Aux membres du Conseil national

22.073 : Loi sur la sécurité de l'information – inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques

Proposition relative aux projets d'art. 73b ss. LSI : soutenir la minorité Zuberbühler (selon le Conseil des États)

Madame la Conseillère nationale,
Monsieur le Conseiller national,

Le 11 septembre, vous vous pencherez à nouveau sur la loi sur la sécurité de l'information (22.073). Les exploitants d'infrastructures critiques et leurs associations saluent l'introduction d'une obligation de signaler des cyberattaques. Toutefois, l'obligation de signaler des « vulnérabilités informatiques » proposée ne renforcera pas la cybersécurité et présente de graves inconvénients pour les infrastructures critiques concernées et pour les autorités. Nous vous recommandons donc de renoncer à introduire une obligation de signaler des « vulnérabilités informatiques » et vous prions de suivre le Conseil des États (minorité Zuberbühler) et de soutenir ainsi également la proposition initiale du Conseil fédéral.

Nous préconisons de renoncer à signaler des vulnérabilités pour les raisons suivantes :

1) Une collecte des vulnérabilités centralisées au niveau de l'État met en danger les infrastructures critiques plus qu'elle ne les protège (cf. les récentes cyberattaques contre les autorités fédérales Fedpol et OFAC ainsi que le site web des Chambres fédérales). D'autant plus que la liste des organismes publics et privés soumis à l'obligation de signaler est très longue (cf. projet d'art. 74b LSI) et comprend notamment toutes les autorités fédérales, cantonales et communales, les fournisseurs d'énergie, les prestataires de services financiers ainsi que les entreprises de communication ou de transport, etc.
2) Les systèmes informatiques et les évolutions intégrées dans ceux-ci étant très divers, les vulnérabilités critiques que connaissent les exploitants d'infrastructures critiques ne sont pas comparables. Signaler des vulnérabilités ne génère ainsi aucune valeur ajoutée, car les logiciels critiques peuvent varier considérablement d'un opérateur à l'autre.
3) Le signalement de vulnérabilités entraîne des charges administratives lourdes pour les organismes publics et privés soumis à l'obligation de signaler et pour l'autorité compétente (NCSC), ce qui détourne l'attention des véritables cyberattaques.
4) Il n'est pas précisé qui est responsable, en cas d'attaque réussie sur la collecte centrale et étatique des vulnérabilités signalées, pour les dommages qui en résultent.

5) L’obligation de signaler des vulnérabilités serait une spécificité helvétique, ce qui créerait une insécurité juridique et des charges administratives supplémentaires pour les entreprises actives au niveau international.

Notre position détaillée

Ces dernières années, l’opinion publique a bien pris conscience de la menace liée aux cyber-risques. En tant qu’exploitants d'infrastructures critiques, nous avons nous aussi une responsabilité et soutenons l’introduction d’une obligation de signaler les cyberattaques, comme le prévoit la modification de la loi. Une harmonisation et une coordination de l’obligation de signaler au niveau fédéral ainsi que la promotion de l’échange d’informations entre les secteurs sont positifs. Nous sommes préoccupés par une exigence que vous avez insérée dans le projet : vous demandez que les vulnérabilités des moyens informatiques critiques pour l’exploitation soient également soumises à l’obligation de signaler. Cela nous paraît contre-productif pour les raisons ci-après.

1) Réduire le risque sécuritaire et non l’accroître

Le risque est grand que l’obligation de signaler les vulnérabilités informatiques ne renforce pas la sécurité des systèmes d’infrastructures critiques, mais la mette potentiellement en danger (cf. aussi la très longue liste des organismes publics et privés soumis à l’obligation de signaler). La grande base d’informations extrêmement sensibles qui en résulterait accroîtrait les possibilités d’attaque (pour des cyberattaques à caractère politique, par exemple). Signaler des vulnérabilités informatiques et les collecter auprès d’une autorité centrale de l’État suppose ainsi que le système de sécurité de cette autorité (NCSC, par exemple) soit bien protégé. Il faut exclure totalement et à tout moment des fuites éventuelles et, si elles se produisent, elles doivent pouvoir être colmatées à tout moment et sans délai. Plusieurs incidents récents, comme les attaques contre Fedpol, l’OFAC et l’administration américaine, montrent que cette exigence est peu réaliste et difficile à satisfaire. Il serait très délicat que des informations sur la vulnérabilité informatique des infrastructures critiques en Suisse tombent entre les mains de personnes ou d’organisations avec des intentions malhonnêtes ou criminelles.

La collecte et le stockage centralisés d’informations pourraient donc exposer les points faibles des systèmes informatiques des infrastructures critiques en cas de cyberattaque contre cette autorité étatique – et, dans le pire des cas, provoquer d’autres attaques. Cela ne saurait être dans l’intérêt des infrastructures critiques ni dans celui du législateur.

2) Les systèmes informatiques ne sont pas comparables

Une gestion active des risques fait partie intégrante d’une infrastructure critique saine et des systèmes de gestion de la sécurité de l’information prescrits. Cela comprend la vérification des systèmes pour détecter d’éventuelles vulnérabilités qui pourraient être exploitées lors d’une cyberattaque. Il convient toutefois de noter que les systèmes informatiques critiques d’infrastructures critiques ne peuvent pas être comparés les uns aux autres. En raison du grand nombre de développements propres utilisés dans les infrastructures critiques ou de logiciels achetés à des tiers et adaptés pour leurs besoins, les produits ne peuvent pas être comparés. Un fournisseur d’énergie (production d’électricité et exploitation du réseau) dispose ainsi d’une infrastructure et de solutions informatiques différentes de celles des banques (système de paiement) ou des aéroports (sécurité du trafic aérien), par exemple. Même au sein des différents secteurs, les systèmes informatiques sont parfois si différents qu’il n’est ni possible ni utile de comparer des points faibles. Autrement dit, la saisie centralisée des vulnérabilités n’apporte pas ou peu de valeur ajoutée systémique.

3) Accroissement des charges et des risques

L’obligation de signaler des vulnérabilités informatiques ne tient pas compte des contraintes économiques et opérationnelles des infrastructures critiques et de l’État. Un grand nombre de points de données devraient être communiqués régulièrement. Pour ces signalements continus et l’évaluation constante des données, il faudrait créer des postes supplémentaires au sein des entreprises et de l’État. Cela risquerait de provoquer une surcharge administrative et pourrait absorber les ressources nécessaires pour lutter contre des cyberattaques graves ou accroître la cyber-résilience. Dans une telle situation, l’obligation de signaler étendue n’offre aucune valeur ajoutée aux entreprises utilisatrices, ni pour le NCSC ni pour les infrastructures critiques.

4) Question de responsabilité

Du point de vue des exploitants d'infrastructures critiques, la collecte centralisée de vulnérabilités dans un service étatique accroît le risque de divulgation d'informations sensibles en cas de fuite ou de cyberattaque réussie. Celles-ci peuvent provoquer à leur tour d'autres cyberattaques contre des infrastructures critiques, qui ont le potentiel de causer des dommages étendus à notre pays. Il n'est pas précisé qui est responsable dans de tels cas et si l'État est prêt à assumer la responsabilité des dommages occasionnés. En effet, si les vulnérabilités sont signalées à un organisme étatique central, l'État doit également s'assurer qu'elles sont strictement protégées.

5) « Swiss finish »

La décision d'étendre l'obligation de signaler des vulnérabilités de systèmes informatiques des infrastructures critiques serait une spécificité suisse. Une multitude d'entreprises actives à l'échelle internationale devraient distinguer les prescriptions nationales et internationales, ce qui créerait une incertitude juridique et entraînerait des charges administratives supplémentaires.

Notre position sur la proposition de la majorité de la CPS-N relative au projet d'art. 74d al. 2 LSI

Lors de sa séance de juin, la majorité de la CPS-N a introduit une modification qui exclut le signalement de vulnérabilités touchant des développements propres. Pour les exploitants d'infrastructures critiques, même avec cette adaptation, la loi n'atteint pas l'objectif visé et crée de nouvelles incertitudes juridiques.

1) On ne peut pas dire précisément ce qui peut être qualifié de développement propre ou pas, notamment en ce qui concerne les produits tiers achetés et les logiciels standard qui sont adaptés et intégrés dans l'infrastructure informatique propre.
2) Les infrastructures critiques ne sont souvent pas en mesure de signaler les vulnérabilités de produits de tiers en raison des dispositions contractuelles et, surtout, du secret professionnel.
3) Des vulnérabilités peuvent être découvertes dans des produits open source. On peut se demander ce que ferait le NCSC du signalement d'une telle vulnérabilité et donc quelle serait la valeur ajoutée d'un tel signalement.
4) Il n'est pas non plus clair si des fabricants de logiciels qui découvrent des vulnérabilités dans leurs produits seraient également soumis à une obligation de signaler.

On voit que la formulation actuelle accroît les risques et produit donc l'effet contraire à celui visé par le projet initial du Conseil fédéral.

Pour conclure, nous tenons à préciser que les représentants d'infrastructures critiques ont réagi positivement à la proposition du Conseil fédéral lors de la consultation. L'extension de l'obligation de signaler des vulnérabilités informatiques n'a pas été soumise aux acteurs concernés par la loi. Les organisations signataires se tiennent à votre disposition pour montrer comment gérer les cyber-risques et vulnérabilités informatiques en tenant compte des risques. Le cyberespace étant sans frontières et les menaces provenant du monde entier, les infrastructures critiques ont un intérêt intrinsèque à se protéger au mieux contre les cyberattaques. Au vu des arguments ci-dessus et des réserves liées à la sécurité, l'utilité d'une obligation de signaler les vulnérabilités n'est pas manifeste. Au contraire, le risque existe que l'État dispose ainsi d'une collecte centralisée d'informations extrêmement sensibles, dont des personnes non autorisées pourraient faire un mauvais usage.

Pour ces différentes raisons, nous vous recommandons de renoncer à ancrer dans la LSI l'obligation pour les exploitants d'infrastructures critiques de signaler des vulnérabilités informatiques et donc de suivre la minorité Zuberbühler et le Conseil des États.

Nous vous remercions de l'attention que vous voudrez bien accorder à nos préoccupations et vous prions d'agréer, Madame la Conseillère nationale, Monsieur le Conseiller national, l'assurance de notre haute considération.

Exploitants d'infrastructures critiques