

Sécurité des données en télétravail

Retour d'expérience d'un prestataire informatique

28 Avril 2010

Sébastien RAILLARD
(COEXSI)

Prestations de services informatiques à distance

Type de prestation :

- Infogérance (régulière)
- Projet (ponctuelle)

Avantages :

- Réactivité (client)
- Diminution des coûts (client et prestataire)
- Organisation (prestataire)

Inconvénient évident : l'aspect sécurité

Inconvénient à évidence variable

- Sensibilisation à un problème de sécurité généralement liée à la taille de l'entreprise
- Clauses de confidentialités (NDA) signées lorsque c'est généralement inutile et non signées lorsqu'elles auraient un sens
- L'aspect pragmatique arrange généralement toutes les contraintes liées à la sécurité, surtout quand la direction trouve cela pratique
- La sécurité n'est pas finalement pas vraiment un problème
- Y a-t-il vraiment moins de risques à travailler depuis le site?

Infogérance

- Administration régulière
- Les tâches peuvent être bien définies
- Le périmètre de sécurité peut être clair
- Il est plus simple de restreindre le périmètre d'un utilisateur que d'un administrateur
- Avec le temps, risque de se faire apparenter aux internes et de voir son périmètre d'accès s'agrandir – surtout en cas d'interventions sur site

Projet

- Action ponctuelle, de courte durée
- Peut nécessiter des privilèges élevés si la prestation touche l'exploitation ou l'intégration
- Le périmètre d'action initial peut être dépassé et devenir non contrôlé (pression mise en ligne)
- Les équipements et logiciels peuvent manquer de finesse quant à la gestion de privilèges élevés
- Suivant la spécificité des interventions, les interlocuteurs internes peuvent être dépassés

Marque blanche

- Eviter la déstabilisation du client final
- Multiples emails et cartes de visite
- Plusieurs entités intervenantes
- Périmètre flou des responsabilités en cas de problème
- Problème de couverture des accords de confidentialité
- Situation pouvant devenir inconfortable

Les accès

- Télétravail = accès aux infrastructures internes
- Internet est le support universel
- Rarement possible d'utiliser une infrastructure VPN déjà existante
- Solutions de contournement (VPN-SSL)
- Faire son propre trou depuis l'intérieur dans l'indifférence générale (ouverture d'accès)
- Utilisation d'outils à risque comme « LogMeIn »
- Sécurisation du poste de travail
- Penser aux risques pouvant venir de l'infrastructure du client via VPN
- Les DSI psycho-rigides exacerbent le problème !