Département de la défense, de la protection de la population et des sports (DDPS)
Office fédéral de la cybersécurité (OFCS)
Schwarztorstrasse 59
CH-3003 Bern

Soumission par courriel à:
ncsc@ncsc.admin.ch

Zurich, le 13 septembre 2024

Objet: Réponse à la consultation concernant l'Ordonnance sur la cybersécurité (OCys)

Madame la Conseillère fédérale Amherd,
Monsieur Suter,

Nous vous remercions de nous avoir donné l'occasion de nous exprimer dans le cadre de la consultation sur l'Ordonnance sur la cybersécurité (OCys), que nous saisissons ici au nom de digitalswitzerland.

digitalswitzerland se félicite de la précision apportée aux procédures de déclaration des cyberattaques sur les infrastructures critiques, telles que stipulées dans la nouvelle loi LSI. Bien que le projet soit extrêmement clair et compréhensible, nous nous permettons de proposer quelques modifications concrètes (indiquées en jaune) :

Art. 4: Composition du CP CSN

Nous soutenons la création d'un comité de pilotage de la Cyberstratégie nationale (CP CSN), mais nous proposons d'inclure également des représentants des infrastructures critiques dans sa composition. La formulation « représentants de l'économie » n'est pas suffisamment précise à cet égard.

***Art. 4, al. 1** : Le CP CSN se compose de représentants des départements, de la Chancellerie fédérale, des cantons, de l'économie, **notamment des exploitants d'infrastructures critiques**, de la société et des hautes écoles.*

Art. 9: Divulgation cordonnée des vulnérabilités

L'article 9, alinéa 1 stipule que la divulgation des vulnérabilités doit se faire selon des normes internationalement reconnues, bien que celles-ci ne soient pas encore suffisantes.[1] Pour combler cette lacune, les bonnes pratiques doivent également être prises en compte.

La proposition de modification est la suivante :

[1] CERT/CC inclue, par exemple, une politique et un guide. D'autres exemples sont le OWASP Vulnerability Management Guide ou le NIST SP 800-53. FIRST a développé des normes pour la coordination et la divulgation des vulnérabilités, voir ici, ici et ici.

Art. 9, al. 1: Le OFCS veille à coordonner la divulgation des vulnérabilités selon les normes internationales reconnues ***et aux bonnes pratiques.***

La formulation proposée dans la OCys ne couvre pas le domaine des "processus" ou des configurations des services numériques. Les vulnérabilités dans ce domaine ne concernent pas directement des problèmes de matériel informatique ou de logiciel, mais plutôt des configurations incorrectes ou une utilisation inappropriée des services. Des exemples récents de tels cas incluent :

- Une vulnérabilité dans l'authentification permettant aux criminels de contourner la vérification par e-mail nécessaire à la création d'un compte sur un environnement de travail basé sur le cloud.
- Un conteneur Docker public contenant un jeton d'accès GitHub.[2]
- Des indices sur des installations militaires secrètes en raison de l'utilisation des services de localisation par des employés.[3]

Nous proposons donc la modification suivante :

Art. 9, al. 2 : Il fixe ***au responsable du matériel informatique, du logiciel ou des services concernés*** ~~*dispose d'*~~*un délai de 90 jours pour éliminer les vulnérabilités.*

Art. 11: Système de communication permettant l'échange sécurisé d'informations

Tous les opérateurs d'infrastructures critiques dans le pays, y compris ceux sans siège social en Suisse, devraient avoir la possibilité de participer à l'échange d'informations (Art. 74 mod. LSI). Pour les entreprises globales, l'échange transfrontalier est de première importance.

Nous proposons donc la modification suivante :

Art. 11, al. 1 : Les autorités et les organisations dont le siège est en Suisse, ***ou celles admises par l' OFCS à l'échange d'informations et répondant aux exigences définies par celui-ci,*** *ont accès au système de communication de l' OFCS permettant l'échange sécurisé d'informations (art. 74, al. 2, let. a LSI).*

Art. 13 Enregistrement

La formulation actuelle implique une responsabilité de la personne signalée, alors qu'il s'agit selon le message simplement d'une personne de contact. La formulation devrait donc être modifiée en « Informations sur une ou plusieurs personnes de contact ».

Nous proposons donc la modification suivante :

Art. 13, al. 2, lettre b: ~~*coordonnées de la personne ayant procédé à l'enregistrement.*~~ ***Informations sur une ou plusieurs personnes de contact.***

[2] Voir: https://www.schneier.com/blog/archives/2024/08/leaked-github-python-token.html

[3] Voir:: https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/

Art. 18 Cyberattaques à signaler

Nous suggérons de prendre en compte la gravité d'une cyberattaque dans l'obligation de déclaration. Cela permettrait d'éviter une charge administrative excessive. Nous souhaitons éviter que, par exemple, de brèves interruptions du système affectant un nombre limité de personnes doivent être signalées. Les règles de conformité sectorielles[4] existantes tiennent déjà compte de la gravité.

Nous proposons donc les modifications suivantes pour harmoniser l'ordonnance avec d'autres réglementations:

Art. 18, al. 1, lettre a : « des collaborateurs ou des tiers sont touchés par des interruptions des ***systèmes critiques causées par des cyberattaques, qui mettent en danger le fonctionnement stable de l'infrastructure, ou****... »*

Art. 18, al. 2, lettre a : « Les informations importantes ***et critiques*** *pour les affaires ... publiées,* ***volées, détruites, désactivées ou autrement manipulées, affectant les applications ou systèmes essentiels à moyen ou long terme*** *.. par des personnes non autorisées;»*

Nouvelle insertion en al. 2, lettre b : ***« L'intégrité des processus commerciaux est affectée, ou »***

Une gradation ou une définition de la gravité serait également utile pour le flux d'informations. La publication d'un document non problématique ne pèse pas aussi lourd que la divulgation de données sensibles confidentielles au grand public.

Art. 19 Contenu du signalement

Dans le cadre du signalement, des informations sur l'agresseur de la cyberattaque doivent également être fournies. Cela implique des procédures judiciaires complexes, relevant du domaine de la justice pénale, et non des entreprises.

Nous proposons donc la modification suivante :

Art. 19, al. 1, lettre e: les données sur l'agresseur, ***si elles peuvent être déterminées sans procédures judiciaires complexes.***

Art. 20 Transmission du signalement

L'article semble concerner un signalement effectué par un tiers qui n'est pas soumis à l'obligation de déclaration et qui concerne une organisation enregistrée. La formulation proposée entraînerait la divulgation des coordonnées de la personne effectuant le signalement à l'organisation soumise à l'obligation, conformément à l'article 19, al. 4, lettre b. Cela pourrait constituer un obstacle aux signalements anonymes, car des personnes ou organisations non soumises à l'obligation pourraient souhaiter rester anonymes, ce qui ne serait pas possible dans ce cas.

[4] FINMA 05/2020, voir: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20200507-finma-aufsichtsmitteilung-05-2020.pdf

Nous proposons donc les modifications suivantes :

Art. 20: Dans le cas où le signalement n'est pas transmis au moyen du système de communication de l' OFCS, ce dernier informe la personne de contact visé à l'article 13, al. 2, lettre b ***d'une organisation enregistrée et concernée par le signalement*** *de la réception et du contenu du signalement,* ***sans toutefois divulguer les coordonnées de l'organisation ou de la personne effectuant le signalement, sauf si ces coordonnées sont nécessaires à la protection de la cybersécurité.***

Observations supplémentaires

Nous souhaitons également profiter de cette occasion pour soulever quatre points supplémentaires, en lien avec les objectifs de l'LSI et de la OCys, qui préoccupent l'industrie numérique :

Coordination de l' OFCS

L'objectif doit être que les acteurs soumis à l'obligation de déclaration fassent leurs signalements à une seule autorité. L' OFCS joue un rôle central de coordination en ce qui concerne l'obligation de déclaration. Nous suggérons que l' OFCS reçoive tous les incidents soumis à l'obligation de déclaration et les coordonne ensuite avec les autres autorités compétentes. Un point de contact unique évite les efforts supplémentaires et les doublons. Nous pouvons également envisager que les autorités à contacter (FINMA, PFPDT, OFCS) se coordonnent entre elles.

Comportement de déclaration des vulnérabilités

Indépendamment des prescriptions légales de déclaration, pour digitalswitzerland et ses membres, une culture de déclaration proactive et ouverte des vulnérabilités cyber est d'une grande importance. L'article 9 sur la révélation coordonnée des vulnérabilités donne la bonne direction, mais précise uniquement les obligations de l'OFCS envers les fabricants de matériel, de logiciels et les diverses autorités. Il est également nécessaire d'inciter l'industrie à promouvoir un comportement de déclaration proactive. Les mesures et outils visant à augmenter les déclarations volontaires devraient être développés, continuellement testés et améliorés en collaboration avec l'industrie.

Priorisation des déclarations

L'article 8, alinéa 2, fixe la priorisation des signalements en fonction des intérêts publics. Une liste de critères spécifiques ou une gradation des scénarios de dommages concrets, selon laquelle l'établissement des priorités est faite, serait une aide précieuse pour l'industrie numérique.[5] digitalswitzerland a déjà suggéré une catégorisation claire dans sa réponse à la consultation sur la nouvelle loi militaire (notamment Art. 95) concernant une « situation exceptionnelle en temps de paix concernant les menaces cyber ».[6]

[5] Dans le cadre du débat en cours sur la souveraineté numérique, la Swiss Data Alliance apporte des approches utiles pour une évaluation possible d'un scénario de dommages. Voir (en allemand): https://www.swissdataalliance.ch/publikationen/whitepaper-digitale-souveraenitaet

[6] Voir la réponse de consultation de digitalswitzerland concernant la révision de la Loi sur l'armée (art. 95) https://digitalswitzerland.com/wp-content/uploads/2024/03/digitalswitzerland_-Consultation-sur-la-loi-militaire_FR.pdf

Confiance par la fiabilité

Enfin, nous voyons dans l'ordonnance sur la loi sur la sécurité de l'information un pas important vers la promotion d'une infrastructure numérique fiable pour la Suisse. Des procédures de déclaration fiables et rapidement applicables par l'industrie en cas de cyberattaque en sont un pilier fondamental. digitalswitzerland est convaincu que ces éléments façonneront de manière déterminante le succès de la numérisation en Susse sur les prochaines années et se tient à la disposition de l'Office fédéral de la cybersécurité pour dialoguer sur ces questions.

Nous vous remercions de prendre connaissance de ces points,d'examiner et de considérer nos préoccupations avec bienveillance.

Veuillez agréer, Madame la Conseillère fédérale Amherd, Monsieur Suter, l'expression de nos salutations distinguées.

Stefan Metzger
Managing Director digitalswitzerland
stefan@digitalswitzerland.com

Guillaume Gabus
Public Affairs & Management
guillaume@digitalswitzerland.com

---

*L'échange entre l'économie, le milieu académique, les organisations publiques et la politique est au cœur du travail de **digitalswitzerland**. Par le biais d'impulsions et de contributions concrètes, les opportunités offertes par les technologies numériques doivent être exploitées. Par ailleurs, les risques associés doivent être gérés et la confiance du public dans ces technologies renforcée, afin de faire de la Suisse une nation numérique de premier plan.*

Avec l'intelligence artificielle, un nouveau chapitre de la transformation numérique s'est ouvert. Les priorités particulières incluent l'éducation, une infrastructure numérique de confiance, la cybersécurité, l'eSustainability, la santé numérique et l'eGovernment. Les défis associés à ces domaines sont abordés par digitalswitzerland en étroite collaboration avec ses plus de 170 membres, partenaires et autres associations.