Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Commission fédérale de la Consommation (CFC)

CH-3003 Berne, CFC

E-Mail
ncsc@ncsc.admin.ch

Référence : ACF / voj
Votre référence :
Notre référence : teb
Berne, le 1er juillet 2024

Prise de position de la CFC sur le projet d'ordonnance sur la cybersécurité (OCyS)

Mesdames, Messieurs

La CFC se détermine comme suit sur la consultation relative au projet d'ordonnance sur la cybersécurité (OCyS).

- Art. 5a : la période de cinq ans entre deux contrôles de la Cyberstratégie nationale par le Comité de pilotage apparaît longue eu égard à l'évolution rapide des technologies et des menaces en matière de sécurité. Un délai de deux ans au maximum pourrait être plus indiqué.

- Art. 7 al. 1 : la question se pose de savoir comment sera composée l'équipe nationale d'intervention (Computer Emergency Response Team ou CERT), il pourrait être utile de compléter dans ce sens le rapport explicatif, voire le texte de l'ordonnance.

- Art. 7.1 let. a : "Incidents techniques" : le terme semble mal choisi. Un incendie dans un data center est un incident technique, mais il n'est pas nécessairement lié à la cybersécurité. Pour être plus précis, il pourrait être indiqué un incident relevant de la cybersécurité.

- Art. 7 al. 1 let. b : la même remarque que pour la lettre a vaut ici pour "questions techniques".

- Art. 8 al. 1 : la question se pose de savoir s'il faut prévoir de demander l'aide de prestataires privés en cas de crise majeure. Le cas échéant, il pourrait être indiqué de définir les critères permettant de les identifier et les sélectionner à l'avance.

Commission fédérale de la consommation
Jean-Marc Vögele
Secrétariat
Palais fédérale est, CH-3003 Berne
Tel.: +41 58 462 20 46, Fax: +41 58 462 43 70
jean-marc.voegele@bfk.admin.ch
www.konsum.admin.ch

- Art. 9 : une contradiction potentielle apparaît dans la formulation proposée, entre “raccourcir le délai si la vulnérabilité peut être facilement exploitée” et “prolonger le délai lorsque l’élimination de la vulnérabilité s’avère particulièrement complexe”. Que fait-on quand on a une vulnérabilité critique complexe à corriger ? Il pourrait être utile de mentionner la possibilité de mettre en place des mesures d’atténuation le temps de corriger la vulnérabilité.

- Art. 9 al. 5 : la question se pose de savoir s’il ne faudrait pas qu’ « il informe » au lieu de pouvoir informer” ?

- Art. 16 al. 2 : la formulation proposée vise à dispenser les « petites » structures de l’obligation de signaler. Mais ce critère est-il adéquat ? Qu’en est-il si ces petites structures sont d’importance systémique malgré qu’elles comptent “moins de 50 personnes” et que leur bilan “ne dépasse pas 10 millions de francs”. D’autres critères pertinents pourraient être considérés par ex. la taille de la clientèle touchée ? Cette question semble particulièrement pertinente dans une optique de protection des consommateurs.

- Art. 18 al. 2 : une fuite d’informations peut être avérée avant que les informations soient « publiées par des personnes non autorisées », par ex. grâce à une journalisation de l’accès aux données qui permettrait de détecter une intrusion et un téléchargement de données par des personnes non autorisées. Cet élément pourrait être ajouté à la définition.

- Art. 18 al. 4 : la formulation est peu claire et mériterait d’être améliorée.

La question de la détection des cybermenaces est peu traitée dans l’ordonnance, soulevant plusieurs interrogations. Il pourrait être adéquat de définir un cadre minimum en matière de management de la sécurité de l’information à mettre en place dans les organisations concernées par l’ordonnance, par analogie avec ce que prévoient les art. 5 ss de l’Ordonnance sur la sécurité de l’information (OSI). On renvoie également à l’art. 7 al. 1 let. c : comment s’y prend-elle ?

Pour la Commission fédérale de la Consommation

Prof. Dr. Anne-Christine Fornage
Présidente

Prof. Melinda Lohmann
Vice-présidente