Conseil d'Etat
Staatsrat

CANTON DU VALAIS
KANTON WALLIS

RÉPONSE AU POSTULAT

Auteur	Groupe PDCB, par Eric Lattion (suppl.) et Sébastien Clerc (suppl.)	
Objet	Cybercriminalité : les PME valaisannes sont des cibles idéales	
Date	11.09.2018	
Numéro	3.0414	**En collaboration avec le DFE**

Comme relevé dans le postulat, la cybercriminalité est un danger important pouvant impacter gravement toute entreprise, quelle qu'en soit la taille, l'organisation ou le domaine d'activité. Ce constat doit être pris en compte et considéré comme un risque majeur à gérer par toutes les entreprises, y compris pour celles ne représentant a priori aucunement une cible potentielle.

En l'état, il est impossible de recenser les cyberattaques affectant les PME valaisannes. En l'absence de base légale adaptée, aucune obligation d'annonce n'existe à l'heure actuelle. Un tel recensement ne pourrait être réalisé que sur une base volontaire et serait donc, par définition, fort incomplet. Toutefois, l'avant-projet de loi fédérale sur la protection des données, qui sera traité en 2019 par le Parlement fédéral, introduit l'obligation d'annonce dès lors qu'une cyberattaque impacte des données à caractère personnel.

MELANI, la Centrale fédérale d'enregistrement et d'analyse pour la sûreté de l'information, met à disposition un site Web à l'attention des PME. Ce site très complet offre de multiples documents en lien avec la cyberprotection des entreprises. De plus, l'Office fédéral pour l'approvisionnement économique du pays (OFAE) a édité en septembre 2018 un document référence à l'attention de l'économie suisse intitulé « Norme minimale pour améliorer la résilience informatique ». La Confédération, dans son « plan d'action cyberdéfense du Département fédéral de la défense, de la protection de la population et des sports (DDPS) », est claire quant à la responsabilité de chaque entreprise de gérer sa propre cyberprotection.

Il incombe à notre avis aux associations professionnelles valaisannes de sensibiliser l'économie valaisanne, comme certaines le font déjà, en proposant des conférences en lien avec la cybersécurité ainsi que d'autres appuis divers et variés. En automne 2018, BusiNETvs a organisé une conférence sur la protection des données pour les PME, alors que la Chambre valaisanne de commerce et d'industrie a mis sur pied le 3e Forum Cybersécurité.

En conclusion, la Confédération, les associations professionnelles et les entreprises spécialisées font déjà un travail important de sensibilisation à l'attention des PME valaisannes et le principe selon lequel chaque entreprise est responsable de sa propre cyberprotection apparaît comme pragmatique dans l'environnement économique actuel.

On peut encore relever qu'il n'est pas possible pour chaque PME d'avoir un spécialiste de haut niveau en matière de sécurité. Un appui par des entreprises spécialisées peut donc être souhaitable. Mettre en place dans l'entreprise d'une certaine taille une fonction de sécurité (physique et logique) rattachée à un cahier des charges existant peut également représenter une bonne pratique, afin que ce domaine soit considéré à sa juste valeur.

Il est proposé le rejet de ce postulat.

Conséquences sur la bureaucratie : Préparation d'une loi spécifique d'encadrement.

Conséquences financières (estimations) :

- Coûts uniques : 50'000 fr. à 100'000 fr. pour la préparation d'une loi spécifique d'encadrement.
- Coûts récurrents : 340'000 fr. à 390'000 fr. par an pour la création, hébergement et gestion d'un site Internet, la mise à disposition d'une solution de *eLearning* de sensibilisation à disposition

des entreprises, le financement d'événements liés à la sécurité, le financement de deux places de travail (Basé sur le coût indicatif communément admis pour une ressource, à savoir 120'000 fr./an, à noter que le coût de bon spécialistes de la sécurité peut aller bien au-delà par EPT), ainsi que l'appel à divers spécialistes.

Conséquences équivalent plein temps (EPT): 2 EPT estimés, à savoir :

- 1 personne chargée de la sensibilisation des entreprises effectuant la tournée des entreprises afin de les sensibiliser par des présentations et la mise sur pied de séminaires et formations dédiés.
- 1 personne chargée d'aider les entreprises en répondant à leurs interrogations, en proposant des exemples de politiques, directives et recommandations de sécurité et de bonnes pratiques et se chargeant de la centralisation et de l'analyse des cyberattaques annoncées.

Conséquences RPT : aucune

Lieu, date Sion, le 5 juin 2019