Question écrite N° 3778

Risques de l'univers numérique

Sandra Nobs (PLR)

Réponse du Gouvernement

Le Gouvernement répond comme il suit aux questions posées :

1. Le Gouvernement a-t-il établi un protocole de sécurité informatique ? Ou tout autre protocole semblable ?

La République et Canton du Jura (RCJU) dispose d'une Stratégie de cybersécurité (SCJU) spécifique à cette thématique. Cette stratégie est basée sur le référentiel international de bonnes pratiques du NIST Cybersecurity Framework. Celui-ci a été conçu initialement afin de protéger des infrastructures publiques jugées comme critiques. Il est aujourd'hui reconnu internationalement et largement utilisé.

La SCJU est articulée autour des cinq grands piliers du NIST : identifier, protéger, détecter, répondre et rétablir. Ces piliers sont chapeautés par une gouvernance forte. Ils permettent un suivi dynamique de l'organisation, des systèmes internes ainsi que des cyber-risques au niveau technique.

Le pilier « Détection » impose aux entités soumises au droit public de réaliser des évaluations et des audits de leur propre système d'information, ainsi que de ceux des tiers (sous-traitants) qui interagissent avec celui-ci.

La SCJU décrit les différents outils mis à disposition du Gouvernement afin d'atteindre les objectifs fixés. Ces outils sont principalement de nature organisationnelle et visent à garantir que le flux d'information nécessaire à des prises de décision parfois rapides soit assuré.

2. Si oui, à quelle fréquence ces tests sont-ils effectués et sur quels services en particulier

Les cyber-risques actuels nécessitent une approche continue et transversale. C'est la somme de l'ensemble des éléments de contrôle qui permet d'adresser les différents points de vulnérabilité, en évaluant leur probabilité d'occurrence ainsi que leur impact sur les missions de l'État.

Ces contrôles ne sont pas uniquement d'ordre technologique, mais également organisationnels, sous la forme d'audits de la gouvernance de la cybersécurité. Ceux-ci visent à s'assurer de l'application des bonnes pratiques issues du cadre NIST CSF.

Ces pratiques sont évaluées tous les trois ans, et il en ressort des mesures d'amélioration.

Le périmètre est complet, mais le point d'entrée reste le Service de l'informatique cantonal (SDI). En auditant le système d'information dans son ensemble, le SDI cherche à garantir que tous les acteurs impliqués dans les missions de l'État soient évalués, et qu'aucun point de vulnérabilité ne vienne compromettre la chaîne de valeur reliant chaque service et ainsi d'assurer la continuité des activités.

Le SDI dispose de plusieurs outils qui évaluent en continu les vulnérabilités présentes dans le système d'information de la RCJU. Ces systèmes alertent directement le groupe de cybersécurité du SDI, ce qui permet de réagir rapidement aux incidents grâce à des mesures techniques et organisationnelles.

Des campagnes spécifiques via des simulations d'attaques sont réalisés sur les éléments périmétriques et exposés à l'Internet via des services externes de type « hacking éthique ». Ceux-ci permettent de vérifier en continue et avec les dernières techniques connues la capacité de détection, de protection des systèmes. Une attention particulière est donnée aux éléments sensibles comme le Guichet virtuel.

En complément, des audits techniques ciblés sont réalisés ponctuellement sur les éléments d'infrastructure identifiés comme critiques ou lors de la mise en exploitation de nouvelles solutions, afin de s'assurer que les bonnes pratiques de cybersécurité sont bien appliquées.

3. Si non, le Gouvernement envisage-t-il de mettre en place des contrôles renforcés

-

4. Les collaborateurs sont-ils formés à l'hameçonnage

L'ensemble des collaborateurs de la RCJU suivent obligatoirement un cursus de formation en cybersécurité. Celui-ci dépasse les seules thématiques liées aux techniques d'hameçonnage et à l'ingénierie sociale, et inclut d'autres sujets abordés sous forme de campagnes, tels que les risques liés à l'intelligence artificielle, l'utilisation du téléphone mobile dans l'espace public ou encore les rançongiciels.

Le degré de maturité des utilisateurs est évalué, du stade « débutant » au stade « avancé », à l'aide de différents tests réalisés durant le cursus de formation. Ces évaluations prennent la forme de questionnaires spécifiques, enrichis par des tests réguliers sous forme de courriels d'hameçonnage.

Lorsqu'un collaborateur reçoit un courriel suspect et qu'il a un doute quant à sa légitimité, il dispose d'un outil lui permettant de le signaler. Ces courriels sont ensuite analysés par le SDI, et le résultat de l'analyse est retourné à l'utilisateur. Ce processus contribue à une formation continue, ainsi qu'au partage des connaissances et au renforcement des capacités de détection propres à ce type d'attaque.

Lors de la journée d'accueil des nouveaux collaborateurs de la RCJU le volet de la cybersécurité dispose d'un espace dédié animé par un collaborateur du SDI membre de la cellule de cybersécurité.

5. Quelle est la situation dans les communes et les institutions paraétatiques ? Des discussions sont-elles actuellement menées dans le domaine en partenariat avec les communes afin d'établir un protocole commun entre l'État et ces dernières

La stratégie de cybersécurité de la RCJU est impérative pour les entités soumises au droit public. Toutefois, comme défini dans celle-ci, les communes et les institutions paraétatiques, comme la Caisse de pensions, l'ECAS ainsi que l'Hôpital du Jura, sont souveraines dans l'application de la SCJU et disposent d'une large autonomie, à leur propre échelon, dans la planification et la mise en œuvre des devoirs et obligations qui y sont décrits. De même que pour le choix des sous-traitants qui hébergent et traitent leurs données.

Cela relève de leur responsabilité d'appliquer les mesures qui leur sont dévolues, et en particulier de procéder à des audits de leurs dispositifs et d'analyser les impacts en cas d'événements significatifs.

Toutefois, le Gouvernement s'appuie sur le cadre organisationnel défini par la loi relative au guichet virtuel sécurisé (LGVS), et plus précisément sur la Commission du Guichet Virtuel Sécurisé (CGVS), pour mettre à disposition des communes des compétences en cybersécurité. Ceci au travers d'un groupe de travail ayant pour vocation d'aider les communes qui le souhaitent à se mettre en conformité avec les exigences et les responsabilités de la SCJU. Ce groupe de travail est actuellement composé d'un représentant communal par district ainsi que du Responsable de la Sécurité des Systèmes d'Information (RSSI) cantonal. Il a pour mission de proposer des outils concrets pour l'application des mesures. Celles-ci sont proposées à la CGVS, qui en assure la priorisation et le suivi, et qui rapporte ensuite directement au Gouvernement.

À ce jour, trois mesures urgentes ont été identifiées par la CGVS. Il s'agit, en premier, d'un outil de sensibilisation aux risques cyber sous la forme d'un cursus de formation proposé par la Confédération. Deuxièmement, de proposer un canevas de réponse à incident sous la forme d'un guide et d'un plan établi par l'Office fédéral de la cybersécurité (OFCS), à destination spécifiquement des communes suisses. Ainsi que, troisièmement, de mettre en place les éléments nécessaires permettant d'auditer leur système d'information dans un objectif d'efficience et de mutualisation dès l'année prochaine.

Lors du Forum cyber des communes, organisé par la CGVS le 13 novembre 2025, un espace dédié à la présentation et aux échanges est consacré à la thématique de la cybersécurité. Des représentants du groupe de travail cantonal ainsi que de l'Office fédéral de la cybersécurité seront présents pour y partager leurs travaux, leurs outils et leurs compétences respectives à destination des communes.

Delémont, le 4 novembre 2025

Certifié conforme par le chancelier d'Etat
Jean-Baptiste Maître