

Mettre en œuvre une télémaintenance sécurisée

La télémaintenance permet au responsable informatique ou au prestataire informatique chargé de la maintenance d'une entreprise, d'intervenir de l'extérieur sur le système informatique pour dépanner ou administrer à distance les applications métiers (installation, configuration, mise à jour) ou les équipements (serveurs, postes de travail, pare-feu, routeur d'accès à Internet).

Le responsable informatique ou le prestataire passent en fait à travers le réseau public à risque Internet pour s'introduire sur le réseau interne de l'entreprise, dont on a laissé une porte d'entrée ouverte, quelquefois en permanence. Ceci implique des risques importants de sécurité pour l'entreprise.

Les risques liés à une télémaintenance non sécurisée.

- Un pirate peut s'introduire sur le réseau interne de l'entreprise en passant par la porte d'entrée laissée ouverte.
- Les échanges réalisés entre le prestataire et l'entreprise transitent en clair à travers Internet. Un pirate peut donc surveiller ce trafic et récupérer des informations confidentielles comme les mots de passe administrateur des serveurs, des applications métiers ou du routeur d'accès à internet. Il aura ainsi à sa disposition un « jeu de clés » qui pourra par exemple lui donner accès aux documents sensibles de l'entreprise (fichier client, bilan comptable, contrats, business plan etc...).
- L'utilitaire de prise de contrôle le plus utilisé est le Bureau à distance de Windows. Or cet utilitaire est très vulnérable puisqu'il peut permettre la prise de contrôle des serveurs ou postes de travail à l'insu des utilisateurs et qu'il est associé à un point d'entrée au réseau interne de l'entreprise connu de beaucoup de personnes. En fait, l'utilisation du Bureau à distance facilite la tâche d'un pirate qui veut s'introduire dans le réseau de l'entreprise, prendre le contrôle des serveurs ou postes de travail et récupérer des documents confidentiels.
- Enfin, l'entreprise peut perdre le contrôle sur les interventions extérieures du prestataire informatique, qui peut se connecter quand il le désire. Elle peut par exemple se rendre compte trop tard d'une mise à jour de l'application métier qui a été effectuée à son insu, car celle-ci ne fonctionne plus correctement.

Il est donc très important de sécuriser le cadre dans lequel se déroule la télémaintenance.

Nous allons traiter le cas le plus représentatif, c.à.d. le cas de l'entreprise Encélade qui veut sécuriser les télé-interventions de son prestataire informatique chargé de l'administration et du dépannage de l'application métier, du serveur, des postes de travail Windows et de son réseau.



Cas : L'entreprise Encélade

L'entreprise Encélade veut sécuriser les télé - interventions de son prestataire informatique chargé de l'administration et du dépannage de l'application métier, du serveur, des postes de travail Windows et de son réseau.

Facilité de mise en œuvre : moyenne
Facilité d'exploitation : moyenne
Hauteur de l'investissement humain : moyenne

Les règles que l'entreprise doit suivre pour sécuriser les télé-interventions

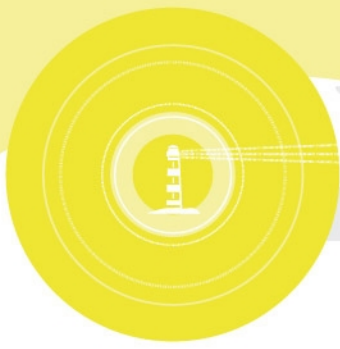
1. Bien déterminer le périmètre d'intervention, les ressources à télé administrer ainsi que les objectifs à atteindre.

Consigner dans le contrat de maintenance des règles précises sur l'intervention par télémaintenance comme :

- aucune télé – intervention ne peut être réalisée sans accord préalable de l'entreprise ;
- les inconvénients liés à l'intervention (machine indisponible, redémarrage serveur...) doivent être indiqués par le télé-intervenant, avant de commencer quoique ce soit.
- l'intervention doit être consignée et détaillée dans un compte-rendu (objet de l'intervention, changements effectués....)
- Crypter les échanges entre le télé - intervenant et le réseau interne de l'entreprise, afin de garantir la confidentialité des informations qui transitent sur Internet. La création de canaux de communications cryptés à travers Internet est donc nécessaire à chaque fois qu'une intervention est décidée.

Désactiver le Bureau à distance sur le serveur et Postes de travail, afin de limiter les risques de télé -intervention « sauvage ».

- Utiliser de préférence, un utilitaire de prise de contrôle, qui ne fonctionne qu'après avoir été lancé par une personne située dans l'entreprise.
- protéger le lancement de cet utilitaire, par un mot de passe ;
- et penser à le désactiver à la fin de l'intervention.
- Installer les consoles d'administration du routeur, du pare-feu ou des autres équipements administrables, sur un poste de travail dédié plutôt que sur le serveur. On évite ainsi d'affaiblir sa protection.
- Ne pas mémoriser les mots de passe dans les consoles d'administration, afin d'éviter qu'une personne qui a pris le contrôle du poste de travail ne puisse pas accéder facilement à l'administration des autres équipements.
- Activer et enregistrer les journaux d'évènements qui peuvent être créés au niveau du routeur d'accès, afin de disposer d'un contrôle des tentatives d'accès de l'extérieur au réseau interne de l'entreprise.



La solution technique adoptée par l'entreprise :

- Le routeur d'accès à Internet n'ayant pas la fonction de concentrateur VPN, un 2^{ème} routeur, qui intègre cette fonction et qui peut créer les canaux de communication cryptés, a été installé sur un 2^{ème} accès Internet. Le trafic lié à la télémaintenance est ainsi mieux maîtrisé et surveillé.
- Le logiciel de prise de contrôle Ultra VNC, (logiciel gratuit) a été installé sur le serveur, les postes de travail et le poste qui héberge les différentes consoles d'administration. Le télé-intervenant devra ainsi appeler avant toute intervention, afin de demander le lancement de ce logiciel.
- Ce logiciel ultra VNC a également été installé sur le poste du télé – intervenant, qui est équipé d'un client VPN, afin de créer à la demande un tunnel crypté à travers Internet entre ce poste et le concentrateur VPN, qui est situé sur le réseau interne de l'entreprise.