Réponse du Conseil d'Etat à un instrument parlementaire
—
Question 2024-GC-183
Comment le canton de Fribourg assure-t-il sa résilience face aux pannes informatiques ?

Auteurs :	**Dorthe Sébastien / Michellod Savio**
Nombre de cosignataires :	**0**
Dépôt :	**22.07.2024**
Développement :	**---**
Transmission au Conseil d'Etat :	**22.07.2024**
Réponse du Conseil d'Etat :	**24.09.2024**

I. Question

Dans la question 2024-GC-168 « SITel, quelles conséquences à la suite de la perte de certains mandats ? », nous nous inquiétions notamment de la souveraineté informatique du canton. La panne informatique mondiale causée par CrowdStrike, ayant affecté des millions d'ordinateurs le 19 juillet dernier, a eu des répercussions significatives et rend la question de la souveraineté informatique encore plus actuelle.

Par conséquent, nous posons les questions complémentaires suivantes :

1. L'Administration cantonale a-t-elle été touchée par cette panne ? Le cas échéant, dans quelle mesure et avec quelles conséquences pour les citoyennes et citoyens ?
2. Quelles actions spécifiques le Conseil d'Etat envisage-t-il pour réduire la dépendance aux prestataires externes ? Quelles mesures sont prises pour renforcer les infrastructures informatiques internes et accroître la résilience face à de futures pannes mondiales ?
3. Le Conseil d'Etat a-t-il déjà effectué une estimation des coûts directs et indirects occasionnés par une panne d'ampleur affectant les services publics (pertes de données, interruptions de services, heures de travail perdues, etc.) ? Le cas échéant, quels sont ces coûts ?

II. Réponse du Conseil d'Etat

1. L'Administration cantonale a-t-elle été touchée par cette panne ? Le cas échéant, dans quelle mesure et avec quelles conséquences pour les citoyennes et citoyens ?

Non, l'Administration cantonale n'a pas été touchée par la panne informatique « CrowdStrike ».

2. Quelles actions spécifiques le Conseil d'Etat envisage-t-il pour réduire la dépendance aux prestataires externes ? Quelles mesures sont prises pour renforcer les infrastructures informatiques internes et accroître la résilience face à de futures pannes mondiales ?

Si l'Etat de Fribourg n'a pas été impacté par la panne précitée, il n'est toutefois pas à l'abri d'une panne d'ampleur. Il est en effet constaté une accélération des cyberincidents et une multiplication des défis de la mutation numérique.

C'est dans ce cadre que s'inscrit la stratégie de cyberrésilience et de souveraineté numérique pour l'Etat de Fribourg. L'établissement de cette stratégie a été initié par le Service de l'informatique et des télécommunication (SITel) et porté au printemps 2024 devant le Conseil d'Etat, qui en a validé le principe. Le but recherché est un Etat de Fribourg qui puisse maitriser les défis et les risques du numérique en étant résilient, souverain et proactif. Pour ce faire, deux pans principaux de la stratégie précitée peuvent être relevés. Il s'agit premièrement d'une stratégie pour renforcer la résilience des infrastructures numériques de l'Etat en case de crise et pour renforcer sa souveraineté numérique. Est visée ici la capacité de l'Etat à assurer en toute circonstance la continuité de sa conduite, de ses tâches systémiques et de la sécurité publique face aux cyberrisques. Le deuxième pan, plus large, consiste en une stratégie cantonale de cybersécurité.

Pour des raisons évidentes de sécurité, les stratégies précitées ne font pas l'objet d'une publication. Le sujet pourrait par contre faire l'objet de discussions à la Commission des finances et de gestion, sous-commission SITel.

Le domaine de la cybersécurité est pris très au sérieux par le SITel et également par d'autres entités, par exemple la Police qui est aussi impliquée. Le SITel entreprend toutes les actions, dans la limite des moyens qui lui sont attribués, afin de limiter les risques. Par exemple, un « security operation center » (SOC) assure une surveillance permanente du trafic de données.

A relever que les ressources internes (EPT) accordées au SITel par le Conseil d'Etat, dans le cadre de l'établissement des budgets et des priorités que doit faire ce dernier, ne permettent pas d'internaliser toutes les prestations souhaitées. Il n'y a ainsi pas d'autres choix que de financer certaines prestations par des contrats avec des tiers. Sur ce sujet, le Conseil d'Etat précise qu'il a décidé de lancer une analyse sur les mandats externes (base comptes 2024) octroyés par SITel. Il sera en outre examiné l'opportunité d'engager des forces internes au SITel, en diminuant les coûts d'externalisation. Cette opération pourrait s'avérer bénéfique pour l'Etat, tant au niveau financier qu'au niveau des connaissances internes.

3. *Le Conseil d'Etat a-t-il déjà effectué une estimation des coûts directs et indirects occasionnés par une panne d'ampleur affectant les services publics (pertes de données, interruptions de services, heures de travail perdues, etc.) ? Le cas échéant, quels sont ces coûts ?*

Une telle estimation n'a pas été réalisée, les hypothèses à retenir pouvant fortement varier.