Ordonnance sur la cybersécurité (OCyS)

du …

Le Conseil fédéral suisse,

vu les art. 74*c* et 84, al. 1, de la loi fédérale du 18 décembre 2020 sur la sécurité de l'information (LSI)[1],

arrête:

Section 1 Objet

Art. 1

La présente ordonnance règle:

a. les grandes lignes et l'élaboration de la Cyberstratégie nationale (CSN);

b. les tâches de l'Office fédéral de la cybersécurité (OFCS);

c. l'échange d'informations entre l'OFCS et les autorités ou organisations chargées de la protection contre les cyberincidents et les cybermenaces;

d. l'obligation de signaler les cyberattaques.

Section 2 Cyberstratégie nationale

Art. 2

[1] La CSN définit les points suivants:

a. le cadre stratégique de la prévention dans le domaine de la cybersécurité;

b. la détection précoce des cybermenaces;

c. les possibilités de réaction et la résilience en cas d'incident;

d. la lutte contre la cybercriminalité;

1 RS **128**

e. la coopération internationale.

[2] L'OFCS élabore la CSN en collaboration avec des représentants des cantons, de l'économie, des exploitants d'infrastructures critiques, des milieux scientifiques, de la société, des départements et de la Chancellerie fédérale.

Section 3 Tâches de l'OFCS

Art. 3 Demande de renseignements sur les titulaires de nom de domaine

Afin d'avertir les autorités, les organisations ou les personnes concernées en cas de cybermenace imminente ou de cyberattaque en cours, l'OFCS peut requérir les coordonnées des titulaires de noms de domaine auprès de l'exploitant du registre des noms de domaine qui relèvent de la compétence de la Confédération.

Art. 4 Analyse technique des cyberincidents et des cybermenaces

[1] L'OFCS gère une équipe nationale d'intervention en cas d'urgence informatique, qui assume notamment les tâches suivantes:

a. le soutien dans la gestion technique des cyberincidents;

b. l'analyse des questions techniques;

c. l'identification et l'évaluation des cybermenaces.

[2] Il exploite une infrastructure résiliente et indépendante du reste de l'informatique fédérale pour analyser les cyberincidents et les cybermenaces.

Art. 5 Priorités pour les conseils et l'assistance en cas de cyberattaque

[1] En cas de cyberattaque, l'OFCS peut établir des priorités concernant le délai et l'étendue de ses conseils et de son assistance lorsque les demandes dépassent ses capacités.

[2] Il prend alors en compte les impératifs de la sécurité et de l'ordre publics, du bien-être de la population et du fonctionnement de l'économie.

Art. 6 Annonce des vulnérabilités

[1] L'OFCS veille à ce que les vulnérabilités du matériel et des logiciels soient annoncées de manière coordonnée en tenant compte des normes internationalement reconnues.

[2] Il fixe au fabricant du matériel informatique ou du logiciel concerné un délai de 90 jours pour éliminer les vulnérabilités.

[3] Il peut raccourcir ce délai si la vulnérabilité

a. met en péril le fonctionnement d'infrastructures critiques;

b. concerne des systèmes très répandus, ou

c. est exploitée pour une cyberattaque ou peut être très facilement utilisée à cette fin.

[4] Il peut prolonger le délai lorsque l'élimination de la vulnérabilité s'avère particulièrement compliquée.

[5] Il peut informer les exploitants d'infrastructures critiques de la présence de vulnérabilités avant même l'annonce ou l'élimination de celles-ci.

[6] Il informe immédiatement l'Office fédéral de la communication (OFCOM) des vulnérabilités relatives aux installations de télécommunication au sens de l'art. 3, let. d, de la loi du 30 avril 1997 sur les télécommunications[2].

[7] Les al. 1 à 4 ne s'appliquent pas aux vulnérabilités que l'OFCOM découvre et annonce à l'OFCS dans le cadre de ses contrôles de surveillance (art. 36 ss de l'ordonnance du 25 novembre 2015 sur les installations de télécommunication[3]).

Art. 7 Soutien aux autorités

L'OFCS soutient les autorités de la Confédération et des cantons dans le développement, la mise en œuvre et l'examen de normes et de réglementations dans le domaine de la cybersécurité.

Section 4 Échange d'informations

Art. 8 Système de communication pour l'échange sécurisé d'informations et systèmes d'échange automatique d'informations

[1] Les exploitants d'infrastructures critiques soumis à l'obligation de signaler les cyberattaques, les organisations ayant leur siège en Suisse et les autorités ont accès au système de communication pour l'échange sécurisé d'informations de l'OFCS.

[2] L'OFCS met à la disposition des exploitants d'infrastructures critiques les informations techniques visées à l'art. 74, al. 2, let. b, LSI, concernant les cybermenaces et les cyberincidents au moyen d'un système d'échange automatique d'informations.

[3] Il est responsable de la sécurité du système de communication et des systèmes d'information ainsi que de la légalité du traitement des données.

Art. 9 Enregistrement

[1] Les organisations et les autorités sont tenues de s'enregistrer avant de pouvoir utiliser le système de communication. Elles doivent communiquer sans délai toute modification de leurs données.

[2] L'enregistrement doit au moins comporter les informations suivantes:

a. la raison sociale, le nom ou la désignation et l'adresse de l'organisation ou de l'autorité;

2 RS **784.10**
3 RS **784.101.2**

b. la personne de contact.

Art. 10 Fournisseurs de prestations de cybersécurité

[1] Les exploitants d'infrastructures critiques peuvent annoncer à l'OFCS leurs fournisseurs de prestations de cybersécurité qui souhaitent participer à l'échange d'informations.

[2] Ces fournisseurs doivent s'enregistrer en indiquant leur raison sociale ou leur nom ainsi que les coordonnées de la personne de contact enregistrée.

Art. 11 Transmission et utilisation des informations

[1] Lorsque les organisations et les autorités enregistrées transmettent des informations, elles précisent à qui l'OFCS peut les transmettre dans le système de communication pour l'échange sécurisé d'informations, à moins que la transmission soit prévue par la loi.

[2] L'OFCS décide s'il y a lieu de publier des informations autorisées.

[3] Les destinataires doivent garantir la protection des informations qu'ils reçoivent.

[4] Les fournisseurs de prestations de cybersécurité enregistrés des exploitants d'infrastructures critiques peuvent exploiter les informations qu'ils reçoivent exclusivement à des fins de protection desdites infrastructures.

Section 5 Obligation de signaler

Art. 12 Exceptions à l'obligation de signaler

[1] Les autorités et les organisations ci-après sont exemptées de l'obligation de signaler lorsqu'elles remplissent les conditions suivantes:

a. les hautes écoles au sens de l'art. 74*b* al. 1, let. a, LSI, pour autant qu'elles comptent moins de 2000 étudiants;

b. les entreprises visées à l'art. 74*b*, al. 1, let. d, LSI, pour autant qu'elles:

1. ne soient pas tenues de respecter le niveau de protection A ou B en tant que gestionnaires de réseau, producteurs d'électricité, gestionnaires d'installations de stockage d'électricité ou prestataires visés à l'art. 5*a*, al. 1, et l'annexe 1*a* de l'ordonnance du 14 mars 2008 sur l'approvisionnement en électricité[4], ou

2. attestent, en tant qu'exploitants de gazoducs au sens de l'art. 2, al. 3, de l'ordonnance du 4 juin 2021 sur la sécurité des installations de transport par conduites[5], un transport annuel d'énergie de moins de 400 GWh en moyenne sur les cinq dernières années;

4 RS **734.71**
5 RS **746.12**

c. les entreprises ferroviaires, les entreprises d'installations à câbles, de trolleybus, d'autobus et de navigation visées à l'art. 74*b*, al. 1, let. m, LSI, pour autant qu'elles:

1. ne soient pas chargées de tâches systémiques (art. 37 de la loi fédérale du 20 décembre 1957 sur les chemins de fer [LCdF])[6],

2. disposent d'une concession de transport de voyageurs conformément à l'art. 6 de la loi du 20 mars 2009 sur le transport de voyageurs (LTV)[7], mais ne fournissent pas de prestations commandées conjointement par la Confédération et les cantons (art. 28 à 31*c* LTV),

3. disposent d'une concession d'infrastructure conformément à l'art. 5 LCdF, mais que celle-ci n'a pas été octroyée en raison d'un intérêt public à la construction et à l'exploitation de l'infrastructure (art. 6, al. 1, let. a, LCdF);

d. les entreprises visées à l'art. 74*b*, al. 1, let. n, LSI, pour autant qu'elles:

1. ne soient pas tenues d'installer un système de gestion de la sécurité de l'information conformément aux art. 2 et 4 et à l'annexe II du règlement d'exécution (UE) 2023/203[8] ou à l'art. 2 et à l'annexe du règlement délégué (UE) 2022/1645[9],

2. ne soient pas tenues d'appliquer les conditions du ch. 1.7 de l'annexe du règlement d'exécution (UE) 2015/1998[10] dans

6 RS **742.101**
7 RS **745.1**
8 Règlement d'exécution (UE) 2023/203 de la Commission du 27 octobre 2022 portant modalités d'application du règlement (UE) 2018/1139 du Parlement européen et du Conseil en ce qui concerne les exigences en matière de gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne pour les organismes relevant des règlements (UE) n° 1321/2014, (UE) n° 965/2012, (UE) n° 1178/2011 et (UE) 2015/340 de la Commission, des règlements d'exécution (UE) 2017/373 et (UE) 2021/664 de la Commission, et pour les autorités compétentes relevant des règlements (UE) n° 748/2012, (UE) n° 1321/2014, (UE) n° 965/2012, (UE) n° 1178/2011, (UE) 2015/340 et (UE) n° 139/2014 de la Commission, des règlements d'exécution (UE) 2017/373 et (UE) 2021/664 de la Commission, et modifiant les règlements (UE) n° 1178/2011, (UE) n° 748/2012, (UE) n° 965/2012, (UE) n° 139/2014, (UE) n° 1321/2014 et (UE) 2015/340 de la Commission, et les règlements d'exécution (UE) 2017/373 et (UE) 2021/664 de la Commission, dans la version contraignante pour la Suisse selon le ch. 3 de l'annexe à l'Accord du 21 juin 1999 entre la Confédération suisse et la Communauté européenne sur le transport aérien (RS 0.748.127.192.68).
9 Règlement délégué (UE) 2022/1645 de la Commission du 14 juillet 2022 portant modalités d'application du règlement (UE) 2018/1139 du Parlement européen et du Conseil en ce qui concerne les exigences relatives à la gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne imposées aux organismes relevant des règlements (UE) n° 748/2012 et (UE) n° 139/2014 de la Commission et modifiant les règlements (UE) n° 748/2012 et (UE) n° 139/2014 de la Commission, dans la version contraignante pour la Suisse selon le ch. 3 de l'annexe à l'Accord du 21 juin 1999 entre la Confédération suisse et la Communauté européenne sur le transport aérien (RS 0.748.127.192.68).
10 Règlement d'exécution (UE) 2015/1998 de la Commission du 5 novembre 2015 fixant des mesures détaillées pour la mise en œuvre des normes de base communes dans le domaine de la sûreté de l'aviation civile, dans la version contraignante pour la Suisse selon

leur programme de sûreté visé aux art. 2, 12, 13 ou 14 du règlement (CE) nº 300/2008[11];

e. les fournisseurs et les exploitants visés à l'art. 74b, al. 1, let. t, LSI qui ne fournissent pas de prestations, en tout ou en partie, à des tiers et contre rémunération.

[2] Les autorités et organisations visées à l'art. 74*b*, al. 1, let. g, h, l et p, LSI sont exemptées de l'obligation de signaler, pour autant qu'elles emploient moins de 50 personnes dans le domaine concerné et que leur chiffre d'affaires annuel ou la somme inscrite au bilan annuel ne dépasse pas 10 millions de francs dans le domaine concerné.

Art. 13 Remise de documents pour la clarification de l'obligation de signaler

Les autorités et les organisations intéressées sont tenues de mettre à la disposition de l'OFCS tout document dont il a besoin pour fournir des renseignements sur la soumission à l'obligation de signaler.

Art. 14 Cyberattaques à signaler

[1] Le fonctionnement d'une infrastructure critique est mis en péril lorsque:

a. des collaborateurs ou des tiers sont touchés par des interruptions de système, ou

b. l'organisation ou l'autorité touchée ne peut maintenir ses activités qu'à l'aide de plans d'urgence.

[2] Une manipulation ou une fuite d'informations est avérée:

a. lorsque des personnes non autorisées consultent, modifient ou publient des informations importantes pour les affaires;

b. lorsqu'une violation de la sécurité de données est annoncée conformément à l'art. 24 de la loi fédérale du 25 septembre 2020 sur la protection des données[12].

[3] Une cyberattaque est considérée comme indétectée pendant une période prolongée si elle s'est produite plus de 90 jours auparavant.

[4] Une cyberattaque est considérée comme liée à des actes de chantage, de menace ou de contrainte lorsque de tels agissements sont dirigés contre une autorité ou une organisation soumise à l'obligation de signaler, ou contre des personnes travaillant pour celle-ci.

le ch. 4 de l'annexe à l'Accord du 21 juin 1999 entre la Confédération suisse et la Communauté européenne sur le transport aérien (RS 0.748.127.192.68).

11 Règlement (CE) n° 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) n° 2320/2002, dans la version contraignante pour la Suisse selon le ch. 4 de l'annexe à l'Accord du 21 juin 1999 entre la Confédération suisse et la Communauté européenne sur le transport aérien (RS 0.748.127.192.68).

12 RS **235.1**

Art. 15 Contenu du signalement

[1] Outre les informations prévues à l'art. 74*e*, al. 2, LSI, le signalement d'une cyberattaque doit préciser:

a. la date et l'heure de la constatation de l'attaque;

b. la date et l'heure de l'attaque;

c. les données sur l'attaquant.

[2] Il doit aussi indiquer si l'attaque est liée à un acte de chantage, de menace ou de contrainte et si elle a fait l'objet d'une dénonciation pénale.

[3] Il doit fournir les informations suivantes sur les conséquences de la cyberattaque:

a. la gravité du préjudice sur la disponibilité, l'intégrité et la confidentialité des informations, et

b. les effets sur le fonctionnement de l'autorité ou de l'organisation.

[4] Dans le cas où le signalement n'est pas transmis au moyen du système de communication de l'OFCS, il doit aussi contenir les informations suivantes sur l'autorité ou l'organisation soumise à l'obligation de signaler:

a. la raison sociale, le nom ou la désignation et l'adresse, et

b. les coordonnées de l'auteur du signalement.

Art. 16 Délai de saisie du signalement

[1] Si toutes les informations nécessaires ne sont pas connues dans les 24 heures suivant la détection de la cyberattaque, l'OFCS accorde à l'autorité ou à l'organisation concernée un délai de 14 jours pour compléter le signalement.

[2] Si les informations nécessaires n'ont pas toutes été fournies dans le délai accordé, l'OFCS demande à l'autorité ou à l'organisation concernée de les compléter immédiatement ou de confirmer que les informations ne sont pas disponibles.

Art. 17 Transmission du signalement

[1] 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'art. 9, al. 2, let. b, de la réception et du contenu du signalement.

[2] Une ou plusieurs autorités ou organisations soumises à l'obligation de signaler peuvent décider de confier le processus de signalement, individuellement ou collectivement, à une organisation tierce.

Section 6 Dispositions finales

Art. 18 Modification d'autres actes

La modification d'autres actes est réglée en annexe.

Art. 19 Entrée en vigueur

La présente ordonnance entre en vigueur le 1er avril 2025.

… Au nom du Conseil fédéral suisse:

La présidente de la Confédération, Karin Keller-Sutter
Le chancelier de la Confédération, Viktor Rossi

Annexe
(art. 18)

Modification d'autres actes

Les actes mentionnés ci-après sont modifiés comme suit:

1. Ordonnance du 7 mars 2003 sur l'organisation du Département fédéral de la défense, de la protection de la population et des sports[13]

Art. 15a, al. 2, phrase introductive et let. f et h

[2] Il assume notamment les tâches suivantes:

f. il gère l'équipe nationale d'intervention en cas d'urgence informatique;

h. il représente la Suisse dans les organes internationaux de cybersécurité.

2. Ordonnance du 31 août 2022 sur la protection des données[14]

Art. 41, al. 1

Abrogé

13 RS **172.214.1**
14 RS **235.11**