Fiche 9

Gérer et maintenir la politique de sécurité

Les risques liés au changement

Les systèmes d'information évoluent périodiquement. Les changements, souhaités ou subis, peuvent avoir des conséquences sur le niveau minimum de sécurité défini lors de la mise en œuvre de la politique de sécurité :

Changement de responsabilité des collaborateurs
Leur niveau d'accès aux données et applications critiques doit être géré en permanence.

Embauches
Le niveau d'accès aux données et applications critiques des nouveaux collaborateurs doit être défini (voir Charte).

Départs
Supprimer connexions et mots de passe des collaborateurs quittant l'entreprise.

Évolutions
Tester les nouvelles applications, nouveaux postes de travail, nouveaux réseaux, nouvelle version du site web, …

Renouvellement des menaces
Le système d'information doit faire face à des menaces externes sans cesse renouvelées (nouveaux virus ou vers, nouvelles vulnérabilités…).

Une politique de sécurité n'est valable dans le temps que si elle est évaluée régulièrement contre les nouvelles menaces et les changements d'organisation ou de périmètre de l'entreprise.

Maintenance minimum

Mise à jour périodique de la Charte d'Utilisation
L'entreprise se dote de nouveaux moyens de communication, déploie de nouvelles applications, les droits et devoirs des collaborateurs évoluent et doivent impliquer une mise à jour de la Charte.

Gestion des niveaux d'accès
Vous avez choisi un moyen d'authentification (voir fiche 4). Il vous faudra impérativement en assurer un bon suivi. Cette tâche est relativement complexe ; elle dépend des moyens utilisés, des effectifs et du nombre de sites de l'entreprise. Les outils d'administration permettent d'assurer la pérennité des moyens déployés.

Gestion des moyens de protection minimums
Certains moyens de protection sont aujourd'hui incontournables pour une sécurité minimum. Il ne suffit pas de les installer ou de les configurer une fois pour toutes, encore faut-t-il veiller à ce qu'ils soient activés et mis à jour en permanence.

Valider régulièrement la configuration de vos pare-feu
- Pour être efficaces, vos pare-feu ont été configurés au moment de leur mise en place en ligne avec vos politiques de sécurité (voir fiche 1).
- Pour rester efficaces, leur configuration doit être testée périodiquement et les alertes générées contrôlées et corrélées.
- Pour mieux maîtriser ces changements et affiner la configuration de vos firewalls, vous devez connaître les flux applicatifs. Cette connaissance vous permettra en outre de savoir ce que les utilisateurs font des moyens de communication que vous mettez à leur disposition.

Valider les mises à jour correctives régulièrement et tester périodiquement les vulnérabilités de tous les composants logiciels de votre système d'information.

Veiller à l'activation permanente de vos antivirus (et éventuellement anti-spam, anti-spyware). Les antivirus peuvent être désactivés par mégarde ou volontairement, en particulier lorsqu'ils sont déployés sur chaque poste de travail.

Gestion des procédures de sauvegarde
Le contenu de la sauvegarde peut évoluer avec le temps avec l'ajout de nouvelles applications ou de données. Cette contrainte doit être prise en compte et il faut veiller à la complétude des sauvegardes régulièrement.

Moyens

La maintenance (des pare-feu, VPN, antivirus, mises à jour correctives, moyens d'authentification, sauvegarde, gestion des flux applicatifs) peut être réalisée :
- Par les ressources propres de l'entreprise et/ou avec sous-traitance à une société de service qui délèguera du personnel qualifié sur votre site (voir contrats fiche 10).
- Par un prestataire de services ou un Opérateur (appelé MSSP – Managed Security Service Provider) qui gère la sécurité à distance à partir d'un centre mutualisé (SOC - Security Operation Centre) :
  - Gestion du trafic en temps réel 24/24 et 7/7 ;
  - Gestion des incidents en temps réel et conseils d'intervention ;
  - Mise à jour permanente des éléments de protection et des mises à jour correctives ;
  - Gestion des « logs » (archives des anomalies) ;
  - Reconnaissance et enregistrement des attaques ;
  - Rapports journaliers et assistance sur leur interprétation à la demande ;
  - Garantie de service et procédures de support ;
  - Corrélation et interprétation des alertes ;
  - Plan de continuité incluant les procédures de sauvegarde.