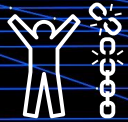


Souveraineté

Les défis de la cybersécurité pour la Suisse politique



Etat des lieux

Avec la numérisation croissante des processus opérationnels, l'importance des solutions matérielles et logicielles performantes est devenue cruciale mais aussi sensible. À première vue, le marché des fournisseurs semble être extrêmement diversifié et les solutions proposées nombreuses et variées. Toutefois, si l'on considère les pays d'origine des fournisseurs, cette diversité apparente ne l'est pas vraiment. Le marché est clairement dominé par les entreprises américaines, suivies de près par les entreprises chinoises et des acteurs mondiaux isolés de Corée (Samsung), de Russie (Kaspersky) et d'Allemagne (SAP).

Actuellement, sans les solutions matérielles et logicielles des entreprises américaines, chinoises et autres, la numérisation à large échelle des processus telle que nous la connaissons serait impossible. Cette numérisation va également de pair avec une simplification théorique de l'accès aux systèmes TIC des fabricants et prestataires indigènes et, de ce fait, aux informations stockées, traitées ou fournies, pour autant que les lois du pays d'origine de l'entreprise le permettent – ce qui se fait d'ordinaire en Chine, aux États-Unis ou ailleurs.

Un débat général sur la manière de s'affranchir de la dépendance, notamment vis-à-vis des deux géants

Defis

On peut véritablement se demander si, dans un avenir proche, la place industrielle suisse sera en mesure de développer des alternatives aux solutions matérielles et logicielles prédominantes des fournisseurs étrangers. Même une politique industrielle coordonnée dans ce secteur peu courant en Suisse n'aurait le cas échéant des effets qu'à long terme. Cependant, la numérisation des processus

Recommandations

1. Contrôle cyclique des dépendances sensibles, p. ex. pour les composants délicats des infrastructures sensibles
2. Coordination centrale du contrôle des dépendances
3. Vérification de la responsabilité du fait des produits
4. Promotion des initiatives européennes sur les dépendances sensibles et la responsabilité du fait des produits
5. Promotion de la collaboration avec les fournisseurs locaux, y compris les start-up suisses

technologiques que sont les États-Unis et la Chine, de créer une sorte d'industrie nationale indépendante et de prévoir des alternatives est en cours dans de nombreux pays dont la Suisse. En Suisse, ce débat à large échelle a été lancé sous le mot-clé «cybersouveraineté». Que faire en sachant que 99% du matériel, des logiciels et, par conséquent, de nos données et informations sont protégés non seulement par le droit suisse, mais aussi par celui d'autres nations? Cette question devrait elle aussi être abordée.

opérationnels, la «cybersanté», le développement de la 5G et d'autres initiatives similaires sont déjà en cours aujourd'hui et les composants et solutions TIC nécessaires ne sont quasiment pas produits en Suisse ou qu'en très petites quantités et à grands frais

Nécessité d'agir

En tant que petite économie ouverte, la Suisse est dépendante des fabricants TIC étrangers. D'autre part, il serait profitable à notre pays d'être en mesure de répondre aux demandes les plus variées des différents pays avec une industrie TIC de pointe adéquate. En matière de numérisation, l'économie suisse continuera à dépendre partiellement des fabricants TIC étrangers. Il convient donc d'introduire une gestion des risques cohérente qui tienne compte de l'interaction avec les fabricants, les fournisseurs et les vendeurs de solutions matérielles et logicielles en vue des éventuelles interventions étatiques et de leur mise en vigueur.

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