthode à partir d'un cas concret ayant permis de mettre en évidence les modalités d'évaluation.

Une conclusion reprend les réflexions effectuées dans le cadre de cette étude pour en dégager les apports et orienter les travaux ultérieurs.

1.3 Bibliographie

Le tableau ci-dessous indique les documents les plus importants traités dans le cadre de cette étude. Lorsqu'une référence est citée dans ce document, le numéro correspondant est mis entre crochets (la numérotation de l'ensemble de la documentation de l'étude a été conservée).

Ref	*Auteur(s)*	*Date*	*Titre*	
[SALI]	R. MACKEY	Juin 2002	Security Architecture, Layered Insecurity	http://www.infosecuritymag.com/2002/jun/insec
[RATP]	J. VALANCOGNE	28 février 2002	La défense en profondeur (de la RATP)	http://www.institutbull.com.fr/sujets/valancogne
[SBGN]	Bob Clark	11 juin 2002	Small Business Guide to Network Security	http://www.giac.org/practical/Bob_Clark_GSEC
[DRQR]	Tim Bass Silk Road, LLC Vienna, VA		Defense-in-depth revisited: qualitive risk analysis methodology for complex network-centric operations	http://www.silkroad.com/papers/pdf/milcom200
[IATF]	IATF Release 3.1	.Septembre 2002	Chapter 2 Defense in Depth	http://www.iatf.net
[DNCW]	CAPT Dan Galik, USN		Defense in Depth: Security for Network-Centric Warfare	http://www.chips.navy.mil/archives/98_apr/Gali
[DRA7]	D. HOURTOLOU	Septembre 2002	Analyse des risques et prévention des accidents majeurs (DRA-007)	http://www.ineris.fr/recherches/download/assura
[DEQS]	Yves Deswarte, Mohamed Kaâniche, Rodolphe Ortalo		Évaluation quantitative de sécurité	http://www.inria.fr/rapportsactivite/RA95/saturn

Tableau 1 : index bibliographique simplifié

1.4 Sigles et abréviations

Les sigles et abréviations utilisés dans ce document sont indiqués dans le tableau suivant.

Terme	*Signification*
AIEA	Agence Internationale de l'Energie Atomique
CDES	Commandement de la Doctrine et de l'Enseignement militaire Supérieur
DoD	Department of Defense (Département de la Défense des Etats-Unis)
IATF	Information Assurance Technical Framework
IDS	Intrusion Detection System (système de détection d'intrusion)
IIS	Internet Information Services (serveur internet Microsoft)
INERIS	Institut National de l'Environnement Industriel et des Risques
INSAG	International Nuclear Safety Advisor Group
IPSN	Institut de Protection et de Sûreté Nucléaire
SI	Système d'Information
SFEN	Société Française d'Energie Nucléaire
SSI	Sécurité des Systèmes d'Information

Tableau 2 : sigles et abréviations

2 Analyse du concept

2.1 Concepts au travers de la bibliographie

2.1.1 Étude du domaine militaire

Le concept de défense en profondeur semble prendre ses lettres de noblesse avec Vauban. L'apparition de boulets métalliques au XV^{ème} siècle capable de détruire les fortifications verticales entraîne la construction de fortifications beaucoup plus basses qui utilisent la profondeur du terrain. Les concepts sous-jacents sont les suivants :

- les biens à protéger sont **entourés** de plusieurs lignes de défense ;
- chaque ligne de défense participe à la **défense globale** ;
- chaque ligne de défense à un **rôle** à jouer : affaiblir l'attaque, la gêner, la retarder (échange de terrain contre du temps par exemple) ;
- chaque ligne de défense est **autonome** (la perte de la ligne précédente est prévue pour éviter un effet château de cartes) : la perte d'une ligne de défense affaiblit la suivante mais celle-ci dispose de ses propres moyens de défense face aux différentes attaques (chaque processus d'attaque possible entraîne une défense correspondante) ;
- Tous les moyens sont mis en œuvre pour renforcer la défense des différentes lignes :
  - utilisation du terrain (la fortification est un aménagement du terrain) ;
  - cloisonnement pour limiter les effets d'une percée et les tirs par ricochet ;
  - renseignement pour éviter la surprise.

Actuellement, le concept de défense en profondeur n'est plus à l'ordre du jour, la défensive n'étant que la résultante d'une position d'infériorité qui sera utilisée dans le but de reprendre l'initiative. Deux principes ont donc pris une très grande importance :

- le renseignement, qui permet de valider ou infirmer les hypothèses faites sur les actions ennemies, détecter son intention, etc. ;
- le mouvement (aspect dynamique de la défense).

Les grands principes de la défense en profondeurs sont les suivants :

- le **renseignement** est la première ligne de défense : depuis l'information sur les menaces effectives, la détection d'agissements souvent précurseurs d'attaques, jusqu'à toute détection non seulement d'attaques avérées et identifiées, mais encore de tout comportement « anormal » et donc suspect ;
- Il faut plusieurs lignes de défenses **coordonnées et ordonnées** par capacité de défense ;
- la perte d'une ligne de défense doit **affaiblir l'attaque** (au moins indirectement en recueillant un maximum d'information sur son ou ses origines, sa nature, sur les prochaines étapes possibles ou probables), ne pas entraîner la perte des autres lignes de défense mais au contraire permettre de les **renforcer** ;
- une ligne de défense doit comporter les parades (mêmes si cela se limite à détection d'anomalies et traçage dans le cas d'attaques de type non identifiable) à toutes les attaques possibles (**complétude** d'une ligne en elle-même) ;
- la défense n'exclue pas des actions offensives.

2.1.2 Étude du domaine industriel

2.1.2.1 Nucléaire

Le concept de la défense en profondeur appliqué dans le cadre de la sûreté nucléaire, est issu des travaux consécutifs à l'accident de « Three Miles Island » du jeudi 29 mars 1979 où le cœur du réacteur, insuffisamment refroidi, fond partiellement. Elle est définie comme une défense comprenant trois barrières successives indépendantes qui ramènent à un niveau extrêmement faible la probabilité qu'un accident puisse avoir des répercussions à l'extérieur de la centrale. L'idée est que chaque dispositif de sécurité doit a priori être considéré comme vulnérable et doit donc être protégé par un autre dispositif[1].
L'EDF identifie également trois lignes de défense de natures différentes :

- La pertinence de la conception (en particulier la mise en œuvre de la redondance et de la diversification) ;
- La détection des défauts latents et des incidents ;
- La limitation des conséquences ("mitigation").

La défense en profondeur est associée à une gestion de risques dont les 8 niveaux normalisés sont présentés ci-dessous.

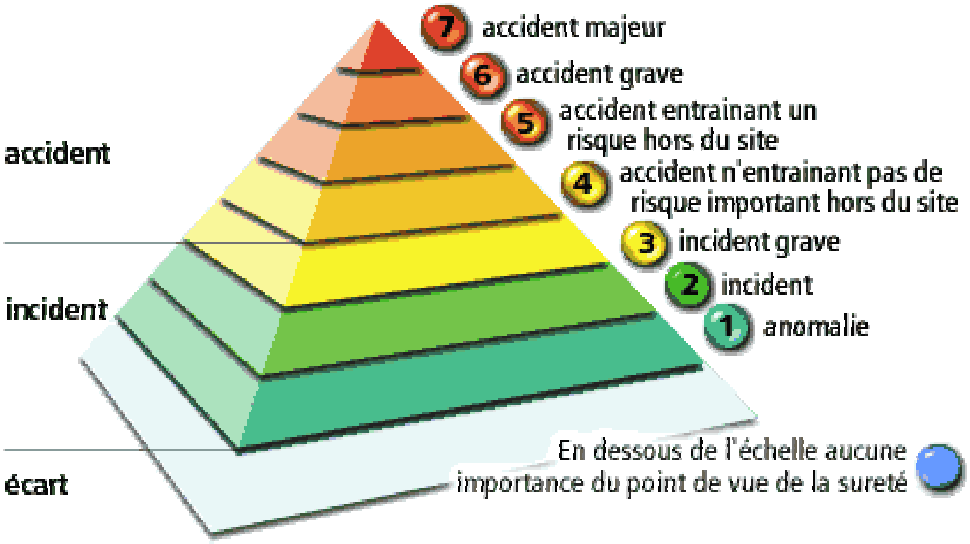


Figure 1 : échelle INES[2]

[1] « La sûreté des centrales nucléaires est, en particulier en France, fondée sur la philosophie de la "défense en profondeur" qui s'organise autour de niveaux multiples de protection comprenant des barrières successives qui ramènent à un niveau extrêmement faible la probabilité qu'un accident puisse avoir des répercussions à l'extérieur de la centrale. L'idée est que chaque dispositif de sécurité doit *a priori* être considéré comme vulnérable et doit donc être protégé par un autre dispositif. » Clefs CEA n° 45 Encadré D Les trois barrières, illustration du concept de "défense en profondeur" (Mise à jour Mars 2002).
[2] Source : http://nucleaire.queret.net

Les trois barrières (la gaine du combustible, la cuve en acier du réacteur épaisse de 20 centimètres, l'enceinte de confinement (épaisse de 90 centimètres) qui entoure le réacteur[3] sont montrées dans le schéma ci-après.

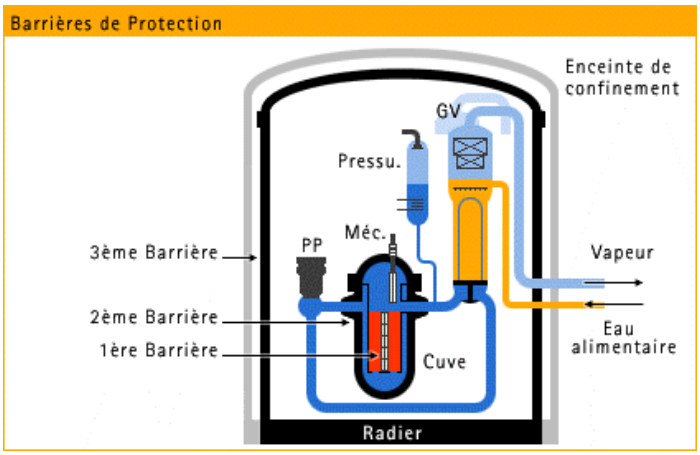


Figure 2 : les trois barrières[4]

[3] Cette enceinte étant elle-même doublée dans les réacteurs modernes.
[4] Source : http://perso.club-internet.fr/sorinj/la_surete.htm

2.1.2.2 RATP

Les principes de défense en profondeur mis en œuvre dans le nucléaire se retrouve dans beaucoup de complexes industriels présentant des risques majeurs. Tout comme le nucléaire, le risque vient le plus souvent de l'intérieur et les différentes barrières ont pour objectif le confinement. Dans [4], J. Valancogne introduit une caractérisation des barrières :

- les barrières peuvent être soit technologiques, soit procédurales soit humaines. Elles peuvent être également mixtes, c'est-à-dire combiner ces différents attributs ;
- les barrières sont soit statiques soit dynamiques (une enceinte de confinement est une barrière statique alors qu'un automatisme chargé d'ouvrir une vanne est une barrière dynamique) ; Les barrières dynamiques (s'ouvrent et se ferment) peuvent être :
  - technologiques, humaines ou mixtes,
  - inhiber l'agression au moment où elle se manifeste (elle se ferme) ou au contraire s'ouvrir au flux si celui-ci n'est pas agressif (elle s'ouvre),
  - agir sur des échelles de temps différentes,
  - être en réussite ou en échec,
  - utiliser différents principes de réalisation (intrinsèque, probabiliste) ;
- elles peuvent agir soit sur l'élément agresseur, soit sur le flux, soit sur l'élément à protéger.

L'efficacité des barrières ne dépend pas uniquement de leur conception ; les aspects maintenance et évolution dans le temps sont également très importants. On peut associer à chaque barrière un arbre de défaillance. L'exemple de la catastrophe de Bhôpal, montre l'échec successif des trois barrières prévues pour éviter l'accident, principalement du fait de défauts de procédure et de maintenance. J. Valancogne insiste également sur l'importance du retour d'expérience et en particulier sur l'analyse des incidents (on retrouve ces éléments dans le nucléaire). De plus, le système n'étant pas figé, l'efficacité des défenses doit être réévaluée périodiquement.

2.1.2.3 Chimie

Un ouvrage particulièrement intéressant intitulé "Analyse des risques et prévention des accidents majeurs" (DRA-007) [43] a été publié par l'INERIS (Institut national de l'Environnement Industriel et des Risques). Il s'agit du rapport final (septembre 2002) du projet ASSURANCE dont l'objectif était de réaliser une analyse comparée des méthodes d'analyse des risques et approches sécurité en Europe au travers de l'étude d'une installation chimique réelle prise en référence. La démarche globale comprend les phases suivantes :

- détermination des risques ;
- hiérarchisation des risques :
  - classes de gravité en fonction des effets (létaux, irréversibles) ;
  - fréquence/probabilité en fonction du nombre de barrières ;
  - matrice d'acceptabilité des risques (en fonction de gravité et fréquence) : zones autorisées, acceptables et critiques ;
- analyse qualitative, les méthodes utilisées se répartissent en trois catégories :
  - les méthodes d'analyse inductives (la majorité : HAZSCAN, SWIFT, HAZOP, APR) sont fondées sur une analyse descendante de la séquence accidentelle (des causes vers les conséquences) ;
  - les méthodes d'analyse déductives (arbre de défaillance) s'appuient sur une analyse ascendante de la séquence accidentelle (des conséquences vers les causes) ;

  - les méthodes fondées sur l'identification systématique des causes de rejets, construites sur la base du jugement d'expert et du retour d'expérience (guide national ou grille d'audit).
- analyse quantitative, les méthodes utilisées se répartissent en deux catégories faisant l'objet du schéma ci-dessous :
  - approche probabiliste ;
  - approche déterministe.

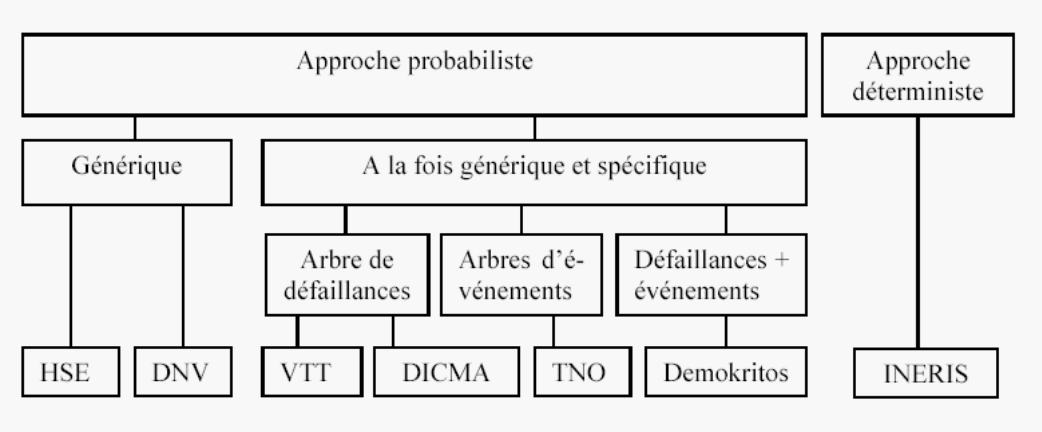


Figure 3 : les approches méthodologiques (source : [DRA7])

Suite à une analyse comparée entre les approches déterministe et probabiliste du risque, aucune des deux n'est parfaitement adaptée à la gestion du risque SSI. Une solution alternative proposée serait alors de s'appuyer sur le concept des barrières de défense et de la défense en profondeur, qui est le principe fondateur de la sécurité, dans les installations nucléaires ou industrielles en France. De l'avis de l'INERIS, l'approche par barrières de défense permet plus de transparence dans la présentation de la gestion des risques, et donc une communication mieux perçue par le public et les associations.

2.1.3 Étude du domaine SSI

On distingue trois types de documents:

- des documents dans lesquels il ne s'agit d'une simple référence au bon sens : la défense ne doit pas se limiter à la périphérie ou reposer sur un moyen unique ;
- des documents, principalement aux Etats-Unis à partir de 1998, traitant de la sécurité des systèmes d'information du ministère de la défense en particulier et qui utilisent ce terme ;
- des documents qui sont plus méthodologiques ont été détaillés dans le document de la phase 2 :
  - [13] se voulant être une méthode simplifiée pour organisme de petite taille ;
  - [31] se rapprochant plus d'une analyse de risques qualitative ;
  - [3], prônant la défense en profondeur par un contre-exemple ;
  - [7], d'origine NSA à l'origine des concepts mis en œuvre par le DoD.

2.1.4 Analyse des contextes

Dans un premier temps il est nécessaire de prendre en compte les différences de contexte entre les trois domaines étudiés. Les points suivants paraissent intéressants :

- le facteur surprise :
  - dans le domaine militaire, il est systématiquement recherché et fait partie de la manœuvre ;
  - dans le domaine nucléaire, il est, sans doute, le facteur que l'on cherche à réduire au maximum même s'il ne doit pas être écarté ;
  - dans le domaine de la sécurité informatique, il est présent par le fait qu'il existera toujours de nouvelles formes d'attaques (actuellement la défense n'a pas l'initiative) ;

- le renseignement : il va en particulier permettre de diminuer l'incertitude sur les actions ennemies en confirmant ou infirmant les hypothèses et éviter les méfaits de la surprise ; le renseignement ne doit pas être dissocié de la planification ;

- la coopération entre les différentes lignes de défense :
  - dans le domaine militaire, il est systématiquement recherché la synergie entre les différents moyens : l'ajout d'un moyen supplémentaire doit procurer un avantage plus important que la simple somme des lignes de défense qui ne sont pas indépendantes ;
  - dans le domaine nucléaire, on insiste sur l'aspect d'indépendance vis-à-vis des menaces (les causes de défaillances) des différentes lignes de protection ;
  - dans la sécurité informatique il semble que l'ajout des dispositifs de protection est fortement lié à la présence de menaces, celles-ci étant prises de manière unitaire ;

- l'origine des menaces (interne/externe) :
  - la notion de défense rapprochée illustre bien ce principe : l'ennemi peut se trouver dans toute la profondeur du dispositif et par conséquent, quelque soit son rôle, chaque combattant doit assurer sa propre protection rapprochée ;
  - dans le milieu industriel, les menaces externes (terrorisme par exemple) sont prises en compte ; de même que les menaces internes (le processus industriel lui-même) ;
  - pour la sécurité informatique on retrouve le côté global de l'attaque qui provient de l'intérieur et de l'extérieur ; la profondeur du dispositif de protection doit donc être définies dans plusieurs dimensions. Cela signifie que la profondeur de la défense devra prendre en compte l'organisation, la mise en œuvre et les technologies et ne pas se contenter d'une simple défense périmétrique vis à vis de l' « extérieur » du système.

- pour qu'il y ait défense en profondeur il faut au minimum :
  - plusieurs lignes de défenses indépendantes dans le sens où chacune est capable de se défendre seule contre toutes les attaques (c'est-à-dire que la perte de la ligne précédente est prévue, il n'y a pas de présupposition que la ligne précédente existe) ; en toute rigueur il conviendrait de parler de lignes de défense autonomes ou complètes c'est-à-dire aptes à répondre à toutes les menaces ; en effet, l'un des principes de la doctrine militaire veut qu'en plus, les lignes participent à la défense globale qui présente alors une force de défense supérieure à la somme défense de chaque ligne (ce point n'étant pas repris comme principe dans le milieu industriel qui s'attache plus à l'indépendance des barrières) ;

- coopération entre les lignes de défenses sinon le concept est ramené uniquement à de simples barrières successives dont la résistance ne dépend pas de la précédente (on peut alors les attaquer successivement) ;
- la perte d'une ligne doit permettre de renforcer la défense et non l'affaiblir (ce point étant un corollaire du précédent mais laissé ici pour apporter l'aspect dynamique de la défense).

L'origine du concept de défense en profondeur est militaire. Ce mot est utilisé par la suite dans le domaine nucléaire qui en fait une méthode. Le concept est repris ensuite dans le cadre plus général de l'industrie (chimie) et des transports (RATP). Dans le milieu industriel, la défense en profondeur permet de compléter l'analyse de risques probabiliste par un aspect déterministe et une modélisation au niveau des composants. Le concept est ensuite repris au niveau de la sécurité des systèmes d'information aux Etats-Unis principalement mais sans le développer réellement, car il semble regrouper différentes notions qui tournent autour du mot profondeur dans le sens de plusieurs moyens redondants ou complémentaires. Toutefois deux approches semblent exister, la première insistant sur l'aspect global de la défense et l'autre plus orientée composants. C'est dans cette dernière approche que la référence à l'analyse de risque est plus explicite.

2.2 Apports des entretiens

De l'entretien mené avec des personnels militaires il ressort l'importance :

- du facteur renseignement, qui avait déjà été signalé, mais qu'il faut encore renforcer ;
- de l'aspect dynamique et de la planification ;
- des notions de responsabilité par niveaux.

Ces trois points doivent se traduire, dans le cadre de la défense en profondeur des systèmes d'information par la prise en compte des principes suivants :

- lors de la mise en place d'une "barrière", il faut prévoir en même temps :
  - le point de contrôle de son bon fonctionnement ou de sa chute (fonction renseignement) ;
  - les informations nécessaires à collecter pour savoir qu'un attaquant va la prendre pour cible ;
- lors de l'élaboration de la politique globale il faut prévoir la chute d'une barrière et donc :
  - prévoir des parades dynamiques ;
  - planifier les actions possibles en fonction des différents cas ;
- la sécurité du système d'information doit être la préoccupation de tous les personnels et non des seuls spécialistes ; des responsables doivent être nommés, à chaque niveau :
  - au niveau individuel (la sûreté immédiate) : charte, un manuel de procédure, etc. ;
  - au niveau de chaque cellule de l'organisation (la sûreté rapprochée) : dossier de sécurité adapté avec des procédures et un ou plusieurs plans de secours de niveau élémentaire ;
  - au niveau de l'organisme (la sûreté éloignée), les plans de secours vont avoir une portée plus générique de type multiservices, sites de secours, etc.

Le concept de la défense en profondeur doit être vu, dans le milieu industriel, comme un aboutissement logique de la maîtrise des risques :

- une fois l'objectif de sécurité défini (éviter une dissipation en dehors du site, un accident, etc.), une analyse du risque est menée selon des méthodes connues, la défense en profondeur combine donc à la fois l'approche déterministe et probabiliste ; ces deux approches complémentaires permettent de prévoir et mettre en place les barrières (approche déterministe au moment de la conception) puis d'évaluer la probabilité de défaillance des barrières (approche probabiliste) ;
- ensuite, on peut graduer les différents incidents dans une échelle globale qui a des avantages pédagogiques et médiatiques importants :
  - échelle de valeurs communes,
  - permet de présenter la défense selon un schéma compréhensible pour tous,
  - permet de déterminer facilement la gravité d'un incident qui est fonction de la barrière franchie ;
- enfin, chaque franchissement de barrière donne lieu à des mesures préventives et correctives et ce, en prévoyant jusqu'à la phase ultime lorsque le fait redouté arrive.

2.3 Conclusion de la première phase

Selon les critères définis pour la défense en profondeur, il n'a pas été trouvé de solution complète exposée dans le cadre de la sécurité des systèmes d'information. En contrepartie, les principes issus des domaines militaire et industriel apportent des idées intéressantes. En effet, le milieu militaire est proche de la sécurité informatique en ce qui concerne les aspects attaque/défense et le milieu industriel apporte le côté global, systématique et quantitatif et donc une rigueur mesurée qui manque dans le domaine informatique.
D'ors et déjà, il apparaît :

- que le terme de défense en profondeur, tel qu'il apparaît actuellement dans le cadre de la sécurité informatique ne représente pas une révolution par rapport aux principes appliqués actuellement ;
- que l'enrichissement des principes actuels de la sécurité informatique par des apports tirés de la méthode de défense en profondeur appliquée dans le milieu industriel et dans le domaine militaire devrait permettre de définir une réelle méthode de défense en profondeur dans laquelle il serait plus question de défense que de sécurité.

3 La défense en profondeur en SSI

3.1 Définition du concept

3.1.1 Appréciations générales du concept

Le principe le plus universel du concept de défense en profondeur et qui se retrouve dans les trois domaines, militaire, industriel et sécurité des systèmes d'information, est celui de plusieurs barrières indépendantes.

Les autres principes sont ensuite plus ou moins bien développés selon les cas. En outre, si dans le milieu industriel le concept est toujours le même, il faut reconnaître que dans la sécurité des systèmes d'informations, ce n'est pas le cas.

Il apparaît toutefois, que le concept de barrière est i) uniquement lié à la composante protectrice (contingentement, cloisonnement) et ignore donc d'autres dimensions essentielles ii) trop dépendant de la menace et donc délicat à manipuler au niveau de la sécurité des systèmes d'information lorsqu'on s'adresse à des décideurs ou des utilisateurs, principalement en raison de leur caractère technique et multiple.

En revanche, la notion de ligne de défense paraît être plus riche et plus parlante, même si cette notion est très arbitraire.

> Dans le cas, par exemple, d'un poste de travail protégé par un FireWall et un antivirus contre les accès non autorisés provenant de l'Internet, l'antivirus constitue la seconde barrière face à une tentative de déposer un code malicieux par intrusion mais devient la première si le vecteur utilisé est un courrier électronique, celui-ci étant autorisé par le FireWall. En effet, dans le cadre de la sécurité informatique, les moyens de protection (ici en l'occurrence le FireWall) sont plus un filtre que de véritables barrières (cf 3.1.2) comme dans le cas du nucléaire.

En effet, il n'est pas possible d'établir un lien direct entre barrière, ligne de défense et niveau de gravité en raison du caractère multiforme et multi-menaces de la défense. En contrepartie, la notion de ligne de défense permet de regrouper des barrières pour un aspect "communication" et de les corréler avec les niveaux de gravité[5]. Une ligne de défense correspond alors à une transition entre deux niveaux de gravité et implique une réaction planifiée correspondante.

La démarche proposée va donc conduire à déterminer les barrières[6] à mettre en place en fonction des menaces et des biens à protéger, puis à déterminer le niveau de gravité des incidents de sécurité provoqués par le franchissement des barrières afin de les regrouper par niveau de gravité et ainsi faire apparaître les lignes de défense. Celles-ci participent à l'effort de communication vers les décideurs et les utilisateurs mais ne remplacent pas l'étude des

[5] Les niveaux de gravité proposés sont indiqués plus avant dans le chapitre.

[6] Le terme de barrière (Cf. définition faite plus avant dans le chapitre) est pris ici comme synonyme de mesure de sécurité (humaine, procédurale, technologique) en reprenant la définition générique de ce terme proposée par M. Valancogne afin de conserver au terme ligne de défense un sens plus global et "communiquant". Nous écartons donc par-là même le sens donné à ces deux termes par le CEA.

barrières pour les spécialistes de la sécurité. Cette démarche est présentée sur la figure suivante.

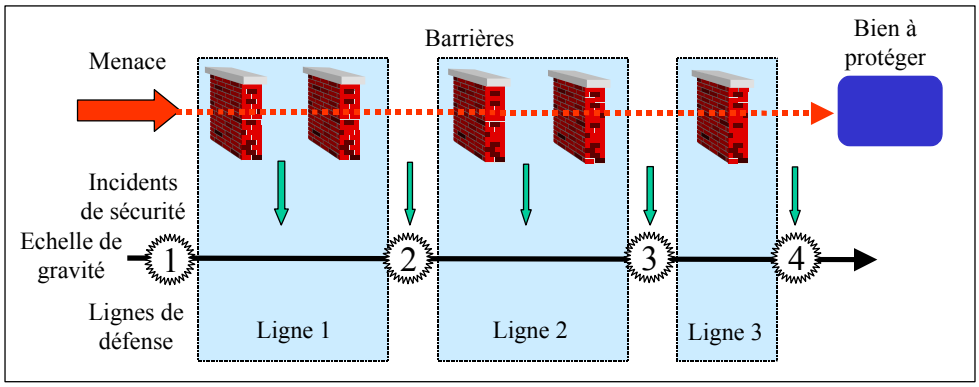


Figure 4 : démarche de mise en évidence des lignes de défense

La démarche doit combiner de manière itérative l'approche déductive (par les ressources) puis inductive (par les menaces). Elle arrête la conception lorsqu'il est possible de valider l'architecture et les moyens de protection et de déterminer les risques résiduels (qualification du système étudié).

Il est à noter que les barrières sont associées à des menaces (ce qui impose une approche inductive) mais que la gravité des incidents de sécurité dépend des ressources (ce qui impose une analyse de risque et une approche déductive). Les deux approches (inductive et déductive) se complètent donc l'une l'autre et sont à réitérer jusqu'à obtenir un niveau de protection suffisant. Il devient alors possible de valider l'architecture et les moyens de protection mis en œuvre en correspondance avec les risques et de faire apparaître les risques résiduels (qualification du système).

En outre, une barrière (et donc une ligne de défense) peut couvrir plusieurs menaces et son franchissement provoque un incident dont la gravité dépend du nombre de lignes de défense restant à franchir et de la valeur des biens à protéger. Il existe donc une double représentation :

- l'une pour les décideurs et les utilisateurs, volontairement globale et simple (l'aspect ligne de défense et échelle de gravité présenté sur le schéma précédent) ;

  Cette représentation est importante pour l'aspect **communication** de la méthode.

- l'autre plus fine, s'appuyant sur des modélisations particulières des processus critiques par menaces principales et destinée aux spécialistes ; dans ce cas il sera sans doute intéressant de subdiviser les différents niveaux, subdivisions qui correspondraient alors à des variantes dans la planification (l'aspect scénario enchaînant barrières et incidents de gravité du schéma précédent).

  Cette représentation est importante pour l'aspect **qualification** de la méthode (représentation schématique des différentes mesures de sécurité associées à une menace et protégeant un bien, élaborée lors de la construction des scénarii et qui permet : i) de déterminer les barrières à mettre en œuvre à partir de l'analyse inductive et puis déductive itérative jusqu'à obtenir le niveau de protection nécessaire ii) d'apprécier la gravité d'un événement de sécurité en fonction de la criticité du bien et du nombre de lignes restantes.

La modélisation particulière effectuée pour les biens critiques et les menaces principales permet de faire le lien direct et par conséquent de détecter les "trous de sécurité" plus facilement et par conséquent d'autoriser une évaluation.

3.1.2 Définitions

L'analyse des différents principes et du concept de défense en profondeur permet de proposer les définitions suivantes :

*La **gravité** d'un événement de sécurité mesure l'impact réel de l'événement en fonction de la criticité du bien (cas où un événement a une conséquence directe sur un bien) ou l'impact potentiel de cet événement sur le bien menacé en fonction du nombre de lignes de défense restantes et de la criticité de ce bien (cas ou l'événement n'a pas d'impact sur le bien mais sur ses moyens de défense).*

*Une échelle fixant les **niveaux de gravité** est proposée par la méthode afin de pouvoir comparer entre eux différents incidents de sécurité. Pour un incident de sécurité donné, il appartient aux responsables utilisateurs de déterminer le niveau de gravité correspondant qui s'apprécie en fonction de l'impact de cet incident sur le bien à protéger.*
*Une **barrière** est un moyen de sécurité capable de protéger une partie du système d'information contre au moins une menace. Une barrière peut être humaine, procédurale ou technique, statique ou dynamique, manuelle ou automatique. Elle doit bénéficier d'un moyen de contrôle de son état.*

*Une **ligne de défense** est un ensemble de barrières, par scénario ou famille de scénarii, dont le franchissement provoque un incident dont la gravité dépend du nombre de barrières restantes à franchir par la ou les menaces pour atteindre le ou les biens protégés et de la valeur de ces biens (c'est-à-dire qu'à un incident de sécurité donné est associé un niveau de gravité qui indique la ligne de défense abstraite franchie). Toute ligne de défense pour être une ligne et pas seulement un ensemble de moyens de protection, doit être munie des dispositifs et moyens de détection/veille et de notification.*

*La **défense en profondeur** du système d'information est une défense globale et dynamique, coordonnant plusieurs lignes de défense couvrant toute la profondeur du système. terme profondeur doit être compris au sens le plus large, c'est à dire dans l'organisation du SI, dans sa mise en œuvre et enfin dans les technologies utilisées. Il s'agit alors de permettre des actions de neutralisation des atteintes contre la sécurité, à moindre coût, grâce à une gestion des risques, un système de renseignement, une planification des réactions et l'enrichissement permanent grâce au retour d'expérience. Cette défense en profondeur a un double but : i) renforcer la protection du système d'information par une approche qualitative permettant de vérifier la complétude et la qualité du dispositif, ii) donner un moyen de communication fort permettant aux décideurs et aux utilisateurs de prendre conscience de la gravité des incidents de sécurité.*

Dans la sécurité des systèmes d'information, une barrière, un moyen ou dispositif, est associé à au moins une menace particulière et placé à un endroit bien défini (entre l'origine de l'agression et le bien à protéger). Elle peut protéger plusieurs biens mais pas obligatoirement de la même manière. Par conséquent, l'analyse des lignes de défense doit être effectuée pour chaque bien (ou ensemble de biens) et pour chaque menace donc pour chaque type d'incident de sécurité.

Cette analyse est faite avec une granularité qui dépend de l'importance du risque considéré (fonction de la criticité du bien et/ou de la probabilité d'apparition de la menace), en combinant l'approche inductive (par les menaces) puis déductive (par les ressources à protéger).

3.1.3 Principes généraux

Le concept de défense en profondeur obéit donc aux grands principes généraux suivants. Chacun de ces principes peut être individuellement mais c'est l'ensemble qui donne la profondeur de la défense.

Titre	*Nature*
Globalité	**La défense doit être globale, ce qui signifie qu'elle englobe toutes les dimensions du système d'information :** a) aspects organisationnels ; b) aspects techniques ; c) aspects mise en œuvre.
Coordination	**La défense doit être coordonnée, ce qui signifie que les moyens mis en place agissent :** a) grâce à une capacité d'alerte et de diffusion ; b) à la suite d'une corrélation des incidents.
Dynamisme	**La défense doit être dynamique, ce qui signifie que le SI dispose d'une politique de sécurité identifiant :** a) une capacité de réaction ; b) une planification des actions ; c) une échelle de gravité.
Suffisance	**La défense doit être suffisante, ce qui signifie que chaque moyen de protection (organisationnel ou technique) doit bénéficier :** a) d'une protection propre ; b) d'un moyen de détection ; c) de procédures de réaction.
Complétude	**La défense doit être complète, ce qui signifie que :** a) les biens à protéger sont protégés en fonction de leur criticité ; b) que chaque est protégé par au minimum trois lignes de défense ; c) le retour d'expérience est formalisé.
Démonstration	**La défense doit être démontrée, ce qui signifie que :** a) la défense est qualifiée ; b) il existe une stratégie d'homologation ; c) l'homologation adhère au cycle de vie du système d'information.

Tableau 3 : les étapes de la méthode

Le principe de complétude, dans sa composante « nombre de barrière minimum », provient d'une approche pragmatique issue du monde nucléaire : on considère que l'une des trois barrières est affectée par l'incident ou l'agression initiatrice de l'incident, que l'une des deux autres est défaillante pour une raison fortuite et qu'ainsi les conséquences sont limitées "à coup sûr" par la troisième.

3.2 Mise en œuvre du concept

La défense en profondeur vise donc à maîtriser l'information et le système qui la supporte par l'équilibre et la coordination de lignes de défense dynamiques ou statiques dans toute la profondeur du système d'information. C'est à dire dans la dimension organisationnelle, de la mise œuvre et des technologies. Il ne s'agit ici de fournir une boite à outils de la défense en profondeur ou bien une de bonnes ou meilleures pratiques mais d'illustrer par des exemples ce que peut être concrètement une défense en profondeur. Pour une démarche cohérence et structurée, il est indispensable de suivre la méthodologie proposée au chapitre suivant.

3.2.1 Profondeur de l'organisation

Mettre de la profondeur dans une organisation au sens de la défense en profondeur ce pourrait être en premier lieu de définir une chaîne de responsabilité de bout en bout c'est à dire de l'utilisateur au responsable sécurité. Cette continuité dans l'organisation passe par des actions de sensibilisation et de formation régulières et testées.

Cette chaîne de responsabilité doit être connue de tous et bénéficier de procédure de remontée d'incidents et de diffusion d'avis ou d'alerte de sécurité. Comme toutes lignes de défense, celles mises en place d'un point de vue organisationnel, doivent être surveillées et des procédures de secours doivent être prévues.

L'organisation dans la profondeur consiste également à prévoir les retours d'expériences afin de faire bénéficier tout le monde de l'expérience des autres. Ces retours d'expérience sont également l'occasion de faire vivre le référentiel de sécurité tout au long du cycle de vie du SI qui ne dépend pas que des technologies utilisées mais également des hommes et des compétences disponibles. Le retour d'expérience doit être différencié selon que l'on s'adresse à des utilisateurs ou à des exploitants du système. Il peut être judicieux de prévoir une organisation du retour d'expérience de façon anonyme ou tout du moins en dehors de toute hiérarchie fonctionnelle.

Le référentiel sécurité du système d'information doit être validé au plus haut niveau, et connu de tous. Cela signifie donc que le référentiel sécurité ne jouera son rôle que dans la mesure où il touchera toute la profondeur de l'organisation. La sécurité doit être l'affaire de tous et non une niche d'expert.

L'organisation doit rechercher de façon continue dynamique à apprécier son niveau de sécurité au regard d'objectifs de sécurité issus d'une analyse de risque. L'organisation doit avoir la capacité soit à s'auto-surveiller soit faire appel à une tierce partie afin d'évaluer son niveau de sécurité.

Le système d'information évolue dans un environnement physique, qui a des interactions permanentes avec lui. Ces actions doivent être surveillées et des procédures d'urgence doivent être prévues.

La notion d'intégration de la sécurité dans les projets témoigne également d'une certaine maturité. Enfin, l'homologation de sécurité et la capacité de l'organisation à la remettre en jeu en fonction de l'environnement, du cycle de vie des systèmes, des incidents de sécurité sont des points clés dans la défense en profondeur.

3.2.2 Profondeur dans la mise en œuvre

La mise en œuvre de la sécurité doit s'appuyer sur des politiques validées et testées. Cela suppose également les utilisateurs participent directement à la remontée des incidents et bénéficient d'information sur les alertes de sécurité.

Pour être défendu dans la profondeur le système d'information doit avoir une politique dynamique de mises à jour des outils et du référentiel documentaire. Sans ces mises à jour et ces remises en question des procédures de sécurité la défense risquerait d'être une illusion.

Toute mise en œuvre d'outils exige leur administration, leur suivi et leur contrôle. Cela passe en particulier par une analyse des traces permettant de détecter des incidents. Une ligne de défense, quel que soit son type, doit être surveillée.

La politique de maintenance doit également avoir une profondeur en diversifiant les fournisseurs, vérifiant et en testant les contrats en s'assurant qu'ils sont conformes aux objectifs de sécurité.

3.2.3 Profondeur dans les technologies

La défense en profondeur consiste donc à opposer aux menaces des lignes défense coordonnées et indépendantes. Sur le plan des technologies cela peut signifier par exemple que la compromission d'un service réseau ne doit pas permettre d'obtenir les droits les plus élevé sur l'ensemble du système. Dans ce contexte, donner des droits d'administration à tous les utilisateurs d'un système est contraire à la défense en profondeur. En matière de protection de l'information cela peut aussi signifier que le chiffrement au niveau applicatif n'est en soi pas suffisant et qu'il pourrait être nécessaire de protéger également la couche IP.

La défense en profondeur a donc pour conséquence de ne pas faire reposer la sécurité sur un élément mais sur un ensemble cohérent. Cela signifie donc qu'il ne doit en théorie pas exister de point sur lequel tout l'édifice repose. Ainsi, la défense ne doit reposer sur une technologie ou un produit de sécurité quelque soit sa qualité. En tant que barrière, un produit de sécurité doit être surveillé, protégé et bénéficié de plan de réaction encas d'incident.

Il est nécessaire de chercher à réduire l'exposition du système aux différentes menaces. Cela signifie par exemple de créer des enclaves à l'aide de firewall et de systèmes de détection d'intrusion. Dans ce cadre de moindre exposition, il est systématiquement nécessaire de limiter les services offerts au strict besoin.

Mettre de la profondeur dans les technologies s'est également défendre jusqu'au poste utilisateurs en installant des firewall sur leur poste ainsi qu'un antivirus régulièrement mis à jour et de nature différente que celui installé sur la passerelle de messagerie. Ces outils doivent s'accompagner d'une formation des utilisateurs afin de leur prendre conscience que la technologie ne suffit pas et qu'il faut rester vigilant quels que soient les outils déployés.

4 La méthode de défense en profondeur

Cette méthode permet à une maîtrise d'ouvrage de prendre en compte les principes de la défense en profondeur tels qu'ils ont été définis précédemment (cf §3.1.3). Elle apporte en particulier la possibilité de qualifier un système et d'une certaine façon d'en mesurer le niveau de défense. Pour atteindre cet objectif, la méthode prend comme hypothèse qu'une gestion des risques a été conduite au préalable. Enfin, cette méthode s'inscrit dans un processus d'intégration de la SSI dans les projets.

La méthode permettant d'appliquer le concept de défense en profondeur à la sécurité des systèmes d'information comprend les étapes suivantes :

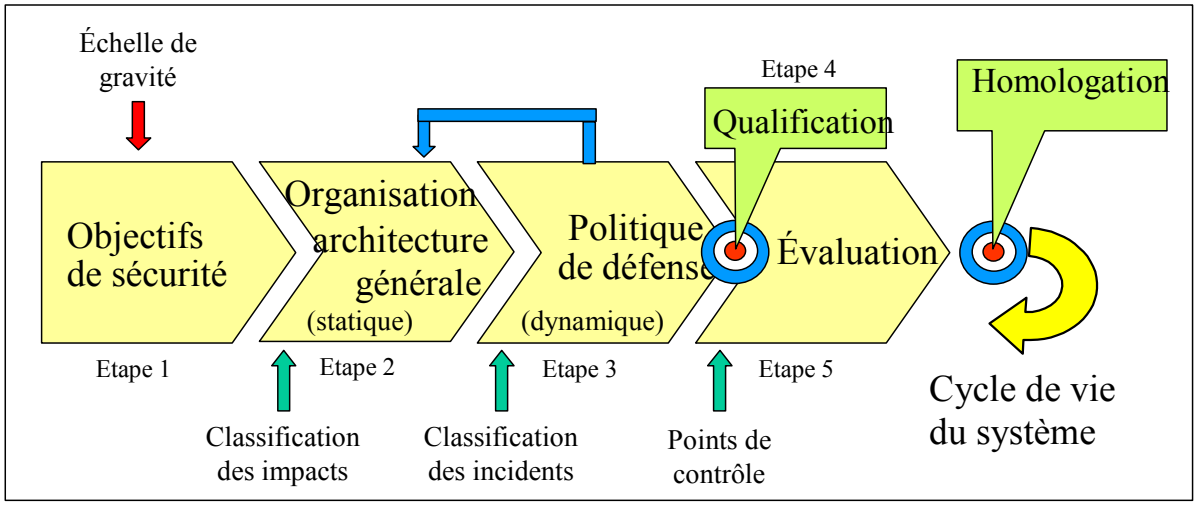


Figure 5 : les étapes de la méthode

1. Détermination des biens des objectifs de sécurité. C'est à partir des résultats de cette étape que sera construite la défense en profondeur . Les objectifs de sécurité permettent de classifier les impacts sur l'échelle de gravité, ce qui permettra ensuite de fixer les incidents de sécurité sur cette échelle et donc de communiquer à partir d'un tableau des incidents, associé à une représentation schématique du système d'information et des lignes de défense.

2. Élaboration de l'organisation et de l'architecture générale du système (la profondeur du dispositif). C'est dans cette étape qu'il faut définir les points de contrôle et d'évaluation. Elle doit être menée le plus en amont possible dans les projets et permet de mettre en évidence les barrières, la gravité des incidents de sécurité (en fonction du nombre de barrières résiduelles) et les lignes de défense.

3. Élaboration de la politique de défense qui comprend deux volets : le premier organise le renseignement et le second la défense réactive correspondante *(inter-réaction, planification)*. Cette étape définit la politique opérationnelle de la défense et met en évidence les points de contrôle. Cette politique de défense doit permettre l'observation du système, la remontée des événements de sécurité pour alimenter le tableau de bord et la prise de décisions sur les moyens de réaction à mettre en

œuvre. Cette étape a un aspect opérationnel et dynamique alors que la précédente est plus statique.

4. La cohérence globale du système ainsi que les mesures complémentaires prises dans les étapes précédentes doivent permettre d'obtenir un haut niveau de protection. Ce niveau doit être ensuite **démontrable**. L'objectif de cette étape est donc de qualifier le système d'information au regard des critères de défense en profondeur.

5. Évaluation de la défense permanente et périodique à partir des méthodes d'attaques et du retour d'expérience. Cette étape correspond à la partie contrôle et audit. Mise à jour de la défense à partir des résultats de l'évaluation et pour prendre en compte les évolutions. Cette étape correspond donc aux opérations de maintien en condition de sécurité. Elle devrait déboucher sur une décision d'homologation qui doit rester cohérente avec les évolutions du système tout au long de son cycle de vie.

4.1.1 Première étape : détermination des biens et des objectifs de sécurité

Cette première étape se compose donc des actions suivantes, somme toute classiques : détermination des biens à défendre et de leur criticité (l'analyse de risque qui permettra ensuite de quantifier la valeur de la défense : la fiabilité d'un équipement doit être pondérée par la valeur de la conséquence de sa perte pour graduer le niveau d'alerte).

A l'issue de cette première étape, les acteurs du modèle sont identifiés et les besoins de sécurité sont définis.

Une méthode de type EBIOS est particulièrement adaptée pour réaliser cette étape. En effet, « **EBIOS contribue à l'élaboration des tâches que la maîtrise d'ouvrage doit réaliser**. Elle permet en effet de déterminer le périmètre de l'étude tout en gardant une vision globale du système étudié dans son contexte, d'exprimer des besoins (liés aux biens à protéger), d'identifier des menaces et de définir un plan de projets et des responsabilités»[7].

L'échelle de gravité proposée pour classer les événements de sécurité en fonction de leur impact sur le système d'information est indiquée dans le tableau suivant. Elle est inspirée de l'échelle INES.
Toutefois, l'échelle INES distingue les incidents des accidents en fonction de l'impact hors site ou non de l'événement. Dans le cadre de la sécurité des systèmes d'information, cette distinction n'a pas de raison d'être. L'échelle proposée est donc fondée uniquement sur l'impact de l'événement.

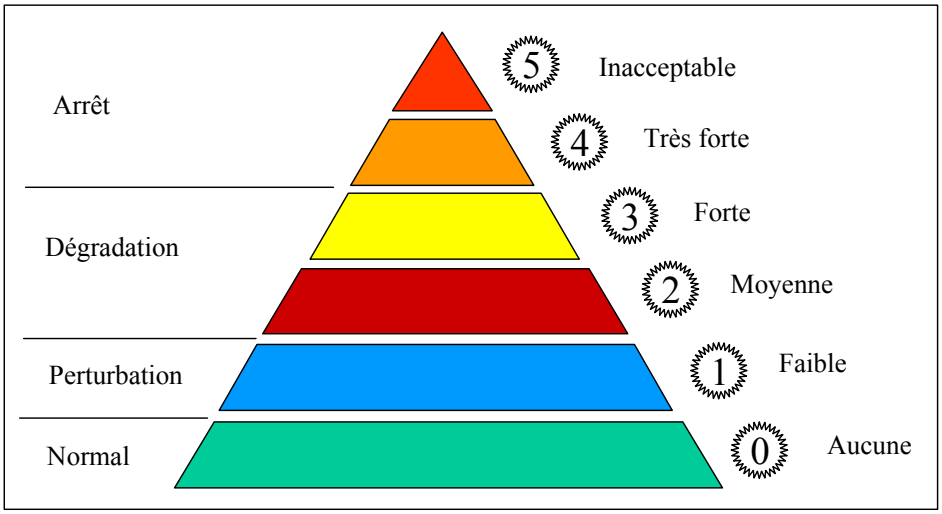


Figure 6 : échelle de gravité SSI

Cette gravité peut se mesurer de façon très variée : dans certains cas il s'agira de mesurer une perte économique dans d'autres cas de comparution devant un tribunal. C'est pourquoi, Il est essentiel de comprendre que cette mesure de la gravité d'un incident doit se faire à la suite d'une gestion des risques et non sur de simples appréciations de situation.

[7] Expression des besoins et identification des objectifs de sécurité – Mémento – Version du 4 février 2004

Catégorie	Niveau	Gravité	Critère
Arrêt	5	Inacceptable	L'événement met en cause la survie de l'entreprise (le fait redouté est arrivé).
	4	Très forte	L'événement présente un risque très important et nécessite donc des mesures d'urgence immédiates.
Dégradation	3	Forte	L'événement n'entraîne pas de risque important mais une partie significative du système a été touchée.
	2	Moyenne	L'événement a une conséquence sur le fonctionnement normal et doit entraîner une réaction immédiate.
Perturbation	1	Faible	L'événement n'a pas de conséquences notables mais doit être traité pour rétablir un fonctionnement normal.
Fonctionnement normal	0	Aucune importance du point de vue de la sécurité	Fonctionnement normal.

Tableau 4 : échelle de gravité SSI.

Dans cette étape, il s'agit donc d'indiquer le niveau de gravité des principaux événements redoutés (on pourra prendre les facteurs de risque étudiés dans l'analyse de risque par exemple) pour les différents biens à protéger.
Il importe que l'analyse menée à cette étape soit le fruit de la combinaison et validation mutuelle d'une approche déductive (par les ressources) puis inductive (par les menaces) et que soit pris en compte le facteur humain. Les *scénarii* élaborés lors de cette étape seront modélisés dans l'étape suivante.

4.1.2 Deuxième étape : architecture générale du système

Cette étape vise à déterminer la profondeur du dispositif et à faire des choix sur les organisations, les technologies et les procédures de sécurité. Pour faire ces choix et identifier les points les plus sensibles aux différentes menaces, il est préconisé par la méthode de procédé d'abord par une approche inductive (la plus naturelle et couramment employée), qui consiste à partir de la menace et à prévoir des lignes de défense jusqu'au bien à protéger. Ensuite, l'expert SSI développe une approche déductive en partant du bien à protéger vers la menace afin de mettre éventuellement en place de nouvelles lignes mais également d'identifier les points les plus exposés dans le système.

On identifie les points suivants dans cette partie :
- découpage des zones en fonction des risques, des acteurs, des grandes fonctions de l'entreprise (l'urbanisation du système d'information) . Ce découpage est établi selon les principes d'indépendance des entités et de cloisonnement ;
- détermination des barrières (moyen technique, procédural et humain) ;
- classification des zones en fonction de leur sensibilité et détermination des règles de passage de l'une à l'autre (c'est dans cette étape qu'il convient de traiter le cas de la classification des informations et des mesures à prendre pour l'interconnexion de deux domaines de niveaux de sécurité différents) ;
- découpage des zones en domaines de confiance : introduction des cloisonnements organisationnels en général (la profondeur de l'organisation) ;
- répartition privé/commun dans chaque domaine et entre domaines.

Il paraît indispensable dans cette étape :

- d'établir un "tableau des mesures" prises afin de bien montrer les moyens de défense dans toute la profondeur ;
- de modéliser les systèmes critiques afin de les évaluer ;

- de fixer les incidents (franchissement d'une barrière) sur l'échelle de gravité globale en fonction de la classification des impacts définie précédemment, car elle permettra au niveau de la politique opérationnelle d'apporter la graduation des actions et de définir les lignes de défense (c'est dans cette étape que la transposition des barrières en lignes de défense est effectuée).

Cette étape doit être menée normalement en amont des projets c'est-à-dire qu'une étude de sécurité doit être **intégrée** dans la gestion du projet. Dans la mesure où le système existe déjà, la méthode est la suivante[8] :

- analyser la topologie du système d'information, tant technique que fonctionnelle ;
- identifier les barrières existantes ;
- modéliser les processus les plus importants (modélisation des données critiques et des principales menaces afin de mettre en évidence les barrières) ;
- évaluer l'architecture déjà en place pour déterminer les modifications à apporter afin qu'elle réponde aux critères (ajout de nouvelles barrières par exemple).

4.1.3 Troisième étape : élaboration de la politique de défense

Cette étape est composée de deux sous-étapes :

- détermination de la défense globale et coordonnée[9] :
  - détection (détermination des points de contrôle et de détection des attaques) ;
  - remontée de l'information ;
  - corrélation des événements ;
  - alerte ;

- planification :
  - détermination des reconfigurations possibles, avec un fonctionnement normal (dispositif de tolérance aux pannes avec des performances identiques) et avec un fonctionnement en mode dégradé (par exemple : fonctionnement en local uniquement, performances moindres, etc.) ;
  - plans de réaction (planification des actions possibles en fonction des événements redoutés, plan de continuité par exemple mais aussi reconfiguration réseau, mise en œuvre de moyens de secours, etc.).

La défense globale se décline selon les trois axes (organisationnel, mise en oeuvre, technologique) qui intègrent les lignes de défense déployées sur les zones définies à l'étape précédente. Chaque ligne dispose idéalement de trois fonctions de sécurité : protection, détection et réaction. La politique de défense doit déterminer pour les différents incidents de sécurité leur gravité afin de bénéficier de l'apport "pédagogique" de la méthode permettant une meilleure sensibilisation des personnels. Les niveaux de gravité des incidents seront déduits ensuite à partir du nombre de lignes de défense restantes.

[8] Pour cette partie, le lecteur se reportera utilement aux meilleures pratiques éditées par la DCSSI :

- **MEILLEURES PRATIQUES POUR LA GESTION DES RISQUES SSI -** Exploitation des résultats de la méthode EBIOS® pour l'étude d'un système existant – Version du 2 févirer 2004 ;
- **MEILLEURES PRATIQUES POUR LA GESTION DES RISQUES SSI -** Exploitation des résultats de la méthode EBIOS® pour l'étude d'un système à concevoir – Version du 13 janvier 2004.
- [9] Pour cette partie, le lecteur se reportera utilement aux meilleures pratiques éditées par la DCSSI : **MEILLEURES PRATIQUES POUR LA GESTION DES RISQUES SSI -** Exploitation des résultats de la méthode EBIOS® pour élaborer une PSSI – Version du 21 mars 2003.

La gravité d'un incident dépend plus des moyens de défense restants que de ceux qui ont été franchis. En effet, par exemple une attaque interne peut permettre de sauter plusieurs barrières qui seraient à franchir en cas d'attaque externe. Il est que selon les principes de la défense en profondeur définit précédemment :

- il y a au minimum 3 lignes de défense ;
- le nombre de lignes de défense doit être adapté au risque (probabilité d'occurrence et criticité du bien).

La défense doit être à la fois globale (tous les moyens participent au même objectif de sécurité) et coordonnée. Cette coordination concerne principalement les moyens de renseignement (permet de préciser la menace réelle par analyse de plusieurs informations concernant une attaque en cours) et de réaction (reconfiguration de moyens de défense à partir de la détection d'un autre moyen de défense, y compris des moyens de filtrage). Il est à noter que cette coordination concerne plus les barrières que les lignes de défense.

La dynamique de la défense est apportée par la planification des réactions en cas d'atteinte à la sécurité. Les incidents et accidents doivent être classifiés selon l'échelle de gravité et déclencher obligatoirement une réaction qui est du niveau technique (réponse automatique), procédural (application de la procédure ou du plan correspondant) ou humaine (décision, initiative, etc.). Les plans de réactions doivent être gradués de la même manière que les atteintes à la sécurité pour renforcer les mesures en fonction du niveau de gravité. En effet, dans le cadre de la défense en profondeur, la prise en compte de plusieurs incidents en même temps doit être prévue.

Parmi les mesures non-techniques à prendre, celles visant à des actions en justice contre des tiers extérieurs sont à prévoir de même que celles prévues au règlement intérieur contre les personnels de l'entreprise (à la technique de fournir les éléments de preuves qui étayerons ces mesures).

4.1.4 Quatrième étape : qualification de la défense en profondeur

Dans cette étape il s'agit de conduire la qualification (validation de l'organisation et de l'architecture) du système qui résulte de deux approches : la première est qualitative tandis que la seconde est démonstrative au travers de l'étude des *scénarii* applicables.

4.1.4.1 L'approche qualitative

Cette approche formelle vise à vérifier le respect des principes de la défense en profondeur définit précédemment (§ 3.1.3). Elle vérifie aussi le respect de la méthode telle qu'elle peut être formalisée au niveau de l'organisme.

Cette partie s'apparente donc à une démarche qualité. Elle est très proche du chapitre 7 (« rational ») de la norme ISO 15408 (critères communs) qui permet de démontrer la complétude des objectifs de sécurité au regard des menaces retenues.

4.1.4.2 L'approche démonstrative

La méthode de qualification doit être cohérente avec la méthode globale de défense en profondeur telle qu'elle a été construite et en particulier s'appuyer sur les résultats produits au cours des différentes étapes.

Cette méthode est schématisée dans la figure ci-dessous et explicitée ci-après.

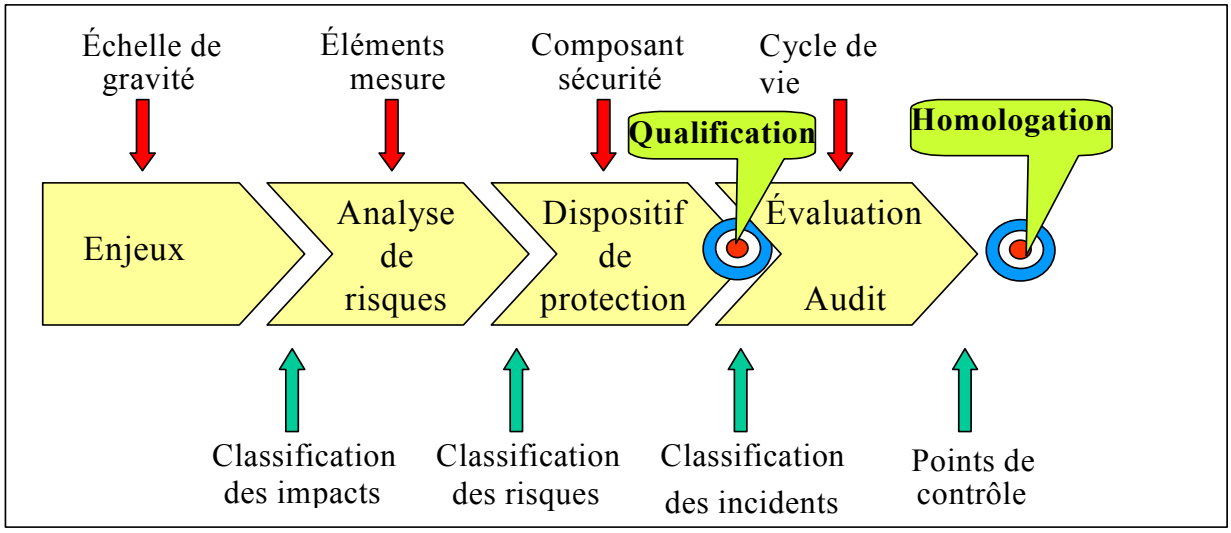


Figure 7 : principes d'une évaluation

La première étape, détermination des objectifs de sécurité, permet d'une part de classer les impacts potentiels sur l'échelle de gravité en fonction des enjeux et d'autre part de déterminer les éléments de mesure pour classifier les risques.

La seconde étape, architecture du système, a comme résultat un classement des incidents de sécurité en fonction des composants défaillants.

La troisième étape, élaboration de la politique de défense, a mis en évidence les points de contrôle qui seront utilisés pour l'évaluation permanente du dispositif au cours de cette étape de qualification.

La méthode s'appuie donc sur :

- une méthode d'analyse de risques de la sécurité des systèmes d'information complétée par la hiérarchisation des risques par composants principaux et par fonctions de sécurité sur l'échelle de gravité, définie précédemment, qui permet de classer les incidents de sécurité ;
- une modélisation de la défense en profondeur appliquée aux risques principaux et l'analyse des *scénarii* les plus importants (*scénarii* "enveloppe" en particulier) ou les plus probables. Ces *scénarii* sont itératifs ; ils permettent de déterminer les barrières et d'évaluer la défense en pratiquant la méthode du composant défaillant jusqu'à obtenir la "démonstration" de la robustesse de la défense ;
- une classification des incidents de sécurité sur l'échelle de gravité précédente effectuée en fonction des risques définis. Les points de contrôle du bon fonctionnement ainsi que ceux permettant de détecter les attaques éventuelles sont mis en évidence ; ils permettront de procéder à l'évaluation permanente et périodique ;

- les évaluations menées d'une part par les méthodes d'audit habituelles et d'autre part par l'évaluation des défenses au travers des *scénarii* et des incidents de sécurité (recherche des conséquences potentielles) ;
- les différentes études permettant de démontrer le niveau de sécurité atteint et de communiquer sur le sujet pour mettre en place la défense en profondeur et sensibiliser les personnels aux incidents de sécurité (aspect communication renforcé par la présence d'un tableau de bord de sécurité mettant en évidence les incidents sur l'échelle de gravité).

La méthode de qualification de défense en profondeur utilise donc deux méthodes démonstratives d'analyse qui sont :

- l'analyse par scénario "enveloppe" : cette analyse consiste à établir un scénario couvrant le risque maximum (la destruction du site principal) et de montrer que les autres *scénarii* (impossibilité de rentrer dans le site principal par exemple) sont inclus dans le cas "enveloppe" et donc que la solution retenue les couvre. Cette approche permet de vérifier la cohérence du nombre de barrières avec la gravité de l'événement redouté ;

- l'analyse par "composant défaillant". Il s'agit de postuler un incident de sécurité et une défaillance aléatoire d'un autre composant situé entre l'incident et l'événement redouté pour analyser la protection restante et vérifier qu'elle est suffisante.

4.1.4.3 Conclusion

En conséquence, la méthode complète l'analyse qualitative globale classique par une analyse quantitative de type déterministe dans les cas particuliers des *scénarii* de risques importants en utilisant la notion de scénario enveloppe et de composant défaillant. Cette méthode est bien adaptée au principe de "démonstration" de la sécurité qui est la règle dans le cas de la sûreté nucléaire et qu'il convient de promouvoir.

La qualification spécifique au concept de défense en profondeur, doit donc permettre de vérifier la cohérence entre le nombre de lignes de défense et la gravité des événements redoutés déterminée à la fin de la première étape ainsi que l'acceptation des risques résiduels en cas d'insuffisance.

Les trois premières étapes ne sont pas séquentielles mais itératives jusqu'à obtenir le niveau de sécurité exigé par la criticité de la ressources à protéger, des menaces potentielles et des risques résiduels. Cette étape permet de mettre en évidence les risques résiduels qui doivent être connus et acceptés.

4.1.5 Cinquième étape : évaluation permanente et périodique

En outre, l'évaluation doit être à la fois périodique (mise en place initiale et révision périodique proprement dite) et permanente (exploitation du retour d'expérience et de la veille technologique).

Cette étape a pour objet d'évaluer la défense de manière systématique :

- étude statique des composants ;
- dynamique sur incident (retour d'expérience) ;
- tableau de bord ;
- audit périodique ;

- rétroaction (Cf. ci-après).

Cette étape est étroitement liée à la suivante car elle participe au même but, actualiser la défense et la renforcer en prenant deux critères essentiels tirés de l'exemple de la RATP pour les cas non quantifiables en terme de coût/gain :

- ne pas régresser ;
- améliorer si le coût en vaut la peine.

Les résultats de cette étape doivent permettre de présenter aux décideurs les mesures prises pour satisfaire aux besoins de sécurité définis à l'étape 1 et ainsi démontrer que les objectifs sont bien atteints.

Un effort de communication est à effectuer dans cette étape pour regrouper les *scénarii* par famille et mettre en évidence les principales lignes de défense ainsi que les mesures planifiées de réactions prévues.

Cette étape s'inscrit dans le cycle de vie du système, et à ce titre elle doit en prendre en compte les opérations de maintien en condition opérationnelle lié à des évolutions des organisations, des technologies et des procédures..

Cette étape doit déboucher sur une décision d'homologation de sécurité permettant de déclarer le système d'information, apte à traiter d'information d'un niveau de sensibilité donné. Cette homologation est intimement liée au cycle de vie du système et n'est jamais une décision permanente.

5 Conclusions

L'étude de la défense en profondeur dans le cadre de la sécurité des systèmes d'information fait apparaître :

- que le concept est souvent cité comme une notion de bon sens sur le redondance des technologies employées ou pour regrouper différents principes largement diffusés, mais la réflexion de fond n'est pas développée actuellement dans le cadre de la SSI ;
- que le concept mis en œuvre dans le milieu industriel est plus riche que les méthodes d'analyse de risques utilisées habituellement mais reste pragmatique et par là même est facilement transposable ;
- que le concept, avec sa dynamique et sa facilité de communication, est un enrichissement notable des méthodes habituelles avec lesquelles il est compatible ;
- que le concept est appliqué concrètement dans le monde nucléaire en particulier, afin de qualifier des systèmes.

Par rapport aux méthodes habituellement utilisées pour la sécurité des systèmes d'information ou proposées dans la bibliographie et se présentant comme issues de la méthode de défense en profondeur, la méthode proposée dans ce document paraît apporter les améliorations suivantes :

- importance de **l'analyse quantitative** permettant d'évaluer le système dans le futur ;
- qualification à partir des **modélisations** particulières donnant une évaluation initiale ; en effet, des scénarii enveloppes paraissent bien mieux adaptés et plus réalisables que des analyses probabilistes ;
- **profondeur de l'organisation** s'appuyant sur une démonstration de la sûreté du dispositif à partir des *scénarii* de risques et des lignes de défense ;
- évaluation selon une **échelle de gravité**, type échelle INES, apportant un aspect **communication** très fort ;
- aspect **global** de la défense ;
- importance du **renseignement** et de l'observation (points de contrôle) préservant la liberté d'action ;
- aspect **dynamique** de la défense intégrant le processus veille, alerte, réponse et la planification ;
- **évolutivité** de la défense par l'organisation des retours d'expériences (recherche des conséquences potentielles et non seulement des causes), celui-ci permettant de valider les *scénarii*, les mettre à jours, etc. ;
- **démonstration** de la défense permettant de qualifier un système d'information.

Il ne faut pas oublier non plus que le terme de **défense** (au lieu de sécurité) est porteur d'idées fortes car il apporte les notions de dynamique, d'initiative et de liberté d'action, de fonctionnement dégradé etc. et ne cantonne pas à mettre des moyens de protection passifs en place.

Ce concept de la défense en profondeur appliquée aux systèmes d'informations apporte également une approche originale sur la problématique de la qualification de systèmes. Les mondes du transport ou du nucléaire se sont appuyés sur ce concept pour qualifier leur installation, la SSI doit pouvoir s'en inspirer. Les principes applicables à la SSI, identifiés

dans ce document et la méthode proposée pour les mettre en œuvre pourraient utilement contribués à définir la qualification d'un système d'information.

Il est à noter que le concept de la défense en profondeur peut s'appliquer à toutes les strates d'un système d'information aussi au niveau macroscopique comme dans ce document que dans des aspects plus microscopique comme par exemple dans l'évaluation d'un produit ou dans l'implémentation d'un algorithme.

Des axes d'étude complémentaires paraissent intéressants :

- le développement d'un outillage de la méthode afin de modéliser les scénarii et de faire apparaître les lignes de défense en fonction des conséquences des incidents de sécurité ;
- la formalisation de la méthode et un travail de recensement des composants, moyens de contrôles, moyens de détection des attaques, etc. ;
- la réalisation d'ensembles de composants d'architectures types, dont la résistance est éprouvée, permettant de capitaliser sur les différentes études (par exemple pour les centrales nucléaires de même technologie) ; ces ensembles devraient être modulaires pour être réutilisables ;
- la réalisation d'études plus théoriques sur la détermination d'une probabilité de résistance des composants qui devrait être liée à une notion de certification ou à l'évaluation quantitative de la sécurité.

6 Annexe : Application de la méthode proposée

Dans ce document, seuls les points particuliers les plus significatifs de la méthode sont présentés.

6.1 Présentation du cas concret

Le cas concret étudié est celui d'un télé-service dédié dédié à la demande via Internet de délivrance d'une pièce d'identité. Chaque usager dispose via ce télé-service d'une fonctionnalité lui permettant de savoir à un instant donné où en est sa demande.

Les usagers sont identifiés avant toute connexion (contrôle de l'identité, détermination des conditions de la demande, etc.). Une fois réalisés, les documents fournis par ce télé-service sont stockés au plus près des usagers (mairie et préfecture) afin de minimiser les déplacements des usagers.

Le télé-service est organisé en plusieurs services correspondant chacun à une fonction :

- centraliser des demandes des usagers parvenant par Internet ;
- donner les ordres aux différents services de l'administration pour le traitement de la demande ;
- transmettre les informations à un service d'archivage.

L'étude sécurité, menée selon la méthode proposée dans le présent document, concerne donc uniquement les systèmes d'information suivants :

- l'interface avec les usagers permettant de recevoir les demandes par e-mail Internet (système de communication comprenant un dispositif d'accès à Internet et un système de messagerie) ;
- l'interface avec les autres administrations (système de communication de type intranet étendu) ;
- l'interface avec l'autorité (système d'interconnexion de deux intranets).

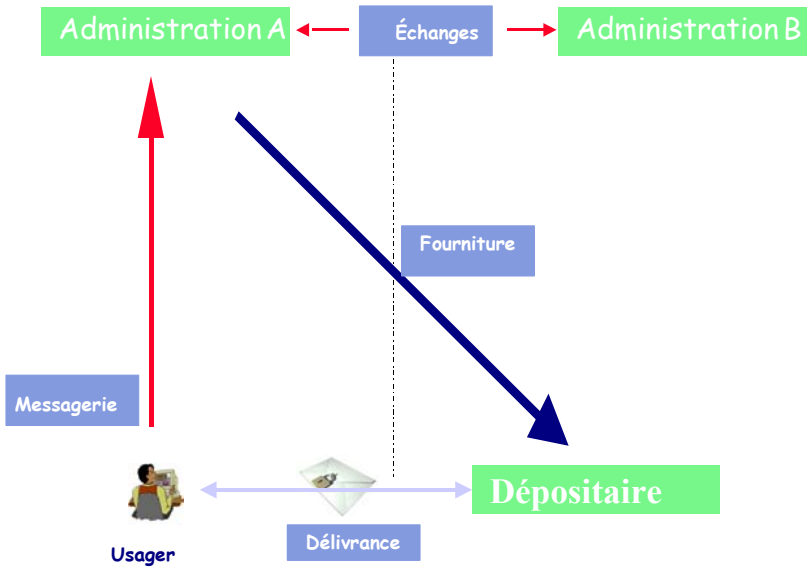


Figure 8 : description du télé-service

Sur le plan de la sécurité, le télé-service se compose d'éléments présentant les caractéristiques suivantes :

- le système (matériel et logiciel et réseau intranet) proprement dit ;
  - les serveurs et les postes de travail, formant un réseau dédié ;
  - ce système est situé dans chaque administration et sous sa responsabilité ;
  - les utilisateurs sont des personnels de l'administration ;
  - le support technique est réalisé par des personnels extérieurs identifiés ;

- l'interface avec les usagers par e-mail Internet (système de communication comprenant un dispositif d'accès à Internet et un système de messagerie) :
  - les mails contenant les pièces jointes arrivent sur un poste dédié disposant de la connexion Internet ; les pièces jointes sont extraites automatiquement par un outil qui contrôle la validité de la commande (adéquation entre l'adresse e-mail et le numéro identifiant l'usager dans la commande) ;
  - utilisation d'un système de communication peu sécurisé (Internet) ;

- l'interface avec les autres administrations (système de communication de type intranet étendu) :
  - connexion entre les deux réseaux par VPN Internet ;
  - utilisation d'un système de communication moyennement sécurisé (VPN Internet) ;

- l'interface avec le dépositaire (système d'interconnexion de deux intranets) :
  - liaison entre les deux réseaux (télé service et archives) par l'intermédiaire d'une passerelle ;
  - personnel de l'administration.

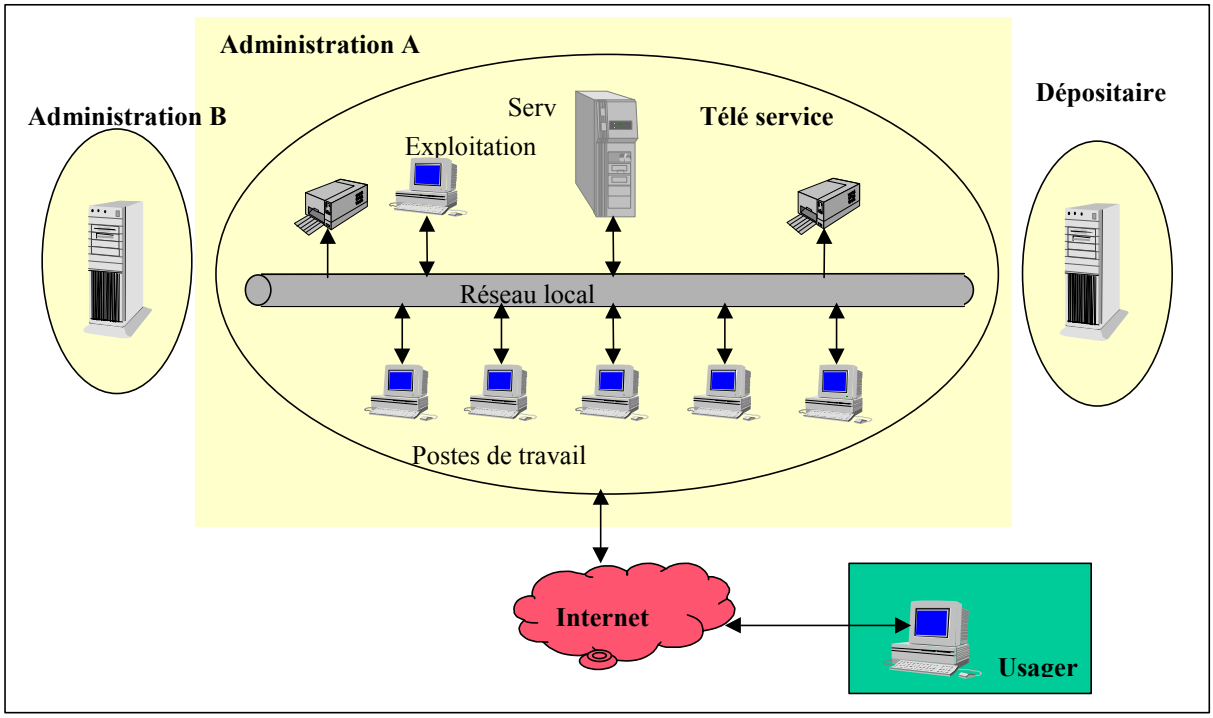
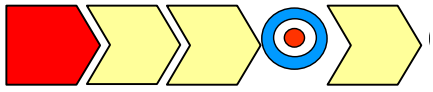


Figure 9 : description du télé-service

6.2 Déroulement de la méthode

Dans ce cas concret, on ne traite que des besoins particuliers de sécurité du télé-service en considérant que les besoins "génériques" (protection physique, protection des personnes, etc.) sont couverts par ailleurs. De même les caractéristiques du système (performance, etc.) devraient être étudiées dans le cadre du projet global proprement dit. Comme décrit dans le déroulement de la méthode, une analyse des risques est un pré requis pour aborder cette méthode. En effet, il serait illusoire de chercher une défense en profondeur de biens que l'on n'a pas identifiés faisant face à des menaces qui ne seraient que le fruit d'une simple appréciation de situation.

6.2.1 Première étape : détermination des objectifs de sécurité



Dans ce cas concret, on ne traite que des besoins particuliers de sécurité du télé-service en considérant que les besoins "génériques" (protection physique, protection des personnes, etc.) sont couverts par ailleurs. De même les caractéristiques du système (performance, etc.) devraient être étudiées dans le cadre du projet global proprement dit.

La première étape permet de définir les besoins de sécurité du système global et de ses composantes par critère de sécurité.

Le télé-service complet a donc un besoin important de disponibilité qu'il est nécessaire d'obtenir par une redondance des moyens informatiques et la présence de moyens de secours systématiques. Au cours de sa période de fonctionnement, il très probable qu'un ou plusieurs composants soient affectés par une panne matérielle, logicielle ou autre. La disponibilité du

système lui-même est le point essentiel. Ce besoin important de disponibilité est lié à l'impact d'une panne sur le fonctionnement du système. La gravité intrinsèque d'un incident mettant en cause durablement la disponibilité du système est donc jugé comme étant « Inacceptable ».

La mise en œuvre de mesures particulières au niveau de la manipulation des informations et des communications doit permettre de satisfaire à un besoin particulier d'intégrité et confidentialité. Compte tenu de l'emploi d'Internet, L'analyse de risque a permis d'identifier un certain de nombre de risques. La gravité intrinsèque d'un incident est donc « Forte » pour l'intégrité et « Très forte » pour la confidentialité, la gravité de ce facteur étant aggravée par la présence de personnels extérieurs susceptibles d'augmenter les risques d'indiscrétions.

Il est à noter que l'ensemble du télé-service doit présenter un important niveau de sécurité sur le plan de la confidentialité car la partie transport est étroitement liée aux informations manipulées. Il convient d'être précautionneux en cas d'échange de postes de travail par le mainteneur qui pourrait être extérieur au circuit. Le cryptage des fichiers stockés est un moyen à envisager si nécessaire.

Les besoins de preuve et de contrôle sont à rechercher dans le fonctionnement du système dans son intégralité car ce point participe à la sécurité complète. La tracabilité de toutes les actions et la recherche systématique des états « stables » du système doit permettre de contrôler en permanence la validité des informations en étant certain de l'authenticité des flux d'informations. La gravité intrinsèque d'un incident, est donc « Forte ».

Les moyens à mettre en œuvre pour obtenir le niveau de sécurité suffisant avec les usagers peuvent dépendre des équipements et systèmes mis en œuvre par ceux-ci, chacun pouvant avoir pris des mesures différentes les uns des autres. On notera toutefois qu'*a priori,* ils devraient utiliser un poste de travail banalisé, avec accès à l'Internet pour leur usage domestique. Dans ce cas il convient de privilégier les solutions habituelles du marché.

Ce point nécessite quand même une étude complémentaire permettant de déterminer une typologie des usagers et des moyens qu'ils comptent mettre en œuvre :

- poste dédié ou banalisé : a priori dédié ;
- lien avec un système informatisé ou non : *a priori* non ;
- etc.

La synthèse des besoins apparaît dans le tableau ci-dessous :

Sous-système	Disponibilité	Intégrité	Confidentialité	Preuve et contrôle
Télé-service proprement dit	Interruption < 1h	Non altération des données	Informations à caractère nominatives donc confidentielles	Contrôle de la validité des informations
Réception et traitement des demandes	Interruption < 2h	Non altération des données	Confidentialité par chiffrement (utilisation Internet)	Authentification de l'émetteur et preuve de la réception
Communication avec les autres administrations	Interruption < 1h	Non altération des données	Confidentialité par chiffrement (utilisation Internet)	Authentification de l'émetteur et preuve de la réception
Communication avec les dépositaires	Interruption < 4h	Non altération des données	Informations confidentielles	Historisation et trace

Tableau 5 : besoins de sécurité par critères

La méthode devant apporter les moyens de l'évaluation, il paraît important à cette étape de l'étude de hiérarchiser les objectifs de sécurité. Cette hiérarchisation permet ensuite de graduer les incidents selon l'échelle de gravité proposée par la méthode. Pour cette hiérarchisation, il convient de prendre en compte les conséquences potentielles des incidents de sécurité.

L'analyse du tableau précédent montre qu'il existe une hiérarchisation implicite des biens à protéger qui sont dans l'ordre décroissant : le télé-service proprement dit, le système de réception des demandes, le système de communication avec les administrations, le système de communication avec les dépositaires.

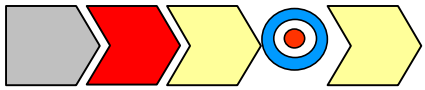
De même il existe une hiérarchisation des objectifs de sécurité : la disponibilité est primordiale, l'intégrité est jugée moins importante que la confidentialité. Le tableau ci-dessous présente donc un exemple de la hiérarchie des incidents potentiels telle qu'elle peut se dégager en utilisant l'échelle de gravité proposée par la méthode.

Gravité de l'événement redouté	Atteinte grave aux besoins de sécurité exprimés pour le critère			
	Disponibilité	Intégrité	Confidentialité	Preuve et contrôle
5 – Inacceptable	Télé-service			
4 – Très forte	Réception des demandes		Télé-service	
3 – Forte	Communication administration	Télé-service	Réception des demandes	Réception des demandes
2 - Moyenne	Communication dépositaire	Réception des demandes	Communication administration	Télé-service
1 - Faible		Communication administration et dépositaire	Communication dépositaire	Communication administration et dépositaire

Tableau 6 : hiérarchisation des événements redoutés

S'agissant dans ce document d'un exemple, la modélisation des chaînes de liaison ne concerne que les risques liés à la présence de communications avec les administrations utilisant le canal Internet, en considérant qu'il est prévu un moyen de cryptographie permettant d'authentifier le correspondant, de garantir l'intégrité des données et de préserver leur confidentialité ainsi qu'un système applicatif de contrôle des demandes.

6.2.2 Deuxième étape : architecture générale du système



6.2.2.1 Présentation de la solution globale

Le schéma ci-après fait apparaître l'architecture générale du système telle qu'elle résulte de la prise en compte des besoins de sécurité.

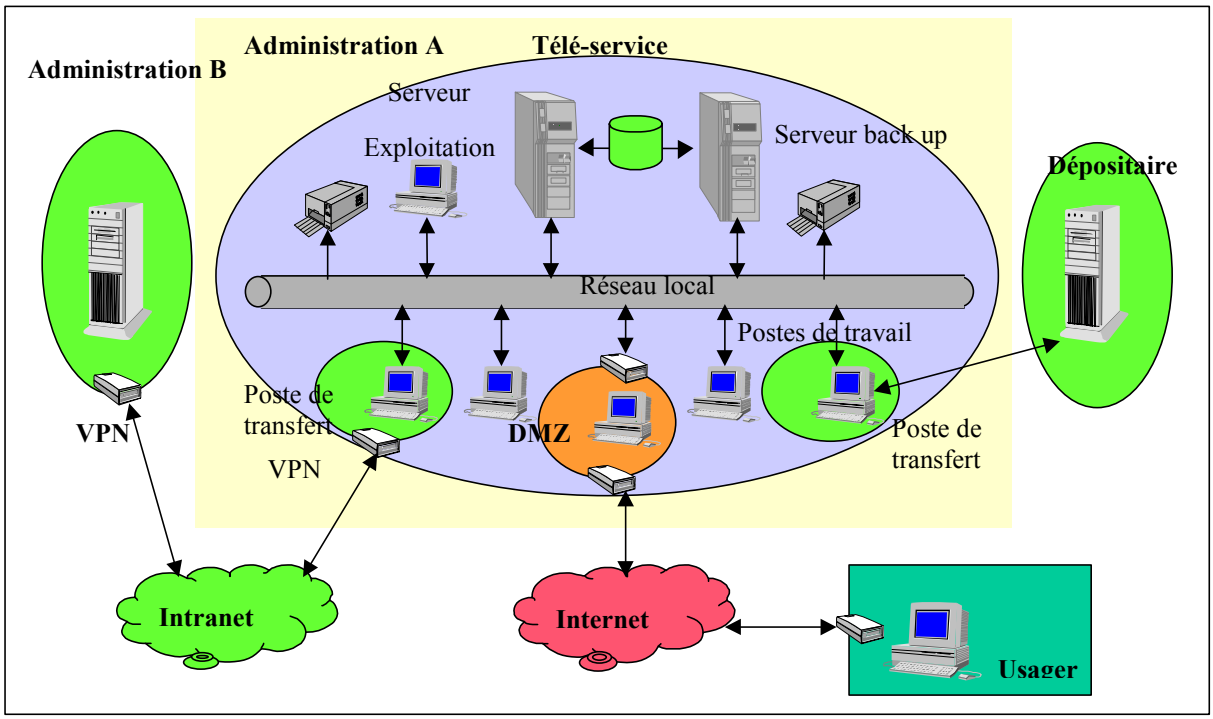


Figure 10 : architecture générale après prise en compte des besoins de sécurité

Le système est conçu autour des principes suivants :

- deux serveurs sont utilisés avec des disques RAID pouvant passer d'un serveur à l'autre, un DAT permet d'alimenter le centre de secours et un graveur de CD sert pour l'archivage ;
- les échanges sont protégés en confidentialité avec l'extérieur mais non avec le dépositaire. Tous les échanges sont effectués à partir de postes de travail dédiés et il existe des possibilités de secours. Les postes permettant les échanges ont des FireWall personnels ;
- l'antivirus est généralisé (serveurs et postes de travail) en raison de la présence d'Internet et de lecteurs de disquettes ;
- des mesures organisationnelles (contrôles par exemples) et logicielles (sur la gestion de l'information, archivage, trace, etc.) sont mises en œuvre.

6.2.2.2 Approche inductive et déductive

Il s'agit maintenant de définir les différentes barrières selon des approches inductive et déductive. Pour ces approches, on retrouve le formalisme de la méthode EBIOS et des critères communs (ISO 15408) dans la description de la menace qui se caractérise par un élément menaçant utilisant une méthode d'attaque pour atteindre un bien. Cette modélisation n'est faite ici que pour une menace jugée principale à l'issu de l'analyse de risque. Le bien critique dans ce cas concret étant les informations situées sur le serveur du télé-service. La menace est donc définie de la façon suivante :

- la **source de danger** est un malveillant cherchant à décrédibiliser le télé-service et porter atteinte à l'image de marque de l'administration ;
- la **méthode d'attaque** est le piégeage du logiciel en exploitant les vulnérabilités liées à l'usage de la messagerie ;
- **l'événement redouté** est une atteinte à la sécurité du système d'information :
  - contre l'intégrité des données : acceptation d'une fausse demande ;
  - contre la disponibilité du SI par l'indisponibilité du serveur ;
  - contre la confidentialité des données par une diffusion d'information.

S'agissant dans ce document d'un exemple, la modélisation des approches ne va concerner que les risques liés à l'usage d'Internet entre les usagers et le télé-service. Dans ce contexte, les principaux risques pris en compte sont les suivants :

- les risques majeurs conduisant à une indisponibilité prolongée du système, ces risques sont couverts par la présence d'un site de secours permettant un redémarrage en moins de 24 heures avec toutes les fonctionnalités mêmes si certaines sont dégradées ;
- l'indisponibilité du télé-service suite à une panne matérielle ou à une erreur humaine. Ce risque est couvert par redondance des moyens et des procédures de contrôle manuels ;
- la perte d'intégrité ou de confidentialité des données lors des échanges entre les différents systèmes : ce risque est partiellement couvert par l'utilisation d'un moyen de chiffrement permettant d'authentifier le correspondant, de garantir l'intégrité des données et de préserver leur confidentialité ;
- une information non valide entrant dans le télé-service par le biais du canal de communication utilisé pour collecter les demandes des usagers.

Approche inductive

Le premier scénario étudie le cas de la réception d'un message de demande au près du télé-service qui pourrait être pris pour un vrai message et donc porter atteinte à l'intégrité du système d'information (CF figure 11). Ce message passe au travers du contrôle d'accès au poste car celui-ci accepte les messages entrant. Les barrières mises en œuvre ensuite sont :

- **barrière n°11** : l'application qui extrait les messages du poste de travail vérifie que la demande est valide et correctement effectuée ;
- **barrière n°12** : l'application procède à la vérification de la signature afin d'authentifier l'émetteur, de vérifier l'intégrité de la demande ;
- **barrière n°13** : l'application contrôle la légitimité de la demande (droits, première demande, renouvellement, etc.) ;
- **barrière n°14** : l'application enregistre la demande ainsi que les erreurs ou rejets et lance éventuellement le traitement.

Le second scénario étudie le cas d'un accès non autorisé introduisant un code malicieux. Dans ce scénario, il s'agit d'un virus destructeur qui risque de porter atteinte à la disponibilité du système d'information.

- **barrière n°21** : le poste de travail est doté d'un pare-feu personnel qui est paramétré pour accepter seulement les flux de type messages en entrée et en sortie. Il est à noter que cette barrière est inefficace pour les codes malicieux transmis par mail ;
- **barrière n°22** : le poste de travail est équipé d'un anti-virus ;
- **barrière n°23** : la politique de sécurité est la seule barrière sur le poste de travail permettant de limiter une attaque du poste par un virus (principe de moindre privilège par exemple, ou politique de mise à jour) ;
- **barrière n°24** : le serveur est équipé d'un anti-virus.

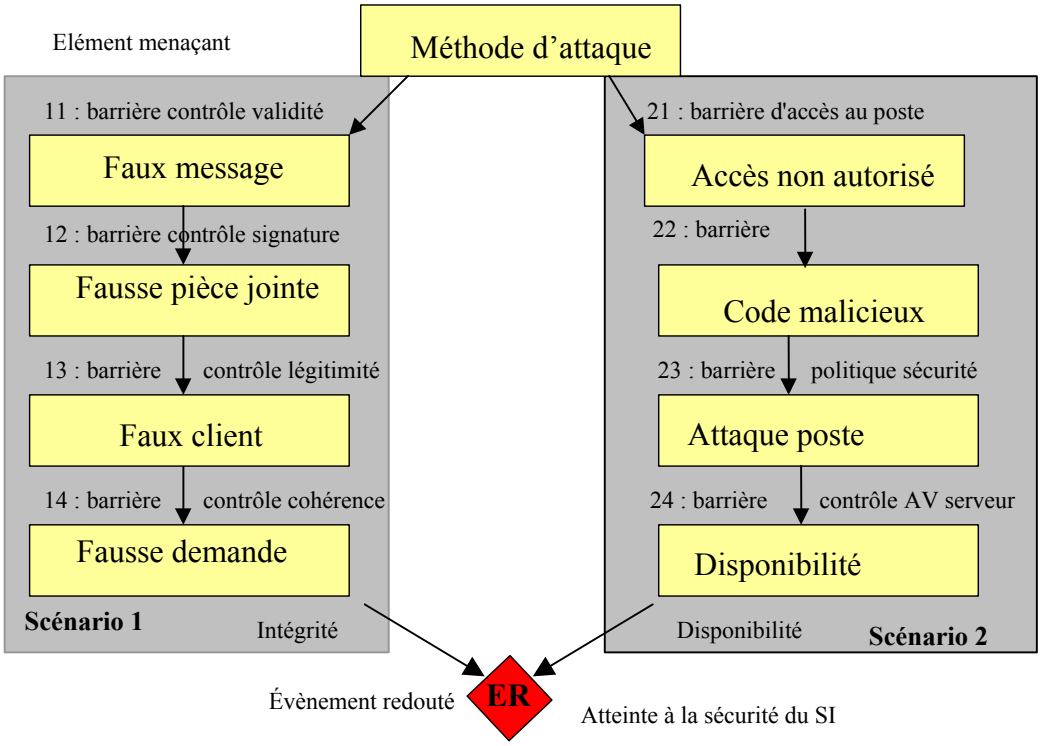


Figure 11: approche inductive

Approche déductive

Dans cette approche, on part du bien à protéger, en s'intéressant ici aux informations à caractère confidentiel, comme les données personnelles des usagers, utilisées dans le cadre du télé-service.

- **barrière n°31** : le contrôle des droits doit interdire les accès non autorisés au serveur de données ;
- **barrière n°32** : le poste de travail est doté d'un pare-feu personnel qui est paramétré pour accepté seulement les flux de type messages en entrée et en sortie ;
- **barrière n°33** : le poste de travail est équipé d'un anti-virus détectant, y compris, les messages dans les pièces jointes.

- **barrière n°34** : le pare-feu personnel est paramétré pour ne laisse sortir que le flux autorisé.

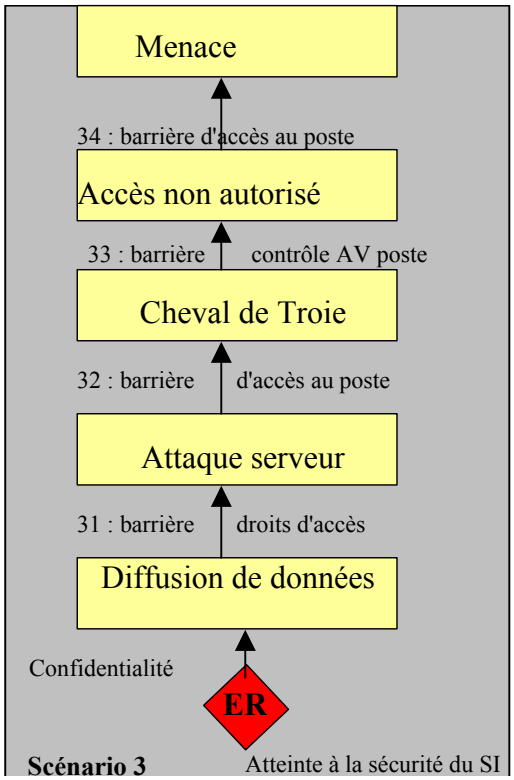


Figure 12 : approche déductive

En combinant les deux approches ont remarques que certaines barrières sont particulièrement exposées dans la mesure où elles se retrouvent dans plusieurs *scénarii* et selon les deux approches. Ce constat contredit le principe d'indépendance : une destruction de la barrière ferait sauter en même temps la première et la dernière ligne de défense et doit donc entraîner un renforcement de ces points clés.

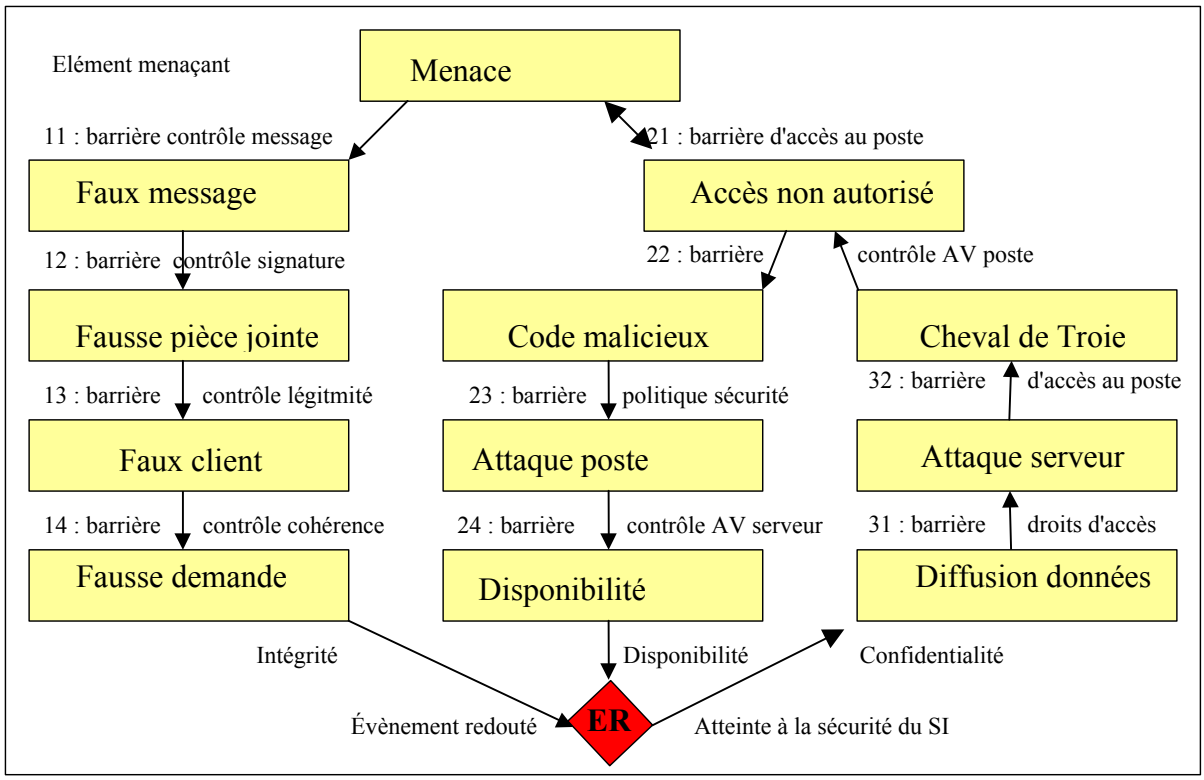


Figure 13 : combinaison des approches

Conclusion

On s'aperçoit donc ainsi que la protection vis-à-vis des virus destructeurs apportés par des mails est très fragile : les barrières efficaces sont les anti-virus du poste et du serveur ainsi que la politique de sécurité des deux matériels. Il est donc particulièrement important de bloquer le virus sur le poste de travail et lui interdire de se propager sur le serveur.

En conséquence, l'étude fait apparaître la nécessité de durcir le poste de travail en :

- appliquant une politique stricte de contrôle des privilèges ;
- ajoutant un second antivirus protégeant le premier qui ne soit pas construit sur le même mode ;
- forçant la signature des messages sortant ;
- sensibilisant les personnels.

Ainsi pour l'interface avec l'usager ou d'une façon plus large avec l'Internet, on retient la solution décrite figure 14.

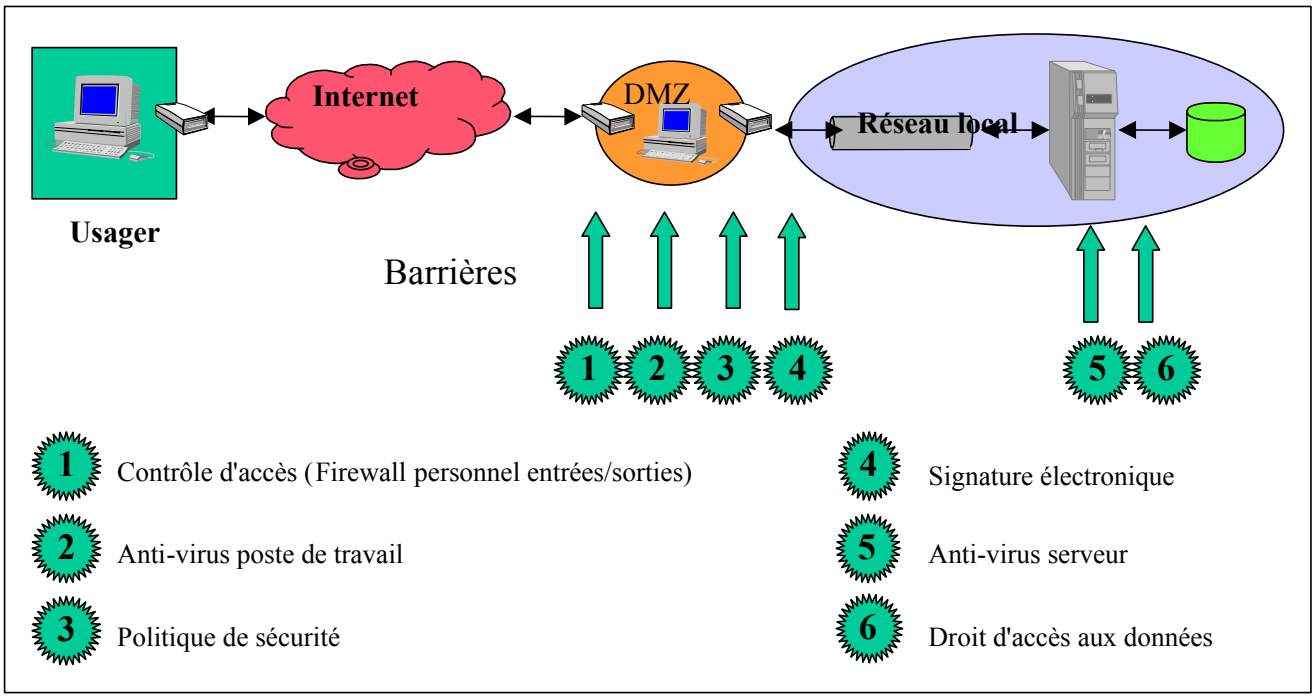


Figure 14 : modélisation de l'interface « Usager/Administration »

6.2.2.3 Hiérarchisation des incidents de sécurité

A partir de l'analyse de ces trois *scénarii* de risques et en particulier de leur impact sur le télé-service, et en la combinant avec la hiérarchie des évènements redoutés (tableau 6), il est possible de placer ces scénarii sur l'échelle de gravité (cf. tableau 7).

Gravité	Code malicieux (Disponibilité)	Faux message (Intégrité)	Cheval de Troie (Confidentialité)
5 – Inacceptable	Serveur indisponible		
4 – Très forte	Poste Internet indisponible		Diffusion de données
3 – Forte	Code malicieux sur poste Internet	Fausse demande	Détection d'une tentative d'accès au serveur
2 - Moyenne	Code malicieux détecté par antivirus du poste Internet	Détection fausse demande au niveau de la siganture	Cheval de Troie détecté par antivirus du poste Internet
1 - Faible	Tentative d'intrusion bloquée par le FireWall	Détection fausse PJ ou expéditeur inconnu	Tentative d'intrusion bloquée par le FireWall

Tableau 7 : hiérarchisation des incidents prévus

Les différentes lignes de défense qui peuvent maintenant être mises en évidence par rapport au bien critique que constitue le serveur de données supportant le télé-service par rapport à la menace retenue sont donc les suivantes :

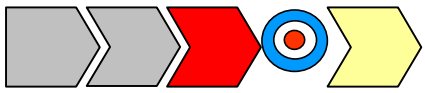
- le FireWall du poste de travail ;
- le poste de travail lui-même (signature électronique, antivirus et politique de défense) ;

- la protection du serveur lui-même (gestion des attributs, antivirus et politique de défense).

Ligne	Code malicieux (Disponibilité)	Faux message (Intégrité)	Cheval de Troie (Confidentialité)
1	Firewall personnel	Contrôle message	Firewall personnel
2	Antivirus du poste	Contrôle signature électronique	Antivirus du poste
3	Politique de sécurité du poste		Signature électronique
4	Antivirus du serveur		Contrôle des droits d'accès au serveur
5			

Tableau 8 : Tableau des lignes de défense

6.2.3 Troisième étape : élaboration de la politique de défense



Cette étape a pour but d'élaborer la politique globale de défense. En effet, il est indispensable de compléter l'étude précédente qui a permis de construire l'architecture générale du système par la définition de la politique de sécurité globale, des procédures à appliquer et de planifier les réactions. C'est donc le problème de la mise en œuvre de la sécurité qui est le thème principal de cette étape.

Pour l'exemple proposé dans ce document, la détermination de la politique de sécurité dans sa totalité n'offre pas d'intérêt. Seules les particularités consécutives à la défense en profondeur sont donc traitées ici :

- coordination des lignes de défense, en particulier en ce qui concerne la détection des incidents de sécurité ;
- planification des réactions aux différents incidents.

6.2.3.1 Détermination de la politique globale et coordonnée

Une fois fixées les différentes barrières, il convient de déterminer les points de contrôle (savoir si la barrière fonctionne ou non) et les points de détection des attaques éventuelles. Cette analyse permettra aussi de choisir les « bons indicateurs » dans la cinquième étape de la méthode.
Le facteur humain ne doit pas être sous estimé. En effet, la détection rapide des incidents de sécurité passe bien souvent par les utilisateurs car il n'est pas toujours possible d'analyser automatiquement et sans délai toute l'information récoltée par les moyens de détection.

La politique de sécurité doit prendre en compte :

- un paramétrage des logiciels permettant de signaler les anomalies aux utilisateurs (en cas de besoin autoriser un flux que le temps nécessaire par exemple pour la mise à jour de l'antivirus) ;

- une formation particulière pour les utilisateurs afin de les sensibiliser aux risques liés à la connexion Internet et en particulier aux virus attachés en pièce jointe des mails qui représentent le risque majeur de cette connexion car le flux des messages est obligatoire ;
- des contrôles de bon fonctionnement de l'ensemble du système (traces, journal de événements, place disque, etc.).:
- un cloisonnement des différents systèmes, chacun disposant de ses propres moyens de protection. La mise en place de moyens de détection particuliers de type IDS ;
- un système de remontée des incidents de sécurité permettant de réagir (voir la partie suivante concernant la planification) et au minimum mettre en garde les utilisateurs en cas de détection d'un nouveau virus par exemple.

6.2.3.2 Planification

La réaction doit être prévue face aux incidents de sécurité prévus.
Dans l'exemple étudié dans ce document, le risque majeur mis en évidence est le manque de disponibilité du télé-service proprement dit qui peut résulter de deux causes principales :

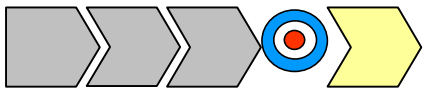
- une panne matérielle ou logicielle (erreur de manipulation par exemple) qui atteindrait le serveur lui-même ou le réseau local et dans une moindre mesure un chaîne de communication ;
- une atteinte à la sécurité du système par une malveillance provenant de l'extérieur (le cas de la malveillance intérieure n'est pas traitée ici et le cas de l'erreur est traitée précédemment).

Dans le cas d'un arrêt du serveur pour une défaillance matérielle, la planification prévoit les différents dépannages possibles :

- démarrage sur le deuxième serveur à partir des disques RAID du premier sans perte de données en trente minutes environ ;
- démarrage sur le deuxième serveur à partir de la sauvegarde effectuée disque à disque avec rattrapage des données provenant des communications et ressaisie des autres informations en une demi-journée ;
- démarrage sur le centre de secours externalisé à partir de la sauvegarde effectuée par cassette avec rattrapage des données provenant par mail (reroutage systématique d'une boîte aux lettres sur une de secours) et ressaisie des autres informations en une journée.

Le secours du réseau est possible par redondance des moyens (deux serveurs et moyen réseau de secours).

6.2.4 Quatrième étape : Qualification



Cette qualification passe par une approche qualitative (respect des principes de la défense en profondeur) et par une approche démonstrative (réaction à des *scénarii* enveloppes et par élément défaillant).

6.2.4.1 approche qualitative

Dans le cadre du cas concret cet aspects démonstration a bien entendu un caractère tout à fait artificiel. C'est pourquoi il est juste rappelé les principes régissant la défense en profondeur pour un système d'information sans que la démonstration soit effectuée

.

Titre	*Nature*
Globalité	**La défense doit être globale, ce qui signifie qu'elle englobe toutes les dimensions du système d'information :** d) aspects organisationnels ; e) aspects techniques ; f) aspects mise en œuvre.
Coordination	**La défense doit être coordonnée, ce qui signifie que les moyens mis en place agissent :** c) grâce à une capacité d'alerte et de diffusion ; d) à la suite d'une corrélation des incidents.
Dynamisme	**La défense doit être dynamique, ce qui signifie que le SI dispose d'une politique de sécurité identifiant :** d) une capacité de réaction ; e) une planification des actions ; f) une échelle de gravité.
Suffisance	**La défense doit être suffisante, ce qui signifie que chaque moyen de protection (organisationnel ou technique) doit bénéficier :** d) d'une protection propre ; e) d'un moyen de détection ; f) de procédures de réaction.
Complétude	**La défense doit être complète, ce qui signifie que :** d) les biens à protéger sont protégés en fonction de leur criticité ; e) que chaque bien est protégé par au minimum trois lignes de défense ; f) le retour d'expérience est formalisé.
Démonstration	**La défense doit être démontrée, ce qui signifie que :** d) la défense est qualifiée ; e) il existe une stratégie d'homologation ; f) l'homologation adhère au cycle de vie du système d'information.

6.2.4.2 approche démonstrative

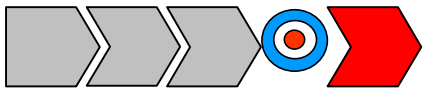
L'approche démonstrative comporte une analyse par scénario enveloppe qui se rapproche de ce qui a été fait à l'étape 2 et par élément défaillant. Dans le cadre de ce cas concret on se contentera de la démonstration par élément défaillant sur un scénario.

Considérons le scénario n°2 présenté précédemment :

- un code malicieux arrivé par messagerie est non détecté par l'antivirus et ce quel qu'en soit la raison ;
- il reste alors comme barrière la politique de sécurité du poste ;
- ainsi que l'antivirus sur le serveur qui est de nature différente que celui qui est sur le poste de travail.

En cas de défaillance de la politique de sécurité, il existe encore une barrière avant l'événement redouté, ce qui est suffisant.

6.2.5 Cinquième étape : Évaluation et audit



Dans le cadre de ce document, il paraît intéressant d'étudier des incidents de sécurité significatifs afin de mettre en évidence la phase dynamique de retour d'expérience et de rétroaction.
Les incidents de sécurité qui vont être étudiés sont :

- une panne de la carte réseau serveur ;
- une panne lecteur DAT.

Une panne de carte réseau du serveur est un **événement inacceptable** s'il n'est pas traité dans le délai requis puisque mettant en cause la disponibilité du télé-service lui même. En attendant le dépannage, l'incident est contourné par application de la procédure prévue de bascule du réseau du serveur principal sur le serveur de secours. Cette procédure entraîne un arrêt de 30 minutes environ pour échanger les rôles des deux serveurs.

Une panne du lecteur DAT est un événement de sécurité non prévu dans l'échelle de gravité. Il met en cause la disponibilité du centre de secours externalisé. En effet, la sécurité du site principal reste intacte car il y a duplication des informations entre les deux serveurs du site principal. Il convient donc d'analyser les moyens prévus de contourner l'événement et d'évaluer les risques potentiels :

- le moyen de secours est prévu sous la forme d'un disque Zip de capacité suffisante (l'extraction est données est faite par vidage des tables et éventuellement compression pour minimiser la place nécessaire au lieu d'une sauvegarde physique de la base comme sur DAT). Il existe donc encore au moins une barrière avant de limiter la disponibilité du centre de secours ;
- le risque potentiel qui est une atteinte de la disponibilité du site principal est couvert par les lignes de défense constituées par la redondance des serveurs et le site de secours. Par rapport à l'événement redouté, il y a donc trois lignes de défense (la redondance des serveurs, le site de secours et le moyen de contournement).

Un virus contenu dans une pièce jointe d'un e-mail met en cause le système de réception des demandes qui a été modélisé précédemment et pour lequel la modélisation a justement fait apparaître une faille dans le scénario. Dans ce paragraphe, on va donc étudier comment dans le cadre du retour d'expérience enrichir la modélisation et les scénarios. Deux aspects sont à considérer :

- le classement de l'événement sur l'échelle de gravité et les mesures correctives issues normalement de la planification ;
- l'étude des risques potentiels et de l'enrichissement des scénarios.

Le classement de l'événement dépend dans un premier temps du moyen de détection de l'incident qui a pu être mis en évidence aux points de contrôle suivants classés par ordre d'importance :

- détection par l'antivirus du poste : ce n'est pas un incident mais un **fonctionnement normal** de l'antivirus ;
- détection par l'utilisateur du poste de travail avant que le virus ai pu faire son effet : c'est un **événement de gravité moyenne** en fonction de la modélisation faite pour les codes malicieux (il reste encore la protection de la communication entre le poste de travail et le serveur puis l'antivirus du serveur et enfin la politique de sécurité du serveur (redondance) et la présence du centre de secours ;
- détection par l'antivirus du serveur : c'est un **événement de gravité très forte** car le système de réception des demandes est inopérant et puisque plus aucune barrière ne va venir protéger le serveur en dehors de la politique de sécurité (si l'on compte le centre de secours, le niveau devient inférieur mais celui-ci correspond à une exigence de disponibilité dégradée en raison de la très faible probabilité d'apparition : sa présence résulte plus de la prise en compte des risques résiduels considérés comme inacceptables).

Cet incident met en évidence l'importance de la formation des utilisateurs, de la mise à jour régulière des applications. Dans ce contexte je retour d'expérience doit être privilégié ainsi que la mise en place d'indicateurs qui permettront de détecter des signaux faibles qui mis en corrélation pourraient prévenir des incidents graves. Ainsi, la détection répétée dans le temps de postes utilisateurs attaqués par des virus doit constituer une alerte pour le système de défense.

Pour chaque nouvelle faiblesse détectée, il convient de la traiter en conservant deux principes à l'esprit :

- ne pas régresser ;
- améliorer si le coût en vaut la peine.

Les autres tâches prévues lors de cette étape ne sont pas spécifiques à la défense en profondeur à l'exception de la partie tableau de bord qui doit intégrer l'échelle de gravité des incidents.

Formulaire de recueil de commentaires

Ce formulaire peut être envoyé à l'adresse suivante :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
conseil.dcssi@sgdn.pm.gouv.fr

Identification de la contribution
Nom et organisme (facultatif) : .....
Adresse électronique : .....
Date : .....

Remarques générales sur le document
Le document répond-il à vos besoins ? Oui ☐ Non ☐

Si oui :

Pensez-vous qu'il puisse être amélioré dans son fond ? Oui ☐ Non ☐

Si oui :

Qu'auriez-vous souhaité y trouver d'autre ?
.....
.....

Quelles parties du document vous paraissent-elles inutiles ou mal adaptées ?
.....
.....

Pensez-vous qu'il puisse être amélioré dans sa forme ? Oui ☐ Non ☐

Si oui :

Dans quel domaine peut-on l'améliorer ?
- lisibilité, compréhension ☐
- présentation ☐
- autre ☐

Précisez vos souhaits quant à la forme :
.....
.....

Si non :

Précisez le domaine pour lequel il ne vous convient pas et définissez ce qui vous aurait convenu :
.....
.....

Quels autres sujets souhaiteriez-vous voir traiter ?

.....
.....

Remarques particulières sur le document

Des commentaires détaillés peuvent être formulés à l'aide du tableau suivant.

"N°" indique un numéro d'ordre.

"Type" est composé de deux lettres :

La première lettre précise la catégorie de remarque :

- O Faute d'orthographe ou de grammaire
- E Manque d'explications ou de clarification d'un point existant
- I Texte incomplet ou manquant
- R Erreur

La seconde lettre précise son caractère :

- m mineur
- M Majeur

"Référence" indique la localisation précise dans le texte (numéro de paragraphe, ligne…).

"Énoncé de la remarque" permet de formaliser le commentaire.

"Solution proposée" permet de soumettre le moyen de résoudre le problème énoncé.

N°	Type	Référence	Énoncé de la remarque	Solution proposée
1				
2				
3				
4				
5				

Merci de votre contribution