mai
2005

GUIDE SSI
Bâtir une politique de sécurité

Fiche 1

MEDEF

Accompagner

Une politique de sécurité est un ensemble, formalisé dans un document applicable, d'éléments stratégiques, de directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du (des) système(s) d'information de l'organisme. Bâtir une politique de sécurité, c'est un projet à long terme visant à mettre en œuvre une sécurité adaptée aux usages, économiquement viable et conforme à la législation en vigueur.

Le plus souvent, il s'agira de bâtir une politique de sécurité prenant en compte les risques aussi bien internes qu'externes, ainsi que la typologie du système d'information, la sécurité devant prendre en compte la spécificité de chaque type de communication. Avant tout, il conviendra de répondre à ces trois questions :

- Que dois-je protéger en priorité ? Quel est mon patrimoine informationnel ?

- Quels sont les risques que je cours (externes, internes)?

- Quels sont les facteurs aggravants de risque ?

Que dois-je protéger ? Quel est mon patrimoine informationnel ?

Un Etat des lieux pour bâtir une politique de sécurité adaptée aux usages .Du réseau au contenu, en passant par les systèmes et les applications, la segmentation de la sécurité en fonction des usages, des risques potentiels et des composantes impliquées est la seule démarche qui garantisse la sécurité globale pour l'entreprise.

Pour bâtir une politique de sécurité adaptée aux besoins et usages, il faut chronologiquement :

➔ Identifier les biens à protéger

- **Les biens matériels et des logiciels** : Les serveurs et les postes de travail (fixes et nomades), les équipements d'interconnexions (routeurs, commutateurs, modems), leur localisation ou leur titulaire, le type et la version des logiciels installés.

- **Les données sensibles** de l'entreprise (procédés de fabrication, codes sources, données commerciales et administratives,…)

- **Les services et applications** : Applications métiers internes et externes communiquant avec le monde extérieur (fournisseurs, site de commerce électronique), applications de gestion. Attention aux services et applications obsolètes et non maintenues mais toujours résidentes.

➔ **Découvrir les réseaux**. Il s'agit de découvrir les interactions des différents matériels/logiciels (en-

tre eux et avec le monde extérieur), d'identifier les vulnérabilités pouvant les affecter, d'identifier les applications qui résident dans les systèmes et qui transitent par le réseau. Cette phase permet en outre, de comparer l'existant réel avec l'inventaire précédent.

- Etape 1 : Lister les moyens d'accès au « réseau de l'entreprise » depuis « le monde extérieur ». Un point d'entrée unique (passerelle d'accès Internet) est plus facile à sécuriser mais il convient de porter une attention particulière aux diverses connexions établies temporairement en dehors de l'entreprise avec des équipements nomades, aux modems individuels (permettant la connexion directe à Internet en contournant les sécurités du point d'entrée principal) et aux réseaux locaux sans fils dont le périmètre d'écoute dépasse l'enceinte physique de l'entreprise.

- Etape 2 : Détecter les vulnérabilités des systèmes et applications (outil ou service en ligne – voir fiche 6).

- Etape 3 : Identifier les flux applicatifs circulant à l'intérieur du réseau de l'entreprise (applications métiers, gestion des stocks, paie…) et ceux communiquant avec le monde extérieur (messagerie, commerce en ligne, échanges partenaires,…). Cette étape permettra de découvrir l'usage des réseaux (internes ou externes) et de leur bande passante. Elle permettra aussi de découvrir comment les collaborateurs de l'entreprise utilisent les ressources mises à leur disposition pour remplir leurs tâches. Les outils d'analyse de flux utilisés seront par ailleurs très utiles pour détecter les applications (parfois non souhaitées) et juger de leur importance par le volume de leurs flux. Ils permettront aussi de faire le point sur la politique d'accès aux données (connexion et mot de passe par exemple) et de réfléchir à la mise en œuvre de moyens plus sophistiqués (authentification forte, chiffrement) pour les données les plus sensibles.

Quels sont les risques externes?

■ **Attaques non ciblées**. Toutes les entreprises sont concernées par la propagation des virus (ou vers) ou les attaques distribuées (déni de service) dont l'objectif est la prise de contrôle d'une machine pour l'utiliser à une attaque d'un site tiers.

■ **Attaques ciblées**. La probabilité de risque physique (vol ou destruction de matériel) et de risque logique (attaques distantes et ciblées pour veille, vol ou destruction) augmente avec la visibilité et les facteurs aggravants.

Quels sont les risques internes?

La sécurité doit impérativement impliquer tous les collaborateurs qu'il faut former à la mise en œuvre des politiques de sécurité, car les plus grandes menaces pour la sécurité informatique des entreprises viennent des utilisateurs eux-mêmes.

Quels sont les facteurs aggravants de risque ?

■ **Nomadisme et nouvelles technologies** : Postes et équipements nomades (assistants numériques de poche, téléphones évolués portables et autres PDA/Smart phones, réseaux sans fil)

■ **Infrastructures, services et applications mal protégées** : Serveurs et postes de travail non mis à jour (« non patchés ») et donc vulnérables, site web mal conçu, messagerie non protégée.

■ **Plan de sauvegarde inexistant ou incomplet**

L'approche des politiques de sécurité par segmentation.

La connaissance acquise au cours de ces phases de découverte et d'inventaire permettra d'élaborer une politique de sécurité pour déployer les moyens de protection adaptés aux usages. La segmentation est la base des politiques de sécurité :

■ **Réseau**. La sécurité commence avec le contrôle d'accès appliquant une politique de sécurité personnalisée par site et par groupe de population, pouvant se compléter par une authentification simple ou renforcée.

■ **Système**. Les systèmes peuvent être hétérogènes ce qui complexifie leur gestion et leur mise à jour. Par ailleurs, la publication régulière de nouvelles vulnérabilités crée un risque permanent.

■ **Application**. Une application Web ouverte, par nature, au monde extérieur présente plus de risques potentiels qu'une application propriétaire (paie, comptabilité, gestion stock, client..) utilisée par une population limitée.

■ **Contenu**. La protection du contenu (fichier de données, image ou texte, programme exécutable, pièce jointe...) doit tenir compte de sa dangerosité potentielle, de sa confidentialité pour l'entreprise et des obligations légales.

Comme il est difficile de tout prévoir, faute de temps et de moyens, il conviendra au minimum de prévoir des sauvegardes et peut-être de considérer une couverture complémentaire pour les dommages résultant des attaques. Souscrire une assurance informatique impose de toutes façons un niveau de sécurité minimum.

La mise en œuvre

Plusieurs possibilités :

➔ **Mise en œuvre par des ressources internes** avec acquisition des outils,

➔ **Sous-traitance** à un prestataire de service informatique qui pourra utiliser ses propres outils. Il faudra prévoir de le faire revenir régulièrement car les menaces évoluent sans cesse.

➔ **Utilisation des services mutualisés à distance** par des MSSP (« Managed Security Service Providers ») pour les tests de vulnérabilités, la découverte de vos flux applicatifs, la gestion des moyens de protection (équipements filtrants et antivirus) et la gestion des identifications/authentifications.