Envoi électronique
ncsc@gs-efd.admin.ch

swissuniversities

Comité de swissuniversities

Luciana Vaccaro
Présidente
T +41 31 335 07 40
luciana.vaccaro@
swissuniversities.ch

swissuniversities
Effingerstrasse 15, Case Postale
3001 Berne
www.swissuniversities.ch

3001 Berne, le 13 septembre 2024

Prise de position de swissuniversities concernant le projet d'ordonnance sur la cybersécurité

Madame, Monsieur,

Nous vous remercions de la possibilité qui nous est offerte de prendre position sur le projet d'ordonnance sur la cybersécurité (OCyS).

swissuniversities est favorable à l'augmentation de la transparence concernant les cyberattaques et soutient en principe le projet d'ordonnance. Nous sommes en effet convaincu·es qu'une meilleure information sur la situation de la menace, les scénarios d'attaque concrets et les expériences tirées des stratégies de défense mises en place bénéficiera à tous les acteurs et contribuera à une augmentation de la cybersécurité en Suisse.

Nous considérons cependant que le regroupement de toutes les hautes écoles sous le terme "hautes écoles" à l'art. 74, al. 1, let. a de la Loi sur la sécurité de l'information (LSI) est trop peu différencié en ce qui concerne la cybersécurité et l'obligation de déclaration. Des valeurs seuils, telles que proposées dans le Message relatif à la modification de la loi sur la sécurité de l'information du 2 décembre 2022 devraient également être introduites pour les hautes écoles (voir ci-après notre suggestion d'exception à l'obligation de signaler). En effet, ledit message prévoit que le Conseil fédéral fixe des exceptions à l'obligation de signaler au sein de certains domaines au moyen de valeurs seuils, et qu'il est donc tenu de veiller à la proportionnalité de l'obligation de signaler en exemptant les organisations qui ne sont pas essentielles pour le fonctionnement de l'économie ou pour le bien-être de la population, comme prévu à l'art. 74c.

Par ailleurs, nous relevons dans notre commentaire ci-après des différents articles de l'ordonnance plusieurs éléments, notamment concernant la représentation des hautes écoles dans les instances qui seront créées, les liens avec les services existants de Switch, le potentiel de coordination que cette organisation offre pour les hautes écoles. Divers autres aspects y sont également abordés et nous vous prions de les considérer.

swissuniversities

Finalement, nous souhaitons relever encore deux points :

- L'introduction d'une obligation de déclaration n'est pas neutre en termes de coûts pour les hautes écoles. Il conviendra de déterminer qui prendra en charge les coûts supplémentaires.
- La création d'un registre contenant des informations sur les incidents de sécurité, les dispositifs de sécurité et les points faibles des composants d'infrastructure comporte le risque que les données collectées soient rendues publiques ou accessibles à des cercles cybercriminels en cas de fuite de données. Différentes obligations de notification (par exemple, par le biais de réglementations cantonales) existent déjà et fonctionnent avec différents délais d'annonce. Nous recommandons de tenir compte de cette situation de départ dans la perspective de la nouvelle ordonnance et de prévoir une réglementation aussi uniforme que possible.

Nous vous remercions par avance de la prise en compte de notre position, nous tenons bien volontiers à disposition pour toute précision et vous prions d'agréer, Madame, Monsieur, nos salutations les meilleures.

Dr Luciana Vaccaro
Présidente de swissuniversities

Commentaire des différents articles de l'ordonnance

Art. 4 Composition du CP CSN
En tant que faîtière des hautes écoles suisses, swissuniversities se tient à disposition pour la recherche d'une représentation adéquate des hautes écoles au sein du CP CSN. À ce sujet, le rôle de Switch devra également être clarifié.

Art. 7 Analyse technique des cyberincidents et des cybermenaces
Switch gère également une CERT pour les hautes écoles. La collaboration entre la CERT de l'OFCS, celle de Switch et les organisations de cybersécurité existantes des hautes écoles doit être réglée. Les doublons doivent être évités et Switch pourrait se charger de la coordination, en particulier pour les hautes écoles qui n'ont pas d'organisation spécifique de cybersécurité.

Art. 8 Priorités pour les conseils et l'assistance en cas de Cyberattaque
Si, en cas de cyberattaque, les demandes de conseils et d'assistance dépassent les capacités de l'OFCS, Switch pourrait soulager l'OFCS pour les hautes écoles.

Art. 10 Soutien aux autorités
Il s'agit de vérifier ici si les hautes écoles ne devraient pas également pouvoir bénéficier de ce soutien.

Art. 12 Systèmes d'information permettant l'échange automatique
Les hautes écoles profiteraient grandement de l'obtention d'informations sur les menaces actuelles (Threat Intelligence) directement auprès de l'OFCS ou via Switch et de leur utilisation pour la détection.

swissuniversities

Art. 13 Enregistrement
Les hautes écoles ont un intérêt à pouvoir s'enregistrer dès que possible. Elles se tiennent également à disposition pour tout éventuel pré-enregistrement. Une éventuelle coordination par Switch doit également être examinée.

Art. 16 Exceptions à l'obligation de signaler
Des valeurs seuils ont été définies pour d'autres institutions, cela devrait donc également être le cas pour les hautes écoles. En effet, les exigences et la charge de travail pour satisfaire à l'obligation de déclaration sont proportionnellement bien plus élevées dans les petites hautes écoles et sont difficiles à maîtriser. Des ressources limitées rendent difficile la mise en place des processus nécessaires dans le domaine de la cybersécurité ou l'obtention de ressources supplémentaires pour ce thème. En outre, certaines hautes écoles n'exploitent et n'entretiennent pas leurs propres systèmes et font appel à des prestataires de services (p. ex. fournisseurs de cloud). Par ailleurs, les instances cantonales pourraient vraisemblablement se charger de transmettre les messages de la haute école à l'OFCS.

Une possibilité consisterait à introduire une exception supplémentaire à l'alinéa 1, comme suit :

Les hautes écoles au sens de l'art. 74b, al. 1, let. a, LSI : qui
1. n'exploitent pas leur propre système de communication ou
2. n'exploitent pas leur propre centre de calcul ou
3. comptent moins de 2000 étudiant·es et/ou moins de 500 collaborateurs·trices employés en EQTP (selon la statistique actuelle de l'OFS) ou
4. les hautes écoles sans système de recherche propre ou
5. qui sont soumises à une obligation cantonale de déclaration.

Art. 18 Cyberattaques à signaler
Les annonces des hautes écoles à l'OFCS devront être coordonnées avec SWITCH CERT et une concertation entre les deux entités sera nécessaire à cet effet.

Art. 20 Transmission du signalement
Il devrait être possible pour une entreprise ou plusieurs entreprises de décider conjointement de notifier les incidents par l'intermédiaire d'un organisme tiers spécialisé qui prenne également en charge la notification des incidents, par exemple un MSSP (Managed Security Service Provider), un CERT sectoriel, un ISAC (Information Sharing and Analysis Center) sectoriel et d'autres.... Nous suggérons donc de compléter l'article 20 OCyS par un alinéa supplémentaire :
[2] Une ou plusieurs autorités ou organisations soumises à l'obligation de notification peuvent décider de sous-traiter le processus de notification, individuellement ou collectivement, à une organisation tierce spécialisée.

Art. 21 Délai de saisie du signalement
Les exigences relatives au délai d'annonce de 24 heures posent des défis importants aux petites hautes écoles en ce qui concerne la maturité des processus existants ainsi que le personnel engagé ou nécessaire. Une adaptation de ces processus nécessitera vraisemblablement des moyens financiers supplémentaires, qui devront être libérés par les processus et les instances nécessaires.