mai
2005

GUIDE SSI

Externaliser la mise en œuvre et la maintenance de la politique de sécurité

Fiche 10

MEDEF

Accompagner

La plupart des entreprises font appel aujourd'hui à des prestataires pour leur besoin d'évolution et de maintenance de leur système d'information. Il en va de même pour la sécurité, partie intégrante du système d'information.

Peu d'entreprises disposent des ressources internes pour remplir ces tâches relativement complexes.

La mutualisation permet de réduire les coûts et de s'assurer du maintien permanent d'un niveau acceptable de sécurité.

Installation et configuration par un (des) prestataire(s) de services agissant comme un sous-traitant sur votre site.

Ce prestataire installera et configurera les moyens de protection en conformité avec les politiques de sécurité.

Un autre prestataire pourrait contrôler si cet ensemble de tâches a été mené dans les règles de l'art (comme dans d'autres domaines avec le recours à des organismes de certification et de contrôle).

Maintenance sur site par un (des) prestataire(s) de services agissant comme un sous-traitant qui se rendra périodiquement sur site pour contrôler que ces moyens de défense répondent aux besoins.

Il est aussi envisageable de faire appel ponctuellement au prestataire en cas de modification des politiques de sécurité (à la suite de conditions imposées par exemple par une client ou un fournisseur, voire par une législation nouvelle).

Un autre prestataire pourrait contrôler si cet ensemble de tâches a été mené dans les règles de l'art (il peut s'agir que d'un contrôle très léger, pouvant d'ailleurs être réalisé à distance pour un coût assez faible).

Externalisation

L'externalisation de fonction consiste à confier à un partenaire spécialisé une fonction essentielle à la vie de l'entreprise, mais extérieure à son coeur de métier.

■ **Principes**. L'externalisation des systèmes d'information ou de leur gestion prend aujourd'hui des formes très diverses.

Il est difficile de s'y retrouver dans l'univers prolixe de l'externalisation, entre infogérance et tierce maintenance applicative, entre ASP (Application Service Provider) et BSP (Business Service Provider), MSS (Managed Security Services).

Beaucoup d'entreprises ont recours à l'externalisation de la paie voire de la comptabilité. Dans ce cas, l'entreprise transmet les données brutes au fournisseur de service et reçoit en contrepartie les documents de synthèse (déclarations sociales, fiscales, bilans et compte d'exploitation).

Dans le domaine de la sécurité, il existe un service équivalent pour la maintenance totale ou partielle des politiques de sécurité en permettant l'accès à distance aux systèmes en toute sécurité à une société spécialisée, dénommée « Managed Security Services Provider » (MSSP). Ce prestataire peut être votre fournisseur d'accès (FAI ou Opérateur) ou une filiale spécialisée de société de service informatique.

■ Accès à ce type de services

L'externalisation de la maintenance des politiques de sécurité semble être une solution particulièrement adaptée pour les PME/PMI, qui ne disposent généralement pas des moyens de veille nécessaires avec des ressources financières et humaines par nature très contraintes.

L'externalisation peut porter sur l'ensemble de la maintenance des politiques de sécurité (voir fiche9) mais il semblerait opportun de voir apparaître sur le marché une offre spécifique pour les PME/PMI qui porterait au moins sur les moyens de défense minimums (voir fiche 6).

Cette offre adresserait :

- ➔ la configuration des pare-feu,
- ➔ la gestion des mises à jour des versions correctives (ou veille au minimum),
- ➔ la détection des vulnérabilités
- ➔ le contrôle des mises à jour de signatures pour les anti-virus.

Une telle offre mutualisée pour PME/PMI devrait pouvoir être offerte à un coût acceptable, sous forme d'un abonnement annuel de l'ordre de quelques centaines d'euros pour les plus petites entreprises.

Ces différentes briques prises individuellement font d'ores et déjà partie du catalogue des offres de FAI ou d'Opérateurs.

Une offre globale et accessible financièrement, portant sur la gestion des moyens minimum, serait souhaitable.

■ Les 10 points clé d'un contrat d'externalisation

Afin de limiter le nombre de litiges, il conviendra de s'assurer que les documents contractuels (conditions générales et/ou particulières, proposition technique et financière, devis,..) traitent clairement des 10 points suivants :

♦ Document contractuel :

Le contrat mentionne-t-il la liste de l'ensemble des documents qu'il comprend (annexe, cahier des charges, proposition du prestataire…) et les hiérarchise t-il ?

Il est nécessaire déterminer les documents qui engagent l'entreprise et le prestataire et, en cas de conflit entre ces documents, celui qui prévaudra.

♦ Description des prestations :

Les prestations sont-elles précisément décrites?

Cela permet à l'entreprise de connaître précisément les prestations auxquelles s'engage le prestataire.

♦ Régime de l'obligation du prestataire :

Le contrat précise-t-il si le prestataire, ou telle ou telle de ses prestations, est soumis à une obligation de moyens ou à une obligation de résultats?

L'obligation de résultats portera sur le respect de délais fermes, et/ou d'indicateurs de performance (mesurables). Ces délais et indicateurs devront être stipulés au contrat. Attention en cas d'obligation de moyens, l'entreprise supporte normalement la charge de la preuve de la défaillance du prestataire. Lorsqu'il est possible, le régime de l'obligation de résultats offre plus de sécurité à l'entreprise quant à la bonne exécution des prestations.

♦ Prix des prestations :

Est-il prévu que le prix puisse évoluer (hausse ou baisse) ?
Notamment, si le prestataire baisse ses tarifs, s'engage-t-il a en faire bénéficier l'entreprise en cours de contrat ?

S'agissant de prestations qui s'inscrivent dans un environnement technologique et un marché qui évoluent vite, il faut que l'entreprise ait l'assurance que son contrat « colle au marché », ce d'autant plus que la durée du contrat sera longue (> 1 an).

♦ Pénalités :

Est-il prévu des pénalités en cas de non ou de mauvaise exécution du contrat, en terme de délai et/ou de non-respect de certaines performances (cf. obligation) ?

Elles sont normalement plafonnées (généralement à hauteur de 15% du montant du contrat). Le contrat doit prévoir l'articulation des pénalités avec les dommages et intérêts que l'entreprise doit pouvoir réclamer par ailleurs. Les pénalités visent à indemniser de manière forfaitaire l'entreprise du fait du retard ou de la non performance. Elles ont en même temps un effet dissuasif pour le prestataire.

♦ Statut des matériels et logiciels :

Le contrat devra préciser la propriété et le statut des matériels et des logiciels utilisés par le prestataire dans le cadre de l'exécution du contrat. Seront-ils fournis par l'entreprise ou par le prestataire ? Dans le dernier cas, restent-ils ou pas la propriété de ce dernier ? Seront-ils placés dans l'entreprise ou chez le prestataire ? L'entreprise devra t-elle souscrire ou pas une licence ?

Ce point aura un impact sur la responsabilité de l'entreprise concernant ces matériels et logiciels. Si l'entreprise en est propriétaire ou s'ils sont placés dans ses locaux, elle devra les faire couvrir par ses polices d'assurance.

♦ Étendue de la responsabilité :

Le contrat contient-il une clause limitant la responsabilité du prestataire à certains types de préjudice ou en excluant certains autres ?

Le prestataire n'est en principe pas tenu d'indemniser l'entreprise de ses préjudices indirects (notamment de ses pertes d'exploitation), sauf à être expressément prévu au contrat. L'exclusion, par contrat, de certains préjudices directs ou indirects pré qualifiés peut réduire voire supprimer l'indemnisation à laquelle l'entreprise pourra prétendre.

♦ Limitation du préjudice réparable :

Le contrat prévoit-il une limitation du montant de la réparation à laquelle l'entreprise pourra prétendre en cas de dommage, tous chefs de préjudice confondus ?

Attention : un plafonnement drastique du montant des dommages et intérêts que pourra réclamer l'entreprise aboutit quasiment à « neutraliser » la responsabilité du prestataire en cas d'inexécution de sa part du contrat.

♦ Cession des droits :

Dans le cas où le contrat comporte, à la charge du prestataire, la réalisation ou le développement de tout ou partie d'un logiciel, prévoit-il la cession (autant qu'elle est nécessaire à l'entreprise) de ces créations ?

Attention, en l'absence d'une clause de cession conforme à l'exigence du Code de la propriété intellectuelle, le prestataire reste titulaire des droits d'auteur sur celles-ci. Permet à l'entreprise de s'assurer, autant que de besoin, de la propriété des logiciels qu'elle aura commandé.

♦ Juridiction compétente :

Le contrat désigne t-il la juridiction compétente en cas de litige, notamment au plan géographique ?
N'est-elle pas trop éloignée du siège de l'entreprise ?

En cas de litige, il est plus facile de plaider près de chez soi que dans la ville, parfois éloignée, du siège du prestataire.