INTERPELLATION URGENTE

Auteur	PDCB, par Florentin Carron et Charline Berguerand (suppl.)
Objet	WannaCry – quelle riposte?
Date	06.06.2017
Numéro	1.0213

Actualité de l'événement
Un logiciel d'extorsion a sévi courant mai sur la planète entière et a bloqué des milliers d'ordinateurs touchant des administrations publiques.
Imprévisibilité
L'ampleur d'une telle attaque est à ce jour inégalée.
Nécessité d'une réaction ou d'une mesure immédiate
La cybercriminalité et les logiciels d'extorsion sont appelés à se développer et des correctifs doivent être rapidement apportés.

Le logiciel «WannaCry» débutait son attaque le 12 mai 2017 et continuait une semaine plus tard à bloquer des ordinateurs sur toute la planète. Selon de premières estimations, «WannaCry» était parvenu à bloquer plus de 300'000 ordinateurs dont des machines d'entreprises mais aussi du secteur public.
En Grande-Bretagne, des ambulances avaient été déroutées d'un hôpital à l'autre. Le logiciel avait pris le contrôle de distributeurs d'argent et neutralisé une chaîne de montage en France.

Le processus d'une telle attaque et son mode opératoire reste difficile à saisir. Les pirates peuvent contrôler les machines à distance. Pour «WannaCry», certaines parties du code du logiciel renvoyaient à la Corée du Nord, à la Russie ou à la Chine, des pays eux-mêmes cibles de l'attaque.

Bien que difficile à chiffrer, de telles attaques peuvent occasionner d'énormes frais. L'impact économique est tel que selon certaines estimations les préjudices causés par des logiciels d'extorsion du type de «WannaCry» pourraient avoisiner 3000 milliards de $.

Les sommes investies par le canton du Valais pour sa «stratégie informatique 2015-2024» sont plus modestes; le montant de 90 millions de francs a été voté par le Grand Conseil valaisan en novembre 2015. Ce montant doit servir à moderniser et à développer le réseau informatique de l'administration cantonale. Celui-ci nécessite des rattrapages à plusieurs niveaux car – je cite – c'est une «infrastructure de base qui présente un degré d'obsolescence et des vulnérabilités qui mettent à risque la continuité opérationnelle de l'Etat».

Conclusion
A l'heure où les cyberattaques et la cybercriminalité semblent s'intensifier partout dans le monde, nous nous demandons dans quelle mesure la «stratégie informatique 2015-2024» a intégré ces enjeux:
- Scénario catastrophe. Procédure prévue en cas d'attaque?
- Quelle attitude adopter en cas de demande de rançon d'une grosse somme d'argent?
- Dans quelle mesure l'administration cantonale pourrait-elle poursuivre son activité, sauvegarder les données dont elle a besoin dans sa tâche et protéger les informations concernant les citoyens et contribuables valaisans en cas de piratage informatique?
- Pourrait-on faire appel à une équipe d'experts en cybersécurité, ou peut-être une telle équipe est-elle déjà en place?