economiesuisse

→ Prise de position sur la réglementation concernant la gestion des cyberrisques

LA SUISSE FAIT FACE À UNE DIVERSIFICATION CROISSANTE DES CYBERMENACES SOPHISTIQUÉES. LES ATTAQUES CIBLANT DE MOYENNES ENTREPRISES ET DE GRANDS GROUPES CAUSENT CHAQUE ANNÉE DES DOMMAGES CONSIDÉRABLES ET PEUVENT PARALYSER DES CHAÎNES DE PRODUCTION ENTIÈRES. DES INFRASTRUCTURES CRITIQUES – NOTAMMENT DANS LES DOMAINES DE L'ÉNERGIE, DES TRANSPORTS ET DE LA SANTÉ –, EN PARTICULIER, SONT DANS LE VISEUR DE GROUPES CRIMINELS QUI EXPLOITENT DE MANIÈRE CIBLÉE DES FAIBLESSES POUR MENACER LA SÉCURITÉ D'APPROVISIONNEMENT ET L'ORDRE PUBLIC.

Situation actuelle

→ Les cyberattaques sont en constante évolution. Leurs auteurs adaptent continuellement leurs méthodes – rançongiciels (« ransomware », en anglais), phishing et autres techniques. En utilisant de nouvelles technologies et des outils automatisés, les entreprises sont parvenues à réduire de plus en plus le délai nécessaire pour identifier et combler des failles de sécurité. La pression est élevée : les faiblesses doivent donc être identifiées, évaluées et corrigées avant qu'elles ne soient exploitées[1].

→ Bien comprendre les menaces actuelles est indispensable. Seules une connaissance fondée des cyberrisques permettra de protéger efficacement les infrastructures de communication et d'information en Suisse et au-delà[2].

→ La gestion des cybermenaces nécessite une action commune appropriée.

CONTACT

ERICH HERZOG
Membre de la direction et responsable du département Concurrence et réglementation
erich.herzog@economiesuisse.ch

ANGELA ANTHAMATTEN
Responsable suppléant du département Concurrence et réglementation
angela.anthamatten@economiesuisse.ch

BASILE DACOROGNA
Responsable adjoint du bureau romand et chef de projets Concurrence et réglementation
basile.dacorogna@economiesuisse.ch

1 Cf. par exemple : Office fédéral de cybersécurité (OFCS) – Cybersécurité – La situation en Suisse et sur le plan international, Rapport semestriel 2024/II (juillet-décembre), p. 7 ss. [cit. « BACS »]
2 OFCS, p. 5

Joindre ses forces plutôt que se méfier les uns des autres

Une économie numérique solide nécessite un partenariat étroit et égalitaire entre l'État et les entreprises. Face à des cybermenaces de plus en plus complexes et dynamiques, des réglementations rigides sont insuffisantes. Nous avons au contraire besoin d'un cadre légal flexible qui permette aux entreprises de réagir rapidement et efficacement à de nouvelles menaces. Ce cadre flexible devrait être complété par une autorégulation sectorielle et des recommandations pratiques – afin de garantir la capacité à innover et l'excellence des normes de sécurité à long terme.

Position des milieux économiques :

- **Partenariat d'égal à égal avec l'État :** La collaboration doit s'appuyer sur la confiance réciproque, une gestion des erreurs constructive et les forces communes. L'État doit être un partenaire actif de la responsabilité commune en matière de cybersécurité et non se positionner comme une instance de contrôle.

- **Un cadre réglementaire efficace et équilibré plutôt qu'une répartition unilatérale des charges :** Les entreprises ont besoin de protection face aux risques de cyberattaque – mais elles ne doivent pas porter cette responsabilité seules et leur capacité à innover ne doit pas être restreinte par des exigences excessives. Il faut élaborer un cadre réglementaire équitable et pragmatique.

Le caractère dynamique de la menace appelle une réglementation adaptative

- **Des garde-fous fondés sur des principes plutôt que des prescriptions rigides :** Des réglementations légales rigides ne permettent pas de se protéger des cyberrisques. Il faut une approche coopérative fondée sur la flexibilité, la responsabilité individuelle et la confiance réciproque.

- **Une autorégulation sectorielle renforcée** est cruciale pour permettre la flexibilité, l'agilité et donc une cybersécurité efficace. L'État doit reconnaître les structures existantes, les encourager et les intégrer systématiquement dans le cadre réglementaire.

- **Des bases de données fiables et des échanges d'informations :** Pour l'État et l'économie, une analyse commune de la situation est décisive. Une protection efficace contre les cybermenaces nécessite un flux d'informations continu et bidirectionnel – en particulier avec la mise à disposition de données agrégées ou anonymisées par les autorités publiques.

- **Des incitations plutôt que sur des sanctions – responsabiliser au lieu de décourager :** Une culture sécuritaire constructive ne se développe que si les entreprises peuvent agir sans craindre des conséquences disproportionnées. Les sanctions administratives ou pénales devraient punir les fautes délibérées uniquement – c'est le seul moyen de promouvoir une gestion des erreurs ouverte et tournées vers l'apprentissage.

Spécificités de la réglementation concernant les cyberrisques

- Il n'est pas possible de venir à bout des cyberrisques à coup de réglementation. Sachant qu'aucune entreprise n'aspire à connaître une cyberattaque – ce qui explique l'intérêt naturel de l'économie pour la prévention –, il est d'autant plus important d'encourager et de prendre en compte systématiquement les mesures de prévention au niveau de la réglementation.

- Des exigences fixes en matière de sécurité ne sont pas réalistes. Les menaces évoluent constamment et à grande vitesse. Les réglementations doivent refléter cette réalité – en misant sur des approches adaptatives et ouvertes aux technologies plutôt que sur des règles rigides.

- Une réglementation très stricte crée de nouveaux risques. Elle peut certes offrir une sécurité juridique formelle à court terme (conformité), mais elle entrave des processus d'innovation et le développement agile de mesures de défense contre des cybermenaces. Il faut éviter que des prescriptions rigides deviennent un risque sécuritaire.

Les législations doivent

- être flexibles et tournées vers l'avenir, afin de permettre aux entreprises de faire face aux nouvelles menaces et de réagir de manière adéquate aux progrès technologiques (évolutions autour de l'IA et de la technologie quantique, par exemple) sans risquer d'enfreindre la législation en vigueur ;

- se limiter à des règles générales fondées sur des principes. L'autorégulation et des recommandations sectorielles compléteront ce dispositif afin de maintenir l'agilité nécessaire.

Développer le soutien de l'État, au lieu d'étendre la surveillance

L'État doit

- renforcer de manière ciblée les ressources techniques, car une protection efficace contre les cybermenaces suppose un système d'alerte précoce solide soutenu par l'État. Des ressources techniques et humaines suffisantes doivent être mises à disposition pour cela ;

- promouvoir un partenariat étroit avec les entreprises, car un dialogue continu et fondé sur la confiance entre les pouvoirs publics et les entreprises est essentiel pour identifier, classer et gérer ensemble les différents cyberrisques de manière efficace.

Cette collaboration permet

- le développement de normes de sécurité communes, car les connaissances de l'État sont associées à la pratique des entreprises, ce qui ouvre la voie à la création de normes efficaces et pragmatiques ;

- l'intensification des échanges d'informations, sachant que des échanges d'informations rapides et complets sur les menaces et les incidents sont essentiels. Cela vaut en particulier pour l'État, qui doit mettre de telles informations à la disposition de l'économie sous une forme agrégée ou anonymisée. Le soutien de l'État sous la forme de formations et de plateformes d'information renforce les capacités des entreprises en matière de cybersécurité ;

- l'échange de bonnes pratiques, car un dialogue continu favorise les échanges sur des procédures éprouvées et des solutions innovantes en matière de cyberdéfense ;

- une forte réactivité, car des groupes de travail et des commissions communs permettent des adaptations rapides aux nouvelles menaces et aux évolutions technologiques ;

- la promotion de partenariats public-privé (PPP), grâce auxquels des projets communs font progresser le développement et la mise en œuvre de solutions avancées en matière de sécurité.