Petites structures : comment réduire l'exposition de son SI face aux menaces cyber ?

Difficultés liées à la gestion de son SI

Face aux menaces de cybersécurité telles que les attaques par rançongiciel et l'exfiltration de données, le directeur de la structure doit s'assurer de sa capacité à restaurer des données intègres ainsi que de leur protection en confidentialité en cas d'incident.

Les services socles d'un SI tels qu'un service de virtualisation (hyperviseur) ou un contrôleur de domaine (technologie Windows) doivent être correctement administrés pour maintenir un niveau de sécurité suffisant par rapport à ces menaces. La gestion des sauvegardes revêt ainsi un caractère particulièrement critique en cas de chiffrement des données par un rançongiciel.

Bénéfices d'une externalisation

Lorsque les services numériques et les données de la structure sont externalisés, ils sont beaucoup moins exposés à la compromission du SI local, réduisant considérablement le risque de perte, d'indisponibilité ou de vol. Les postes utilisateurs quant à eux pourront être remplacés facilement en cas de crise.

L'externalisation peut également entrainer une **réduction des coûts par rapport à la maintenance locale** qui nécessite la présence permanente d'un informaticien.

Rappels avant de souscrire une prestation

- Se renseigner sur la qualité de service du prestataire
- Négocier **une clause sur le maintien en conditions de sécurité** de l'infrastructure (vulnérabilités critiques corrigées en moins de 48h)
- Négocier le temps d'indisponibilité du SI en cas de problème (ex : rétablissement sous 4h maximum après incident).
- Négocier **une clause sur le risque de perte des données** (ex : perte maximale de 24h de données saisies après restauration de la dernière sauvegarde)
- Négocier **une clause de réversibilité** et **l'obligation d'une assistance technique** dans le cadre d'une reprise du système

Externalisation par étape

L'objectif est d'**externaliser par étapes** en commençant par les ressources les plus critiques. Une première étape consiste à cartographier son SI et **identifier les serveurs et services métiers pouvant être hébergés** en :

- vérifiant avec les éditeurs des différents services métiers si ces derniers peuvent être externalisés ;
- passant par la version dite « SAAS » d'un service ;
- priorisant les serveurs les plus critiques parmi ceux qui restent.

La deuxième étape consiste à **prioriser l'externalisation des services métiers vitaux**, les serveurs socles critiques (messagerie, partage de fichiers, etc.) puis les serveurs non essentiels.

Enfin, il est important d'évaluer l'utilité de conserver les composants restants et idéalement de les décommissionner plutôt que de les externaliser.
Dans tous les cas, il est **fortement recommandé de disposer de sauvegardes externalisées** qui couvrent les services hébergés.

Sécurité du SI local

Pour limiter les risques de compromission au niveau des serveurs ou des postes utilisateurs qui continueront à être gérés localement, il est conseillé de suivre les recommandations suivantes :

- utiliser **une machine dédiée pour chaque service métier** et la limiter uniquement à cette utilisation ;
- déployer **un antivirus** sur chaque machine et en priorité sur celles portant les services métiers ;
- de **maintenir à jour** au maximum le parc ;
- de s'assurer que les données critiques pour la structure font bien l'objet d'une sauvegarde hors ligne.