Ordonnance sur la cybersécurité (OCyS)

du XX xxxxxxx 2025

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. la Cyberstratégie nationale et son comité de pilotage;
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 et comité de pilotage

Art. 2 Cyberstratégie nationale

[1] La Cyberstratégie nationale (CSN) fixe le cadre stratégique de la prévention dans le domaine de la cybersécurité, de la détection précoce des cybermenaces ainsi que des possibilités de réaction et de la résilience en cas d'incident, ainsi que de la lutte contre la cybercriminalité.

[2] Elle est définie en accord avec les cantons.

1 RS **128**

Art. 3 Instauration et organisation du CP CSN

[1] Le Conseil fédéral instaure un comité de pilotage de la Cyberstratégie nationale (CP CSN).

[2] Le CP CSN dispose d'un secrétariat, exploité par l'OFCS.

Art. 4 Composition du CP CSN

[1] Le CP CSN se compose de représentants des départements, de la Chancellerie fédérale, des cantons, de l'économie, de la société et des hautes écoles.

[2] Le Conseil fédéral désigne tous les cinq ans les membres du CP CSN, à l'exception des représentants des cantons, qui sont nommés par la Conférence des gouvernements cantonaux.

[3] Il nomme un président parmi les représentants de l'économie, de la société et des hautes écoles.

Art. 5 Tâches du CP CSN

Le CP CSN assume les tâches suivantes:

a. il contrôle la CSN au moins une fois tous les cinq ans, il contribue à son développement et, au besoin, élabore des propositions visant à l'adapter;

b. il élabore, en accord avec les acteurs cités dans la CSN, des propositions concernant les priorités et les calendriers de la concrétisation des mesures de la CSN;

c. il évalue régulièrement la concrétisation des mesures et informe le Conseil fédéral et les cantons de tout retard;

d. il soumet au besoin au Conseil fédéral des propositions visant à compléter les mesures;

e. il établit, à l'intention du Conseil fédéral, des cantons et du public, un rapport annuel sur la concrétisation de la CSN.

Section 3 Tâches de l'OFCS

Art. 6 Demande de renseignements sur les titulaires

L'OFCS peut, afin d'avertir les autorités, les organisations ou les personnes d'une cybermenace imminente ou d'une cyberattaque en cours, requérir les coordonnées des titulaires de noms de domaine auprès du registre des noms de domaine relevant de la compétence de la Confédération ou qui sont subordonnés à ceux-ci.

Art. 7 Analyse technique des cyberincidents et des cybermenaces

[1] L'OFCS gère l'équipe nationale d'intervention en cas d'urgence informatique (*Computer Emergency Response Team [CERT]*), qui assume notamment les tâches suivantes:

a. elle gère les incidents techniques;

b. elle analyse les questions techniques;

c. elle identifie et évalue les cybermenaces.

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

Art. 8 Priorités pour les conseils et l'assistance en cas de cyberattaque

[1] Si, en cas de cyberattaque, les demandes de conseils et d'assistance dépassent les capacités de l'OFCS, celui-ci peut alors établir des priorités pour leur traitement en fonction de l'urgence et de l'étendue des conseils et de l'assistance.

[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. 9 Divulgation cordonnée des vulnérabilités

[1] L'OFCS veille à coordonner la divulgation des vulnérabilités selon les normes internationales 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. peut être très facilement exploitée pour une cyberattaque, ou

c. touche des systèmes très répandus.

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

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

[6] Les al. 1 à 4 ne s'appliquent pas aux vulnérabilités découvertes par l'Office fédéral de la communication (OFCOM) dans le cadre de ses contrôles de surveillance (art. 36 ss de l'ordonnance du 25 novembre 2015 sur les

installations de télécommunication[2]). Dans de tels cas, l'OFCOM informe l'OFCS.

[7] L'OFCS informe immédiatement l'OFCOM des vulnérabilités découvertes dans les installations de télécommunication selon à l'art. 3, let. d, de la loi du 30 avril 1997 sur les télécommunications[3].

Art. 10 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. 11 Système de communication permettant l'échange sécurisé d'informations

[1] Les autorités et les organisations dont le siège est en Suisse ont accès au système de communication de l'OFCS permettant l'échange sécurisé d'informations (art. 74, al. 2, let. a LSI).

[2] L'OFCS est responsable de la sécurité du système de communication et de la légalité du traitement des données.

Art. 12 Systèmes d'information permettant l'échange automatique

[1] L'OFCS met à la disposition des exploitants d'infrastructures critiques des systèmes d'information permettant l'échange automatique d'informations techniques sur les cybermenaces et les cyberincidents.

[2] L'OFCS est responsable de la sécurité des systèmes d'information et de la légalité du traitement des données.

Art. 13 Enregistrement

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

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

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

b. coordonnées de la personne ayant procédé à l'enregistrement.

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

Art. 14 Fournisseurs de prestations

[1] Les exploitants d'infrastructures critiques peuvent annoncer à l'OFCS des fournisseurs de prestations souhaitant participer à l'échange d'informations.

[2] Les fournisseurs de prestations doivent s'enregistrer en indiquant leur raison sociale ou leur propre nom ainsi que les coordonnées de la personne ayant procédé à l'enregistrement.

Art. 15 Transmission et utilisation des informations

[1] Les entreprises et les autorités enregistrées transmettent des informations à l'OFCS en indiquant si et à qui elles peuvent être retransmises, dans la mesure où la loi ne prévoit pas un tel processus.

[2] L'OFCS décide de la publication des informations destinées à être transmises sur le système de communication et sur les systèmes d'information en vue de l'échange automatique.

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

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

Section 5 Obligation de signaler

Art. 16 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 organes visés à l'art. 74*b*, al. 1, let. b et c, LSI sont responsables de moins de 1000 habitants; la population résidente est déterminante;

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

1. ne soient pas tenues, en tant que gestionnaires de réseau, producteurs d'électricité, exploitants de stockage d'électricité ou prestataires visé 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], de respecter le niveau de protection A ou B,

2. attestent, en tant qu'exploitants de gazoducs visés à l'art. 2, al. 3, de l'ordonnance du 4 juin 2021 sur la

4 RS **734.71**

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;

c. 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 management de la sécurité de l'information visé aux art. 2 et 4 et à l'annexe II du règlement d'exécution (UE) 2023/203[6] ou à l'art. 2 et à l'annexe II du règlement délégué (UE) 2022/1645[7],

2. ne soient pas tenues d'appliquer les conditions du point 1.7 de l'annexe du règlement d'exécution (UE) 2015/1998[8] dans leur programme de sûreté visé aux art. 2, 12, 13 ou 14 du règlement (CE) 300/2008[9];

d. 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])[10],

5 RS **746.12**

6 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.

7 Règlement délégué (UE) n° 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.

8 Règlement d'exécution (UE) n° 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.

9 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.

10 RS **742.101**

2. disposent d'une concession de transport de voyageurs visée à l'art. 6 de la loi du 20 mars 2009 sur le transport de voyageurs (LTV)[11], mais ne fournissent pas de prestations commandées en commun par la Confédération et les cantons (art. 28 à 31*c* LTV),

3. disposent d'une concession d'infrastructure visée à l'art. 5 LCdF, mais qui 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);

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

[2] Les entreprises visées à l'art. 74*b*, al. 1, let. f, g, h, l et p, LSI pour lesquelles l'al. 1 ne s'applique pas sont dispensées 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. 17 Obligation de documenter en cas de demande de renseignements sur l'assujettissement à 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 l'assujettissement à l'obligation de signaler.

Art. 18 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 lorsque:

a. des informations importantes pour les affaires sont modifiées ou publiées par des personnes non autorisées;

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

11 RS **745.1**
12 RS **235.1**

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

[4] Une cyberattaque est considérée comme étant liée à d'actes de chantage, de menace ou de contrainte lorsque de tels agissements sont dirigés contre une autorité ou une organisation assujettie à l'obligation de signaler, leurs responsables ou leurs collaborateurs, en poste ou anciens, ou contre des personnes agissant pour elle.

Art. 19 Contenu du signalement

[1] Le signalement d'une cyberattaque contient les informations suivantes:

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

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

c. le type d'attaque;

d. les méthodes d'attaque, et

e. les données sur l'agresseur.

[2] Il contient aussi des informations sur l'éventualité d'un chantage, d'une menace ou d'une contrainte en lien avec l'attaque et d'une dénonciation pénale.

[3] Il contient des informations sur les conséquences de la cyberattaque, à savoir:

a. les unités touchées de l'autorité ou de l'organisation;

b. la gravité du préjudice sur la disponibilité, l'intégrité et la confidentialité des informations propres et de celles de tiers, et

c. les effets sur le fonctionnement des unités touchées 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 des informations sur l'autorité ou l'organisation assujettie à l'obligation de signaler, à savoir:

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

d. les coordonnées de l'auteur du signalement.

Art. 20 Transmission du signalement

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 visée à l'art. 13, al. 2, let. b, de la réception et du contenu du signalement.

Art. 21 Délai de saisie du signalement

[1] Si toutes les informations nécessaires ne sont pas communiquées dans les 24 heures, 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.

Section 6 Dispositions finales

Art. 22 Modification d'autres actes

La modification d'autres actes est réglée en annexe.

Art. 23 Entrée en vigueur

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

Annexe
(art. 22)

Modification d'autres actes

Les ordonnances ci-après sont modifiées 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 d'intervention en cas d'urgence informatique (*Computer Emergency Response Team [CERT]*);

h. il représente la Suisse dans les organes internationaux dans le cadre de l'analyse technique des cybermenaces et de la maîtrise des cyberincidents.

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**