Directives informatiques de l'ASGB – édition 2018

Sommaire

Avant-propos

Les directives informatiques ont pour but de fournir aux membres de l'ASGB un aperçu des champs d'action dont ils disposent en ce qui concerne la sécurité informatique, ainsi que de leur donner une vue d'ensemble générale. Les directives informatiques ne peuvent pas aborder chaque question dans le détail. Leur objectif est bien plus de sensibiliser les membres afin qu'ils prennent en considération et évaluent les différents thèmes dans le contexte de leur organisation. Des spécialistes seront ensuite nécessaires pour aller dans le détail de chaque thème.

Il existe en effet des conditions-cadres légales qu'il faut en partie respecter et qui vont au-delà du thème de l'application informatique. L'infrastructure informatique est considérée comme un outil qui vient en soutien à d'autres activités. Le présent document ne peut pas juger de sa pertinence légale et éthique.

La transition entre utilisation professionnelle et privée est courante. Ceci peut toutefois engendrer des conflits concernant les questions de sécurité. Il faut donc définir le niveau de sécurité souhaité: l'objectif est-il de se protéger de «criminels occasionnels» ou de «personnes avec une forte énergie criminelle»?

Le thème de la sécurité informatique devrait toujours être traité selon les aspects suivants:
- aspects stratégiques
- processus opérationnel
- technique

1 Remarque préliminaire/introduction

1.1 Importance de la sécurité informatique pour la branche des graviers et du béton

La sécurité informatique est un terme large, qui peut en partie paraître abstrait. Toute entreprise, aussi petite soit-elle, doit lui donner un sens concret. Dans la suite du texte, la sécurité informatique est considérée dans son ensemble et ne se limite pas aux «logiciels antivirus» et à la «gestion des mots de passe».

Concernant la sécurité des informations, les grandes entreprises et les autorités sont souvent mieux armées à faire face que les petites et moyennes entreprises en raison des moyens financiers et personnels dont elles disposent. Même si la prise de conscience de l'importance de la sécurité informatique ne cesse de gagner en ampleur, les mesures ne peuvent souvent pas être suffisamment mises en œuvre en raison d'un personnel peu qualifié et du manque de ressources financières et de temps.

Les présentes directives informatiques expliquent les étapes nécessaires afin de contrôler le niveau de sécurité informatique existant et propose des mesures simples à mettre en place même avec de

faibles moyens financiers et avec un nombre restreint de collaborateurs qui se chargent pour la première fois de ce type de problématique.

Le plus important est de rester conscient de la nécessité de se pencher sur les questions de sécurité informatique. Ceci vaut également pour la non-application consciente de mesures qui ne semblent pas adéquates dans l'environnement spécifique.

1.2 Protection de base

La norme internationale ISO/CEI 27001 Management de la sécurité de l'information (SMSI) précise les exigences posées à l'implémentation, l'application, la sauvegarde et l'amélioration continue d'un système de management de la sécurité de l'information documenté.

Les méthodes SMSI préconisent trois modes d'action pour l'implémentation de la protection informatique globale:

- La **protection de base** (applicable à chacun) fournit une introduction à la mise en place d'un SMSI.
- La **protection standard** permet la mise en œuvre d'un processus de sécurité complet compatible avec la certification ISO 27001.
- La **protection centrale** (pour les établissements au sein d'un groupe) est une démarche de lancement d'un SMSI qui se penche d'abord sur une petite partie d'un grand concentré d'informations. La protection centrale a pour but de protéger au plus vite les principales ressources et processus commerciaux. Ceci permet, pour commencer, de sécuriser le processus commercial le plus critique puis de continuer soit à protéger les autres processus commerciaux dans leur ordre de criticité, soit à se lancer dans une protection de base ou standard de tous les autres domaines de l'établissement.

La protection de base est préconisée pour les établissements qui répondent aux critères suivants:

- L'implémentation de la sécurité informatique n'en est qu'à ses débuts, son niveau est plutôt faible
- Les processus commerciaux n'ont pas de potentiel de risque rès élevé en ce qui concerne la sécurité informatique
- Le niveau de sécurité visé est normal
- Il n'y a pas de valeurs numériques ou analogiques dont le vol, la destruction ou la compromission engendreraient un dommage qui mettrait en péril la pérennité de l'établissement
- Les petits incidents de sécurité sont tolérables (c'est-à-dire ceux qui coûtent de l'argent ou causent d'autres dommages, mais qui cumulés ne mettent pas en danger la pérennité de l'établissement)

1.3 Pertinence de la sensibilisation du personnel en complément aux mesures techniques

Le personnel d'une entreprise ou d'une autorité représente la base de son succès ou de son échec. Les collaboratrices et collaborateurs jouent aussi un rôle essentiel dans la sécurité des informations. Par expérience, même les dispositifs techniques de sécurité les plus lourds sont inefficaces si les collaborateurs ne se comportent pas correctement. Il est donc essentiel qu'ils

aient conscience de ce que signifie la sécurité des informations pour l'établissement et ses processus commerciaux et qu'ils manipulent correctement les informations à protéger de l'établissement.

Le meilleur antivirus et le meilleur pare-feu ne servent à rien si le personnel n'agit pas, si les autorisations sont mal gérées, en présence d'ingénierie sociale ou de négligence dans la gestion des informations.