



Marc-Eric Trioullier est co-auteur de l'ouvrage

« Sécurité des architectures Web » paru chez Dunod (ISBN : 2100073540)

La politique de sécurité d'une entreprise est classiquement définie comme « l'ensemble des lois, règlements et pratiques qui régissent la façon de gérer, protéger et diffuser les biens, en particulier les informations sensibles, au sein de l'organisation ». Elle est définie par le Responsable de la Sécurité des Systèmes d'Information (RSSI) ou ses équipes.

(ITSEC, Commission européenne, juin 1991 § 2.10).

« Une politique de sécurité définit logiquement des normes au niveau des développements, de l'architecture et de l'infrastructure. Elle doit de plus instaurer des règles organisationnelles (des mécanismes de surveillance de l'architecture, des procédures d'administration, etc.). Elle doit enfin mettre en place une norme d'analyse des risques avec des listes de menaces, des probabilités associées, des règles de criticité, des mesures de prévention et les conséquences induites en cas de réalisation.

Les utilisateurs et les équipes techniques (développeur, exploitant) doivent être sensibilisés à la politique de sécurité.

La politique de sécurité est donc un savant mélange entre des règles au niveau de l'application, au niveau de la machine et au niveau du réseau.

Elle est validée régulièrement par des phases d'audit de conformité. »

Marc-éric TRIOULLIER
Consultant sécurité

Auditer la sécurité du système d'information d'une entreprise

Définir une politique de sécurité au sein d'une entreprise n'est pas une chose aisée. D'ailleurs toutes les entreprises l'ont fait (selon le CLUSIF en 2005, 44 % des entreprises françaises n'en ont pas). Toutefois, les PME et les grandes entreprises semblent avoir pris la mesure de ce problème car, à partir de 500 employés, cette politique est définie à 54 %, et ce chiffre passe à 72% pour les entreprises de plus de 1000 employés.

Souvent reléguée aux équipes d'exploitation pour d'autres tâches, la politique de sécurité devrait être définie par un véritable Responsable de la Sécurité des Systèmes d'Information (RSSI). Elle doit répondre aux objectifs suivants :

- Sensibiliser et informer les employés de l'entreprise sur les risques encourus en terme de sécurité par l'entreprise et ses projets.
- Fournir les moyens techniques et organisationnels pour se prémunir de ces risques et garantir la protection du système d'information.
- Élaborer un cadre général ou une assistance permettant une mise en œuvre opérationnelle et concrète de la politique de sécurité au sein des projets.

La politique de sécurité a pour objectif d'assurer l'intégrité, la cohérence et la confidentialité des données et des traitements du système d'information de l'entreprise. Elle intervient de manière transversale, d'un point de vue organisationnel et technique, en synergie avec les différentes directions métiers, les équipes projets fonctionnelles ou techniques.

La validation d'une politique de sécurité se fait au travers d'un audit de sécurité du système d'information. L'audit est une mission d'évaluation de conformité par rapport à un ensemble de règles de sécurité.

Cette évaluation doit se baser sur une grille d'analyse où chaque caractéristique à valider, doit être aisément qualifiable (mesurable) et contrôlable.

Au final, la mission d'audit dresse un bilan, qui mesure le niveau d'application de règles sur le système par rapport aux règles qui devraient être effectivement appliquées.

Adossé à cet état des lieux un schéma directeur doit être réalisé selon les principes d'urbanisation qui permet d'apporter une vue prospective et efficace de l'évolution du système d'information dans ses aspects sécurité.

Cet audit peut aussi servir de déclencheur pour initier une politique de sécurité transversale et prendre pleinement conscience des risques encourus par de l'entreprise.

Notre offre de conseil – Audit de sécurité d'un système d'information – s'adresse aux acteurs métiers et aux Direction des Systèmes d'Information souhaitant évaluer la conformité sécuritaire du SI de leur entreprise et définir un schéma directeur

