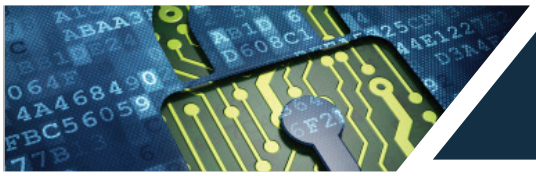
PÔLE RÉSEAUX

Sécuriser le système d'information de l'entreprise

LA SÉCURITÉ DU SYSTÈME D'INFORMATION : UNE APPROCHE GLOBALE

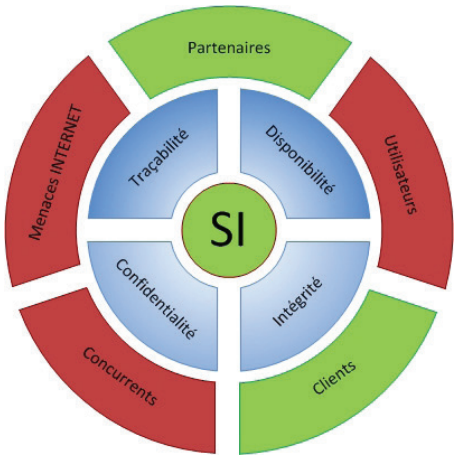
Le système d'information est devenu l'épine dorsale de l'activité de l'entreprise, Complexe et étendu, il est accessible de l'extérieur et touche tous les services. La dématérialisation entraîne par ailleurs une forte dépendance envers l'informatique.

La sécurité du système d'information doit être envisagée de façon globale : rien ne sert de se concentrer sur un point central (par exemple le serveur) et négliger les points périphériques (par exemple l'accès à la salle serveur).



Plusieurs critères d'évaluation

Il est intéressant de définir de façon précise quels sont les risques pour votre entreprise et comme, les prévenir. Alticap vous accompagne en réalisant un audit de vos usages de l'outil informatique ainsi que des matériels et logiciels en place.



VOUS NOUS DITES

«Mon informatique s'est développée de façon pléthorique.

Centre névralgique de mon organisation, j'ai l'impression de ne rien maîtriser.

Quels sont les points qu'il est nécessaire de sécuriser ?»

Les points de vigilance

PROTECTION PHYSIQUE DE ÉQUIPEMENTS

- Accès contrôlé à la salle informatique : salle fermée, accès sécurisé,
- Mise sous onduleur des matériels sensibles : serveur, routeur, firewall...
- Régulation température et hygrométrie de la salle serveur : mise en place éventuelle d'une climatisation,
- Matériels sensibles sous garantie et maintenance : la défaillance d'un matériel sensible doit pouvoir être corrigée rapidement

PROTECTION DES DONNÉES

- Sauvegarde et historisation des données sensibles via un logiciel dédié : seul moyen efficace d'administrer les sauvegardes et permet de sauvegarder les données en mode crypté,
- Externalisation régulière des données sensibles,
- Accès aux données contrôlé : je n'accède qu'aux données pour lesquelles j'ai une autorisation grâce entre autres à la gestion des droits,
- Intégrité des données

PROTECTION DES APPLICATIONS

- • Politique d'accès aux applications par mots de passe : nécessite de faire évoluer les mots de passe et de suivre les changements de personnels,
- • Mise à jour régulière des versions de logiciel proposées par les éditeurs : des versions trop anciennes peuvent entraîner des risques d'indisponibilité en cas d'incident technique,
- • Accès aux applications contrôlé : je n'accède qu'aux applications pour lesquelles j'ai une autorisation grâce entre autres à la gestion des droits.

PROTECTION DU RÉSEAU INFORMATIQUE

- Antivirus postes et serveurs : contrôle des points d'entrée en local,
- Boîtier de sécurité UTM : contrôle des entrées/sorties
- INTERNET,
- Accès WIFI sécurisé : mise en oeuvre de clé de protection, identification des postes/utilisateurs, politique de conformité de la sécurité des OS,
- Mise à jour de sécurité des systèmes d'exploitation postes et serveur,
- Mise à jour de sécurité des logiciels postes et serveur,
- Politique sécurisée d'accès au réseau : par mots de passe (nécessite de faire évoluer les mots de passe et de suivre les changements de personnels), token, identification physique...

PROTECTION DES ÉCHANGES

- Sécurisation des échanges : cryptage des données importantes,
- Sécuriser les interconnections : sites distants et nomades doivent être connectés de façon sécurisés (authentification, cryptage),
- Contrôle de la bande passante : fiabilisation des échanges inter-sites par boîtier de contrôle de flux (type UTM).

SYSTÈME D'INFORMATION EN GÉNÉRAL

En cas de nécessité de haute disponibilité des applications et systèmes : mise en place d'un Plan de Reprise d'Activité (PRA) ou solution de réplication (applications, serveurs, accès INTERNET, inter-connection...).

LES PLUS ALTICAP

Évaluez la sécurité de votre système d'information et obtenez gratuitement votre Indice de Sécurité Réseau