economiesuisse

Cybersécurité: la coopération est plus efficace que la contrainte étatique

La contrainte étatique et la surréglementation sont souvent inefficaces, surtout dans un domaine comme la cybersécurité où tous les acteurs poursuivent le même objectif. Ce qu'il faut, c'est coopérer et trouver des solutions pratiques. Il y a urgence en la matière, comme le prouve le renforcement récent de la loi sur la sécurité de l'information (LSI) par la politique fédérale. Dans leur propre intérêt, les milieux économiques soutiennent eux aussi la grande attention portée à la cybersécurité.

En matière de cybersécurité, tous les acteurs politiques, économiques et sociaux visent un intérêt commun: protéger les données sensibles et les infrastructures critiques. Malgré ces auspices harmonieux, la politique fédérale mise toujours plus sur la réglementation étatique et les mesures de contrainte, en renforçant la loi sur la sécurité de l'information (LSI) par exemple. La confiance envers les entreprises suisses semble faible. Pourtant, dans ce domaine en particulier, l'introduction d'une contrainte décrétée par l'État n'est ni une bonne idée, ni efficace. La voie vers une plus grande sécurité ne passe pas par encore plus de règles détaillées et certainement pas non plus en allant contre les entreprises. D'autres mesures, comme celles discutées actuellement en lien avec la motion 24.3810, tiennent davantage du coup de massue et causent également plus de mal que de bien.

«La politique devrait miser sur la coopération, pas sur la contrainte»

La révision de la LSI et, désormais, le projet d'ordonnance sur la cybersécurité ont montré que, dans ce domaine hautement sensible, l'État revient sans cesse à une compréhension des rôles plus nuisible que favorable. Avec les mesures de contrainte, il prend d'abord une responsabilité qu'il ne peut pas du tout assumer, crée ensuite des obstacles inutiles pour les entreprises qui investissent déjà activement dans leur sécurité et, enfin, entrave une culture positive de l'erreur. Plutôt que de miser sur la contrainte, la politique devrait adopter une approche coopérative où tous les acteurs peuvent apporter leur expertise et leurs ressources.

Il serait peu judicieux que la police vérifie la solidité des cadenas de vélos (aux frais du propriétaire) sur les râteliers à vélos et sanctionne les personnes qui utilisent des modèles jugés trop faibles. Au lieu de cela, il faudrait communiquer

clairement quels cadenas offrent quels avantages en matière de sécurité. La responsabilité demeure auprès des propriétaires, qui choisissent eux-mêmes les mesures leur semblant judicieuses. Il en va de même pour la cybersécurité: la contrainte et les sanctions à elles seules ne suffisent pas. Il est plus important que les entreprises connaissent les mesures vraiment efficaces pour protéger leurs systèmes.

L'objectif doit être de créer un cadre sûr, basé sur la confiance, la coopération et des mesures réalisables, car la cybersécurité ne peut pas être atteinte avec une mentalité «casco complète», où l'on s'attend à ce que des contrôles étatiques remédient à chaque faille. Il faut plutôt un système de clés équilibré – comme dans la vie quotidienne, où nous veillons à la sécurité de nos maisons sans les barricader complètement. C'est le seul moyen de réussir à instaurer une stratégie de sécurité efficace et durable.

La technologie dans le domaine de la cybersécurité progresse très vite et de nouvelles solutions émergent grâce à la concurrence et à l'innovation. Une surréglementation étatique pourrait freiner cette évolution et limiter la capacité d'adaptation du marché. La cybersécurité n'est pas une fin en soi ni une question pouvant être réglée avec toujours plus de dispositions législatives. Il faut une orientation pratique, de la coopération et du pragmatisme.