Avant-propos

Not everything that can be counted counts,
and not everything that counts can be counted.
(Albert Einstein)

La pérennité de toute entreprise passe, entre autre, par une disponibilité permanente de son système d'information. L'information nécessaire au bon fonctionnement de l'entreprise englobe aussi bien les données stratégiques que les données de tous les jours. Le système d'information doit donc être vu comme un ensemble, qui inclut aussi bien l'information elle-même que les systèmes et réseaux nécessaires à sa mise en œuvre.

La continuité de l'activité de l'entreprise appelle celle de son système d'information. Cette continuité ne peut être assurée que par la mise en place de moyens de protection apportant un niveau de sécurité adapté aux enjeux spécifiques de l'entreprise. Ces derniers peuvent varier d'une entreprise à une autre, mais la mise en place de la protection des systèmes d'information répond à des critères communs.

Une information sans système d'information pour la mettre en œuvre est vaine, et un système d'information coupé de ses utilisateurs sans objet. La sécurité des réseaux est donc devenue l'un des éléments clés de la continuité des systèmes d'information de l'entreprise, quelles que soient son activité, sa taille ou sa répartition géographique.

Notre vision du système d'information d'une entreprise doit considérer la composante réseau comme un élément spécifique fondamental de sa sécurité. Comme toute composante critique, le réseau doit faire l'objet d'une politique de sécurité tenant compte de tous les besoins d'accès au réseau d'entreprise (accès distants, commerce électronique, interconnexion avec des tierces parties, etc.).

Fondées sur cette politique de sécurité, des solutions techniques (pare-feu, routage réseau, authentification, chiffrement, etc.) peuvent être déployées de manière cohérente afin de garantir la sécurité. Des tableaux de bord de la sécurité réseau sont ensuite définis pour visualiser et détecter toute modification du niveau de sécurité du réseau d'entreprise.

Le titre de cet ouvrage reflète donc la continuité dans l'effort de sécurisation, culminant dans l'établissement de tableaux de bord.

Reliant toutes les ressources de l'entreprise, le réseau doit assurer les domaines de sécurité suivants :

- sécurité des réseaux, afin de garantir la disponibilité et la qualité de service des connexions du système d'information ;
- sécurité des systèmes d'exploitation, afin de garantir l'intégrité et la fiabilité du système d'information ;
- sécurité des applications, afin de garantir le développement de code sûr et résistant aux attaques ;
- sécurité des accès, afin de garantir les accès aux ressources de l'entreprise par une liste définie d'utilisateurs avec des droits d'accès spécifiés ;
- sécurité des informations afin de garantir la confidentialité, l'invulnérabilité (falsification, plagiat, destruction, etc.) et la non-volatilité (modification d'un logiciel, modification d'une image, etc.) des informations numériques.

Objectifs de l'ouvrage

Cet ouvrage couvre toutes les étapes nécessaires à la sécurisation d'un réseau d'entreprise. Ces étapes décrivent une démarche générique permettant d'appréhender et de construire une politique de sécurité réseau mais aussi de choisir des solutions techniques adaptées à ses besoins de sécurité. Elles permettent également de mettre en place des contrôles de sécurité à la fois pour vérifier que la politique de sécurité réseau est appliquée et pour établir des tableaux de bord de la sécurité réseau.

Ces étapes de sécurité constituent non seulement le fil conducteur du livre, mais aussi celui d'une démarche de sécurité réseau. Elles sont indissociables les unes des autres (politique de sécurité, solution technique, contrôle de sécurité, tableau de bord de sécurité) et apportent ensemble une garantie de la cohérence et de la consistance de la politique de sécurité réseau mise en œuvre.

La sécurisation est un processus permanent, qui doit tenir compte des évolutions des services afin d'adapter et de contrôler ses objectifs aux besoins.

Organisation de l'ouvrage

Cet ouvrage est destiné en premier lieu aux professionnels de la sécurité et aux responsables des systèmes d'information des entreprises. Il est également conçu comme un cours susceptible d'intéresser étudiants et enseignants. Une étude de cas générique et modulaire reprend tous les principes et toutes les techniques présentés dans l'ouvrage.

Le livre est organisé en sept parties :

- La partie I présente les différentes catégories d'attaques qui peuvent être lancées sur un réseau d'entreprise.
- La partie II introduit les principes de base à prendre en compte afin de définir une politique de sécurité réseau permettant de faire face aux menaces et à leurs conséquences

sur le réseau d'entreprise. Cette partie détaille aussi les méthodes d'évaluation de la sécurité existante.

- La partie III détaille les techniques de protection du réseau s'appliquant tant au niveau des équipements physiques qu'à celui des protocoles de routage.
- La partie IV présente les techniques de protection des services réseau couvrant l'accès et en décrivant les différentes topologies de service pouvant être mises en œuvre.
- La partie V introduit les techniques de contrôle permettant de vérifier l'application de la politique de sécurité réseau.
- La partie VI décrit les techniques de supervision de la sécurité ainsi que la façon d'établir des tableaux de bord de sécurité.
- La partie VII présente un ensemble d'outils maison et détaille une étude de cas décrivant l'évolution des besoins en sécurité et les solutions techniques possibles pour une PME se transformant peu à peu en une multinationale avec de fortes contraintes de sécurité. Cette partie est en libre téléchargement depuis le site Internet des Éditions Eyrolles.

Cet ouvrage décrit une démarche générique de sécurité à suivre pour mettre en œuvre une politique de sécurité réseau et fournit de nombreux exemples de tableaux de bord de sécurité réseau permettant de définir des indicateurs de la politique de sécurité mise en œuvre.

Les différentes versions de l'ouvrage

- 2003 : parution de la première édition de *Tableaux de bord de la sécurité réseau* (C. Llorens, L. Levier).
- 2006 : la deuxième édition de l'ouvrage introduit une nouvelle partie dédiée aux outils maison utilisés dans notre étude cas (arrivée du co-auteur D. Valois).
- 2010 : la troisième version couvre des domaines plus larges, tels que la sécurité des systèmes, des applications, de la zone d'administration, etc., et introduit une partie consacrée à la supervision de la sécurité (arrivée du co-auteur B. Morin).