Numérisation | Cyberadministration

Les défis de la cybersécurité pour la Suisse politique

Etat des lieux

La numérisation est le terme générique désignant l'utilisation incontournable et toujours plus répandue des technologies de l'information et de communication au sein des entreprises et de la société. Dans le cas le plus simple, la numérisation signifie le remplacement 1:1 des processus manuels ou papier par des processus informatisés. Cependant, la majorité des projets de numérisation sont destinés à améliorer les processus existants ou à en permettre de nouveaux qui étaient auparavant impossibles à mettre en œuvre ou trop coûteux.

Lorsque les processus informatisés évoluent de manière significative, les méthodes de travail individuelles, la collaboration ou même la profession et l'activité des utilisatrices et des utilisateurs qui ne possèdent généralement pas de connaissances informatiques spécifiques changent elles aussi. Dans ce contexte, il est souvent question de «transformation numérique», également pour indiquer que ces projets ne sont pas des projets purement informatiques, mais qu'ils reposent sur une interaction étroite entre l'informatique et les utilisateurs pour la définition, le développement, la réalisation et la mise en œuvre des projets spécifiques.

Des pays comme l'Estonie, la Lettonie, la Norvège et la Suède sont déjà bien avancés au niveau national et leur économie et leur administration fonctionne largement sans papier – et l'argent liquide a également été remplacé par des moyens de paiement numériques. En Suisse, l'attitude fondamentalement conservatrice de la société, les exigences élevées en matière de sécurité informatique et de protection de la vie privée ainsi que le fédéralisme fortement ancré conduisent à une approche plutôt prudente, très échelonnée et fragmentée, notamment de la part des autorités et des administrations. Des projets tels que l'identité électronique, le vote électronique ou le dossier électronique du patient sont donc controversés.

Recommandations

Une étape importante a été franchie en 2019 avec la création du poste de cyberdélégué du Conseil fédéral. Ueli Maurer, président de la Confédération à l'époque, a également présenté les objectifs du Conseil fédéral pour 2020. Ils sont conformes aux trois lignes directrices du programme de législature 2019-2023 avec, comme axes principaux, «La prospérité» (inclut entre autres le développement de la stratégie «Le numérique» et de la stratégie TIC jusqu'en 2023 ainsi que des projets de cyberadministration), «La cohésion» et «La sécurité» (inclut le combat contre les «cyberrisques» entre autres, en précisant comment augmenter la sécurité et les diminuer les abus dans le très peu contrôlé internet des objets en plein essor).

Les documents, les déclarations d'intention, la volonté de mettre en œuvre la numérisation et de fournir des services spécifiques sécurisés ne manquent pas. Toutefois, il est temps de passer rapidement à des actions concrètes. Dans ce contexte, l'Advisory Board recommande de coordonner et d'harmoniser les projets prévus malgré les structures fédérales et de prendre à temps les mesures d'accompagnement nécessaires (transparence, débat public, expérimentation contrôlée, surveillance suffisante et planification des mesures d'urgence) dans le cas de projets touchant à la sécurité de la population et de l'État.

Défis

Il est important de s'informer à temps de manière approfondie sur la thématique afin d'intervenir au bon moment et de manière documentée dans le débat en cours avec ses exigences, ses préoccupations et ses doutes. Ne pas s'en occuper du tout pour des raisons sécuritaires serait tout aussi inefficace que d'introduire de tels services sans une réflexion approfondie et une sécurité suffisante, avec les risques que cela engendre.

Les autorités, les administrations publiques, etc., doivent accorder une attention particulière au maintien permanent de la souveraineté nationale et à la sauvegarde des intérêts nationaux dans un environnement économique et politique de plus en plus concurrentiel et mondialisé.

Si ces conditions sont remplies, il n'y a aucune de raison de s'inquiéter. Ne pas profiter des opportunités offertes par la numérisation pour l'économie et la société serait plus dommageable à long terme que de prendre des risques ciblés et maîtrisés, reconnus et gérables. Le défi consistera toutefois à impliquer suffisamment toutes les parties prenantes dans un environnement fédéral et à élaborer des solutions viables et consensuelles, à les tester de manière contrôlée, à les améliorer lorsque les besoins sont identifiés et à les mettre en œuvre progressivement.

Nécessité d'agir

Il faut agir dans les domaines suivants, mentionnés selon leur niveau d'urgence:

- Une compréhension large et commune des cyberrisques par toutes les parties prenantes, basée sur les groupes de risques, les scénarios de risques et leur interaction.
- Une discussion élargie et une définition rigoureuse des fondements et des limites du maintien de la souveraineté nationale et des «frontières nationales» dans l'espace numérique.
- Une identité numérique suffisamment sûre, conforme aux directives en matière de protection des données, testée et largement acceptée et, chapeautant ces identités, une organisation pour les personnes physiques et morales adaptée à la souveraineté nationale. Ces éléments sont le fondement de la large gamme de services de cyberadministration fournis par Confédération, les cantons et les communes.
- La gestion et la planification fédérales d'un portefeuille de projets de numérisation au sein des autorités, administrations publiques et des services de cyberadministration correspondants.
- La définition, l'expérimentation et la gestion des processus nécessaires à une coopération efficace et largement acceptée entre les acteurs des secteurs public et privé dans le domaine de la numérisation afin de créer et d'exploiter les opportunités de la Suisse, lieu de formation et place économique.
- La détection précoce et la compensation ou l'exclusion des dépendances élevées inacceptables (de fournisseurs étrangers étatiques notamment) et des risques cumulatifs, y compris une planification suffisante des mesures d'urgence et d'un plan de redémarrage en cas de problèmes.

Références

- Stratégie «Suisse numérique» 2018-2020 : https://www.bakom.admin.ch/bakom/fr/page-daccueil/suisse-numerique-et-internet/strategie-suisse-numerique.html et https://www.digitaldialog.swiss/fr
- Stratégie nationale pour la protection de la Suisse contre les cyberrisques (SNPC): https://www.isb.admin.ch/isb/fr/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html

Plan de mise en œuvre de la Stratégie nationale de la protection de la Suisse contre les cyberrisques (NCS) 2018-2022: https://www.newsd.admin.ch/newsd/message/attachments/56943.pdf

Contact

Nicole Wettstein
Responsable du programme prioritaire Cybersécurité
+41 44 226 50 13

https://www.satw.ch/cybersecurity-defis

Impressum
Académie suisse des sciences techniques SATW
Contributions d'experts
Karl Aberer, EPFL | Umberto Annino, InfoGuard | Alain Beuchat, Banque Lombard Odier & Cie SA | Matthias Bossardt, KPMG | Adolf Doerig, Doerig & Partner | Stefan Frei, ETH Zürich | Roger Halbheer, Microsoft | Pascal Lamia, MELANI | Martin Leuthold, Switch | Hannes Lubich, Verwaltungsrat und Berater | Adrian Perrig, ETH Zürich | Raphael Reischuk, Zühlke Engineering AG | Riccardo Sibilia, VBS | Bernhard Tellenbach, ZHAW | Daniel Walther, Swatch Group Services | Andreas Wespi, IBM Research Lab
Rédaction et graphisme
Beatrice Huber; Claude Naville, Adrian Sulzer, Nicole Wettstein

Les opinions exprimées ici sont celles des membres du conseil consultatif sur la cybersécurité de la SATW et ne reflètent pas nécessairement la position officielle de SATW et de ses membres.

www.satw.ch
Septembre 2020