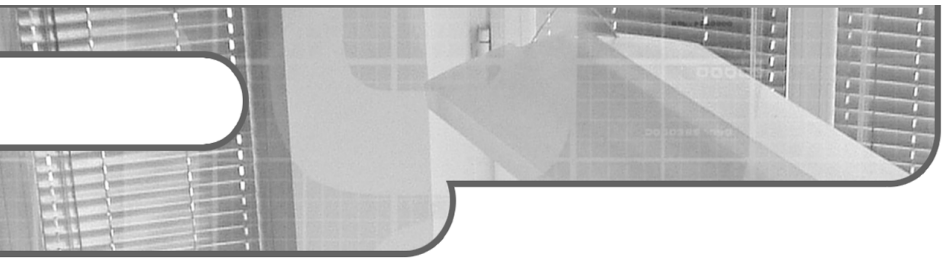


Chapitre 5
Sécurité et virtualisation

1. Rappel sur les grands principes de sécurité

Avant d'aborder la sécurité de la virtualisation en particulier, il est bon de faire quelques rappels sur la sécurité des systèmes d'information.

La sécurité des systèmes d'information repose sur ce qui est appelé le capital informationnel. Il représente la somme des informations de l'entreprise, par exemple, la clientèle, la concurrence, le savoir-faire, le cercle de ses actionnaires, les méthodes de fabrication, les brevets, etc. Ce sont des actifs matériels et surtout immatériels dont il est difficile d'imaginer le coût réel en cas de perte, mais il est certain que l'atteinte, sous quelque forme que ce soit, à ce dernier peut rapidement conduire l'entreprise à fermer ses portes.

"L'immatériel est au cœur de la stratégie des entreprises qui créent de la valeur : résultat le plus frappant de notre étude, 60 % de la valeur des principales entreprises européennes s'explique par leur capital immatériel" selon le cabinet d'étude Ernst & Young.

La sécurité des systèmes d'information consiste à :

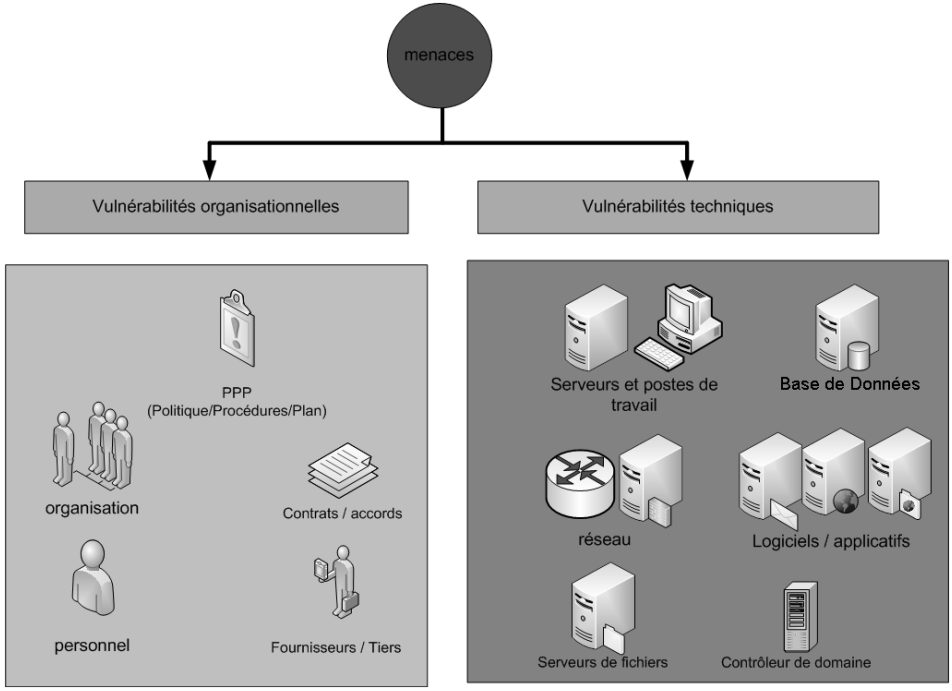
- Garantir que le système d'information est accessible au moment voulu par les personnes autorisées (**D**isponibilité).
- Garantir que seules les personnes autorisées ont accès au système d'information de l'entreprise (**C**onfidentialité).
- Garantir que les éléments considérés du système d'information sont exacts et complets (**I**ntégrité).
- Garantir que les accès et tentatives d'accès aux éléments considérés du système d'information sont tracés et que ces traces sont conservées et exploitables (**T**raçabilité).

Vous retrouverez souvent la notion de DICT avec des experts sécurité au cours de divers projets.

Remarque

Les organismes américains ne considèrent pas la traçabilité comme un critère de sécurité. Ils proposent un modèle dit CIA (Confidentiality - Integrity - Availability).

Des menaces diverses et variées pesent sur les systèmes d'information. Pour peu qu'il existe des vulnérabilités techniques ou organisationnelles dans une entreprise, ces menaces seront capables de les exploiter. À partir du moment où la menace et la vulnérabilité sont présentes, il y a alors un risque.



Afin de vérifier que le risque est réel et tangible, les experts sécurité effectuent ce qui est communément appelé une analyse de risques. Sans trop rentrer dans les détails, l'analyse de risque permet de confronter :

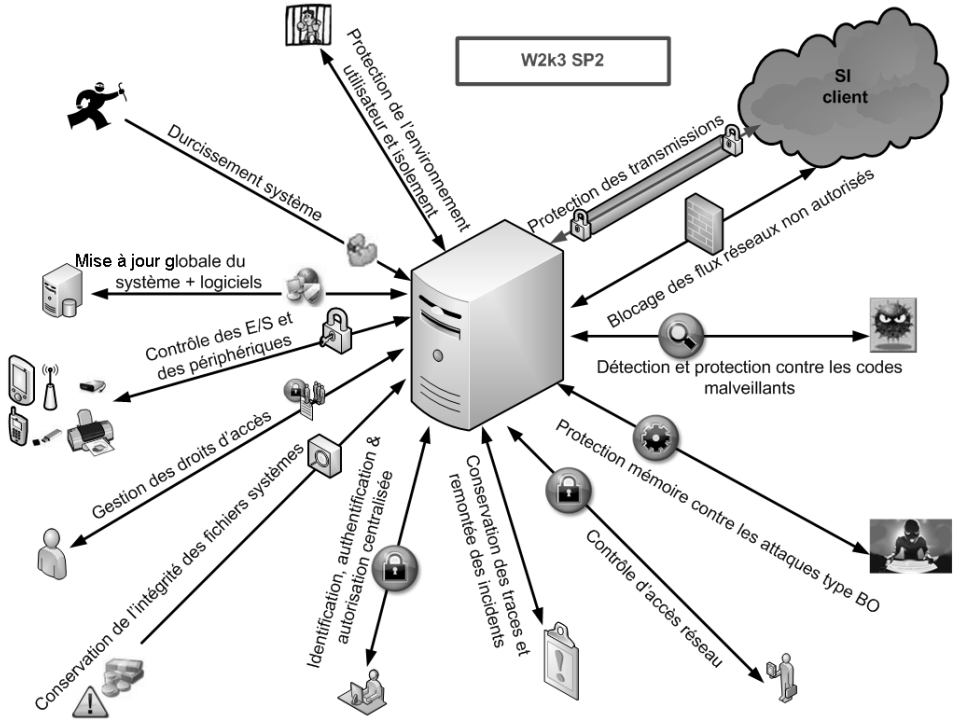
- la probabilité d'apparition d'une menace exploitant une vulnérabilité.
- l'impact généré par cette exploitation.

Une matrice est déduite pour chaque risque en proposant une échelle de valeurs.

Il faut s'imaginer que le connaître parfaitement n'est pas simple ! Combien de personnes pensent aujourd'hui que l'avion n'est pas un moyen très sûr de transport alors que statistiquement, c'est un des plus fiables. En réalité, c'est le transport en voiture qui comporte le plus de dangers. Pour autant, les usagers n'ont pas l'impression de prendre un risque à chaque fois qu'ils conduisent. Avoir ainsi une vision objective demande bien souvent un avis extérieur.

Les menaces sont bien souvent négligées faute de temps et de moyens. Pourtant, les systèmes d'information possèdent un nombre incalculable de points d'entrées. Un simple serveur doit être protégé à tous les niveaux afin de garantir le principe DICT.

En voici un exemple :



2. Challenge N° 1 : Assurer la disponibilité des infrastructures virtuelles

Comme nous l'avons vu, la **D**isponibilité est un élément essentiel de la sécurité des systèmes d'information. Assurer celle-ci dans des environnements virtuels devient donc primordial. Il existe de nombreuses possibilités d'assurer la disponibilité d'un ensemble de services, cependant il existe également un grand nombre de menaces pouvant porter atteinte à cette disponibilité. Sachant comment se définit une infrastructure virtuelle (voir chapitre précédent), il est nécessaire d'assurer au minimum la disponibilité des éléments suivants :

- La haute disponibilité des serveurs.
- La haute disponibilité du stockage.
- La haute disponibilité des machines virtuelles et des applications.
- La haute disponibilité réseau.
- La supervision de l'ensemble de l'infrastructure.

2.1 La haute disponibilité des serveurs

La haute disponibilité des serveurs ou « hôtes » est un élément déterminant afin de garantir que les machines virtuelles qui s'y trouvent héritent d'une haute disponibilité également. Les serveurs doivent bénéficier de mécanismes permettant de pallier plus ou moins des pannes hardware.
Par exemple :

- **Ventilation redondante**. En cas de panne d'un ventilateur, un autre doit pouvoir prendre le relais afin de continuer les opérations.
- **Alimentation redondante**. Aujourd'hui, les serveurs ont souvent au minimum 2 alimentations. Il est nécessaire qu'une d'entre elles défaillante n'endommage pas les autres. Certains constructeurs n'isolent pas suffisamment les alimentations les unes des autres ce qui conduit à la panne totale de toutes les alimentations en cas de problèmes.

- **CPU redondants**. Les constructeurs proposent que les CPU soient isolés les uns des autres pour éviter l'arrêt d'activités, en cas de panne ; malheureusement, au cours des tests élaborés dans nos laboratoires, il s'est avéré que VMware ESX ne supporte pas l'arrêt d'un processeur physique. Le serveur plantera immédiatement.
- **Mémoire redondante**. Les barrettes de mémoire doivent également être indépendantes. Il se peut que certaines deviennent défaillantes. Plus le nombre est important, plus le risque de défaillance est grand. C'est pourquoi il importe que la perte d'une barrette mémoire n'entraîne pas l'arrêt total des activités du serveur. Au niveau test, il s'avère que suivant les constructeurs, les résultats sont différents. VMware semble plutôt bien gérer la perte de mémoire physique tant que le constructeur gère correctement au niveau matériel l'exception générée. Il est préférable de s'assurer également que les barrettes mémoires proviennent du même constructeur et possèdent les mêmes références, ce qui évite des comportements erratiques pouvant conduire à un PSOD (*Purple Screen Of Death*).
- **Carte réseau redondante**. Les serveurs doivent posséder suffisamment de cartes réseau afin de pouvoir pallier la perte de connectivité sur l'une d'entre elles. Généralement, ce type de panne est bien supporté (ex : VMware avec le NIC Teaming).

■ Remarque

Sous VMware, le PSOD est équivalent au BSOD (Blue Screen Of Death) de Microsoft Windows.