Session n°27

De la Sécurité à la Défense des Systèmes d'Information

From Security to Information Systems'Defense

Paul-André PAYS, Denis FARGETTE
Edelweb – Groupe ON-X - France

De la sécurité statique à la défense dynamique

Situation actuelle : la SSI est prise en compte

Les différentes études réalisées pour nos clients montrent que les Directions Générales prennent en compte la Sécurité des Systèmes d'Information (SSI) dans leurs axes stratégiques prioritaires. En effet, faire l'impasse dans ce domaine expose l'organisme à des risques majeurs. Mais les Directions Générales sont fréquemment démunies lorsqu'il s'agit d'organiser, gérer et décider des ressources à mettre en place faute de mesurer le retour sur investissement. En effet, plus la protection est efficace et moins le fait redouté à de chance d'exister. Ceci pourrait conduire à baisser la garde en jugeant l'investissement non rentable.

La nouvelle donne : asymétrie attaque et défense

L'ouverture des entreprises vers l'extérieur, nécessitée par le besoin d'échanger rapidement des informations, entraîne une ouverture des réseaux et donc une vulnérabilité différente. La menace principale pesant sur le système d'information venant à l'esprit des utilisateurs est celle des codes malicieux et non plus celle provenant de personnels de l'entreprise. Or ce changement d'origine a une conséquence majeure qui n'est pas prise en compte dans les esprits : le tiers non identifié a plus de possibilité de nuire que le personnel de l'entreprise dans la mesure où son anonymat le protège. Ceci est à l'origine de l'explosion des incidents qui s'explique par l'augmentation de la possibilité d'attaquer offerte à un plus grand nombre sans moyen de coercition.

Ceci implique qu'il est nécessaire de prendre en compte les faits suivants :

- L'initiative appartient actuellement à l'attaquant qui peut choisir le moment, le lieu et les moyens de son attaque ;
- Le défenseur ne peut même pas utiliser des moyens identiques à ceux de l'attaquant car la légitime défense n'est pas autorisée.

Dans ce type de déséquilibre entre le boulet et la cuirasse, le boulet l'emportera toujours car la protection ne dure que le temps de la franchir ou de la contourner parce qu'il n'y a pas de moyen de faire cesser l'attaque. D'où l'idée sous-jacente qui est de redonner l'initiative au défenseur en amenant l'attaquant sur un terrain défensif préparé à l'avance (Napoléon incitant la coalition à venir dans le piège tendu à Austerlitz).

L'erreur à ne pas commettre : menace externe et interne

Se focaliser sur la menace externe et ignorer la menace interne n'est pas non plus judicieux pour deux raisons :

- La menace interne n'a pas disparu lorsque la menace externe a explosée ;
- Sachant qu'un attaquant ira toujours vers le point le plus faible, il ne faut pas baisser la garde face aux menaces internes, même si elles sont considérées parfois comme secondaires.

Cela veut dire qu'il ne faut pas baser sa défense sur l'origine de la menace mais sur les biens à défendre et assurer cette défense face à toutes les menaces.

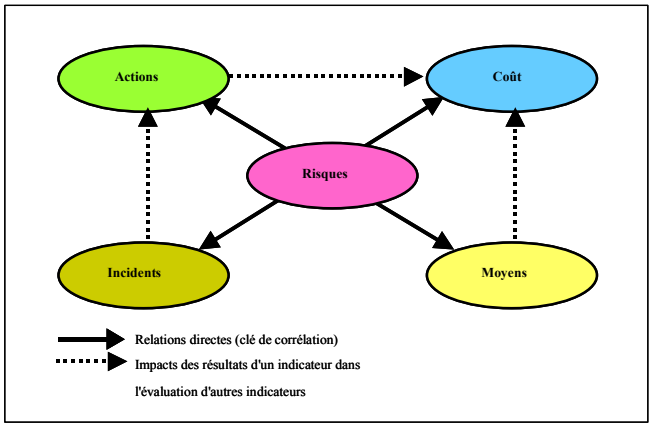
L'architecture de sécurité

Faire face à toutes les menaces nécessite d'optimiser la défense par rapport à l'attaque d'une part mais aussi par rapport aux biens à défendre d'autre part. L'architecture de sécurité est donc construite à partir :

- Des biens à protéger : plus le bien est important et plus il sera protégé ;
- Des risques à couvrir : plus le risque est important et mieux il sera prise en compte.

Les ingrédients d'une bonne défense classique restent valables. Ils sont :

- Les risques pris en compte, acceptables ou acceptées ;
- Les moyens techniques et organisationnels à mettre en œuvre ;
- Les incidents à traiter : la situation ne peut s'apprécier que par de bons renseignements ;
- Les actions à entreprendre : qui reste inactif lorsque le péril est dans la demeure ?
- Le coût global du dispositif, en investissement et en fonctionnement.



De la protection périphérique à la défense en profondeur

Objectif

Mettre en place un moyen de protection unique, aussi sophistiqué soit-il, fait prendre un risque inacceptable car, en cas de défaillance, l'ensemble du système devient sans défense et parfois non opérationnel. A contrario, dans la défense en profondeur, il s'agit en premier lieu de constituer plusieurs lignes de défense composées de différents moyens. Afin que l'ensemble constitué soit plus performant leur simple juxtaposition, leur disposition doit respecter certaines règles d'architecture :

- **Indépendance des lignes de défense** : la compromission d'un moyen ne doit pas donner un avantage à l'attaquant pour en compromettre un autre ; par conséquent une même attaque ne doit pas permettre de compromettre plusieurs lignes de défense (pas de possibilité d'effet château de cartes) ;
- **Coordination des actions** : la défense ne peut pas être isolée ; elle doit envisager le problème posé de manière globale et organiser la coordination des actions dans ce cadre global ;
- **Complétude des moyens** : chaque ligne de défense doit être constituée de moyens (des barrières) permettant de faire face à toutes les menaces retenues.

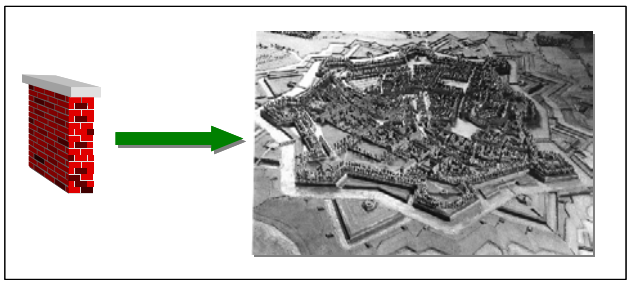
En conséquence, l'utilisation d'une méthode type "**Défense en Profondeur**" appliquée dans les industries à risques en général et nucléaire en particulier, permet de garantir une sécurité bien maîtrisée et à moindres coûts.

Principes

Il s'agit de reprendre l'**initiative** sur l'attaquant en utilisant toute la profondeur du dispositif. On va donc mettre en place plusieurs moyens successifs, de protection mais aussi de détection et de réaction, en respectant les grands principes suivants :

- Un moyen de protection doit être **surveillé** afin qu'il participe au renseignement et permette d'éviter la surprise en décelant l'attaque quand elle se produit et non a posteriori sur ses effets ;
- Un moyen quelconque doit avoir un **rôle à jouer** dans le cadre global de la défense (filtrer, retarder, leurrer, détecter, etc.), en plus de son propre rôle ;
- Une attaque réussie doit **servir la défense** : le caractère malheureusement non absolu de la protection impose d'envisager la réussite d'une attaque ; c'est pourquoi il existe plusieurs lignes de défense qui permettent de faire face à une attaque réussie sur une ligne de défense ; cette dernière doit donc servir la défense en permettant de renforcer les dispositifs suivants ; il convient donc de privilégier le retour d'expériences.

Il faut donc développer une véritable **STRATEGIE** de défense qui utilise toute la profondeur du dispositif créé en organisant le dispositif de sécurité autour des biens à défendre et en fonction des risques encourus.



Les trois volets de la défense en profondeur

La mise en place de plusieurs lignes de défense qui constituent l'architecture sécuritaire adaptée aux systèmes constituant les biens à protéger en fonction de leur criticité, doit s'effectuer en recherchant, en plus, la complétude des types des moyens à mettre en œuvre en couvrant trois volets habituels :

- **Humain** : l'origine des menaces, l'utilisation du système, la détection des incidents et les mesures correctrices mettent très souvent en jeu le facteur humain ; celui-ci est à prendre en compte d'autant plus qu'une partie non négligeable reposera sur lui ; toutefois, une mesure de défense humaine devra être appuyée par une mesure d'un des deux autres types ;
- **Procédural** : l'organisation de la défense doit s'appuyer sur des procédures pour ne pas laisser de place à l'improvisation ;
- **Technique** : s'appuyant sur la technique, la défense doit en utiliser les atouts sans en négliger les faiblesses ; les moyens techniques devront donc s'accompagner de mesures des deux autres types.

Approches méthodologiques

Outre l'utilisation d'une méthode d'analyse de risque (EBIOS par exemple), il convient de mettre en œuvre une démarche itérative en combinant plusieurs approches :

- Déterministe et Probabiliste ;
- **Inductive**[1] (à partir des menaces) et **Déductive**[2] (à partir des biens à protéger).

Dans le cadre de la validation d'une architecture par rapport à un scénario d'attaque, il sera judicieux d'utiliser la méthode du **composant défaillant** :

- On considère que l'attaquant à réussi à franchir la première ligne de défense ;
- On prend comme hypothèse qu'un élément de protection, au hasard, est défaillant pour une raison diverse (erreur humaine, vulnérabilité inconnue, patch non appliqué, etc.) ;
- On vérifie que les moyens de protection restants sont suffisants.

L'utilisation d'une telle méthode oblige à prévoir la redondance des moyens (au minimum trois et indépendants, si possible de type différent) à partir du moment ou le bien présente une certaine criticité (en dessous duquel le risque de double défaillance peut être considéré comme acceptable). L'avantage d'utiliser la profondeur du dispositif pour disposer les biens en fonction de la criticité permet d'adapter la profondeur du dispositif à la criticité.

Une telle étude, par scénario, n'est effectuée que pour les cas « **enveloppes** » : si une vitrine résiste à une voiture bélier, il y a de forte chance qu'elle résiste au jet de pavé. On retiendra donc en premier les scénarios les plus contraignants et on vérifiera ensuite que les autres sont bien déjà couverts.

Les ingrédients d'une bonne défense en profondeur

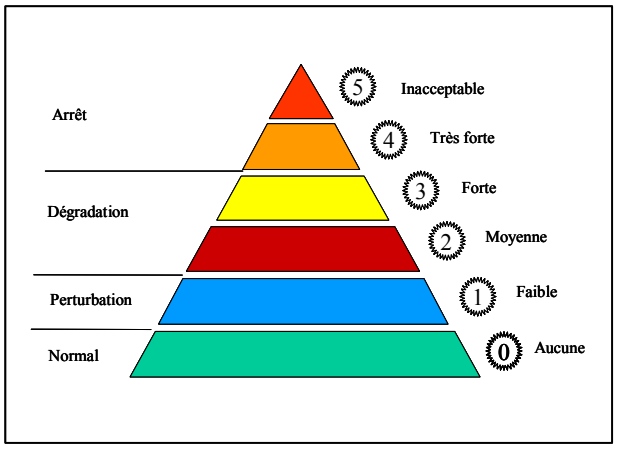
Une fois l'architecture de sécurité validée et mise en place, il est nécessaire de la soutenir par des mesures visant à assurer son bon fonctionnement :

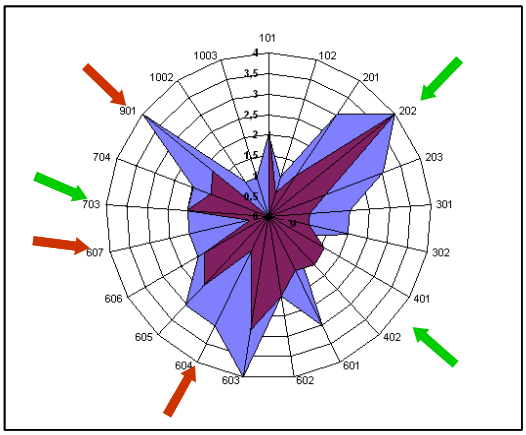
- Une organisation de type « **Veille, Alerte et Réponse** » ;
- Une gestion des incidents de sécurité basée sur une **échelle de gravité** permettant d'établir des priorités ; la gravité d'un incident dépendant de la criticité du bien menacé et de l'importance des défenses restantes ;
- un système de gestion du renseignement :
  - sur l'environnement (fonction veille),
  - sur le système (la détection),
  - sur les incidents (organisation du retour d'expériences)
- La planification des réactions : l'improvisation ne doit pas être de mise mais les incidents et les mesures correctrices prévues ;
- Un tableau de bord de pilotage.

1 Les méthodes d'analyse inductives sont fondées sur une analyse descendante de la séquence accidentelle (des causes vers les conséquences).

2 Les méthodes d'analyse déductives (arbre de défaillance) s'appuient sur une analyse ascendante de la séquence accidentelle (des conséquences vers les causes).

Les schémas ci-dessous montrent une échelle de gravité fondée sur les effets, réels ou potentiels permettant d'apprécier une situation de risques et une sortie d'un l'outil tel qu'Edelcheck, permettant de visualiser la situation vis-à-vis de la sécurité.





Toutes ces mesures visent à organiser la **lutte défensive**. Les aspects offensifs n'étant pas autorisés par la loi, la contre-attaque est le seul moyen à exclure dans le cadre de la défense en profondeur.

Vers une meilleure agilité des entreprises

Le problème posé

Personne ne met en doute les principes fondamentaux suivants :

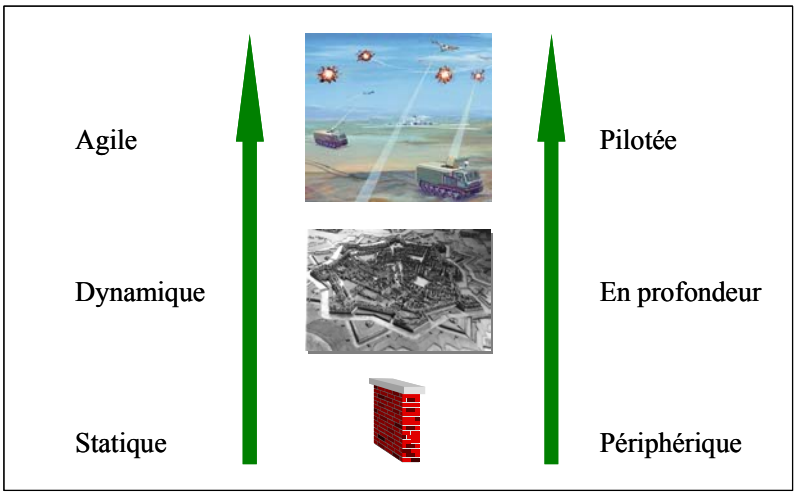
- La sécurité est incontournable ;
- Elle doit protéger des risques inacceptables ;
- Le coût doit être optimisé.

L'ambition de la défense en profondeur est de satisfaire ces trois fondamentaux en obtenant un très haut niveau de sécurité, quand cela est nécessaire, par la mise en œuvre d'une architecture de sécurité et une organisation qui permettent d'obtenir un niveau global de sécurité supérieur par synergie entre les moyens. Le problème posé est maintenant de savoir si ce système est entièrement abouti ou s'il doit lui-même se perfectionner.

Evolution souhaitable

Il a été démontré précédemment que la défense devait être organisée dans la profondeur, être globale et coordonnée. De même, il a été mis en évidence qu'elle devait s'appuyer sur une organisation adaptée et en particulier que l'aspect dynamique nécessitant de remplir les missions de veille, action et réaction. Mais cela n'est pas suffisant : l'agilité, au sens anglo-saxon de la traduction servile, doit être au rendez-vous car les systèmes ne sont pas figés.

La nécessaire flexibilité et les aspects reconfiguration automatique doivent être pris en compte. Cela nécessite des mesures de management : **la défense en profondeur du SI doit être pilotée**.



Toutefois, le **pragmatisme** doit prévaloir, ce qui n'empêche pas d'utiliser une bonne méthode.