digitalswitzerland | Waisenhausplatz 14 | 3011 Bern

Au Conseil des États exclusivement par e-mail

Prise de connaissance de la motion “Réalisation de contrôles de cybersécurité urgents et nécessaires” (24.3810)

Berne, le 13 septembre 2024

Mesdames et Messieurs les Conseillers aux Etats,

Nous partageons ci-dessous notre avis sur la motion “Réalisation de contrôles de cybersécurité urgents et nécessaires” (24.3810), sur laquelle vous voterez le 18 septembre.

Dans l'éventualité probable d'une adoption, nous souhaitons attirer l'attention, sous réserve, sur les mesures suivantes à prendre pour que la motion devienne un véritable instrument de renforcement de la cybersécurité en Suisse.

L'essentiel en bref :

- digitalswitzerland reconnaît que la cybersécurité de la Suisse doit être encore et toujours améliorée.
- Au cas où le Conseil des Etats approuverait la motion, nous demandons des précisions urgentes et nécessaires à la commission du second Conseil.
- Une approche globale de la cybersécurité nécessite une évaluation des coûts et des bénéfices, une amélioration continue, des responsabilités et des champs d'application clairs, la prise en compte des incitations économiques et l'intégration dans le contexte international, tout en évitant la bureaucratie et les charges inutiles et en garantissant la proportionnalité.

Explications :
digitalswitzerland partage l'avis de principe de la motion de renforcer la cybersécurité en Suisse. digitalswitzerland reconnaît également que la complexité croissante des cybermenaces exige des mesures robustes, y compris des audits indépendants, afin de garantir la sécurité nationale, la stabilité économique et la sécurité publique.

En même temps, digitalswitzerland souligne que les fournisseurs et les exploitants de solutions et d'infrastructures numériques remplissent déjà aujourd'hui de nombreuses obligations dans le domaine de la cybersécurité et qu'ils ont un grand intérêt à disposer de produits, d'infrastructures et de services sûrs. Les lois existantes (par exemple les dispositions sur la garantie et la responsabilité civile dans le Code des obligations, la loi sur la protection des données, la loi sur les télécommunications ou la loi sur la sécurité de l'information ainsi que leurs ordonnances d'application) ainsi que les normes et les certifications internationales jouent un rôle important à cet égard. Les organisations qui respectent déjà de telles prescriptions devraient être explicitement exclues de cette motion. La question se pose donc de savoir quels produits, services et infrastructures numériques sont encore insuffisamment contrôlés.

Afin d'améliorer durablement et de manière ciblée la cybersécurité en Suisse, digitalswitzerland propose que la motion, si elle est adoptée par le Conseil des Etats, fasse l'objet de précisions obligatoires - détaillées ci-dessous - au sein de la commission compétente du Conseil national :

1. une définition claire de l'étendue des tests

- **Définition précise du champ d'application :** il est nécessaire de délimiter clairement quels produits, infrastructures, appareils et applications numériques entrent dans le champ d'application de la motion. Il faudrait tenir compte des systèmes particulièrement critiques pour la sécurité et la fonctionnalité de la Suisse et de ceux qui sont déjà contrôlés par des réglementations, des normes ou d'autres prescriptions existantes.
- **Niveaux de criticité :** Introduire un système graduel de classification des infrastructures, des appareils et des applications en fonction de leur criticité pour la sécurité nationale, l'économie et l'ordre public. Les audits de cybersécurité devraient se concentrer en premier lieu sur les systèmes présentant une criticité élevée et très élevée.
- **Approche basée sur les risques :** développer une approche basée sur les risques qui tienne compte de la probabilité et de l'ampleur des cyber-attaques potentielles. Les audits doivent se concentrer sur les domaines à haut risque afin d'utiliser les ressources de manière efficace.
- **Exclusion de certains domaines :** Exclusion explicite de domaines déjà couverts par d'autres lois et réglementations ou pour lesquels il existe déjà des certifications et des normes de sécurité appropriées.

2. financement par des particuliers (entreprises)

- **En principe, les entreprises sont responsables de supporter elles-mêmes les coûts des audits de cybersécurité afin de protéger leurs propres systèmes :** Les audits ne devraient être effectués qu'en cas de besoin ou de demande du marché. Cela correspond à la position du Conseil fédéral de ne financer les audits étatiques que pour les acteurs étatiques. digitalswitzerland s'oppose à une obligation d'audit mandatée publiquement pour les entreprises.
- **Éviter une double charge :** Les entreprises qui respectent déjà des normes de sécurité ou des prescriptions reconnues ne doivent pas être soumises à une charge financière supplémentaire.

3. l'harmonisation avec les normes internationales

- **Équivalence des règles de l'UE :** Prise en compte et adaptation éventuelle à la législation pertinente de l'UE, comme le Cyber Resilience Act, afin d'éviter la double imposition et de faciliter les échanges avec l'UE.
- **Reconnaissance des certifications internationales :** Reconnaissance des certifications de cybersécurité reconnues au niveau international, afin de réduire la charge de travail des entreprises et d'encourager la coopération internationale.
- **Participation aux instances internationales :** Participation active de la Suisse à des instances internationales pour le développement et l'harmonisation de normes de cybersécurité.

4. autres précisions importantes :

- **Définition des “lacunes” :** définir clairement le terme “lacunes” en ce qui concerne les audits de cybersécurité afin d'affiner et de délimiter clairement l'objectif des audits.
- **Responsabilités :** Définition précise des responsabilités pour la réalisation et le financement (voir ci-dessus) des audits de cybersécurité, y compris du côté de la Confédération.
- **Évaluation et adaptation :** mise en place d'un processus d'évaluation régulier afin de vérifier l'efficacité des audits de cybersécurité et de procéder à des ajustements si nécessaire.

digitalswitzerland est prêt à participer activement à l'élaboration de ces précisions et à apporter son expertise dans les domaines de la cybersécurité et de la numérisation.

digitalswitzerland est convaincu qu'une approche collaborative permettra de renforcer la cybersécurité en Suisse sans créer de charges inutiles pour l'économie. Nous vous prions de bien vouloir peser le pour et le contre de cette décision importante. Nous restons à votre disposition pour toute question ou suggestion.

Veuillez agréer, Mesdames et Messieurs les Conseillers aux Etats, l'expression de nos salutations distinguées,

Stefan Metzger
Managing Director digitalswitzerland
stefan@digitalswitzerland.com

Guillaume Gabus
Public Affairs & Extended Management
guillaume@digitalswitzerland.com

A propos digitalswitzerland

L'échange entre l'économie, la science et la politique est au cœur du travail de digitalswitzerland. Des impulsions et des contributions concrètes doivent permettre d'exploiter les possibilités offertes par les technologies numériques. En outre, les risques qui y sont liés doivent être gérés et la confiance des gens dans les technologies doit être encouragée afin de transformer la Suisse en une nation numérique de premier plan. L'intelligence artificielle a ouvert un nouveau chapitre dans la numérisation. Les priorités particulières sont l'éducation, une infrastructure numérique digne de confiance, la cybersécurité, l'eSustainability, la santé numérique et l'eGovernment. Les défis qui en découlent sont abordés par digitalswitzerland en étroite collaboration avec ses plus de 170 membres, partenaires et autres associations.