Département fédéral de la défense, de la protection de la population et des sports, Palais fédéral, 3003 Berne

Réponse à la consultation concernant l'ordonnance sur la cybersécurité (OCyS)

Madame la conseillère fédérale,

Votre correspondance du 22 mai 2024 relative à la procédure de consultation susmentionnée nous est bien parvenue et a retenu notre meilleure attention.

Après une analyse approfondie des nouvelles dispositions proposées, nous tenons à souligner que ces changements n'auront qu'un impact limité sur le canton de Neuchâtel. En effet, nous appliquons déjà en grande partie les mesures suggérées, ce qui nous place en bonne position pour une transition harmonieuse vers ce nouveau cadre réglementaire.

Toutefois, vous trouverez ci-dessous nos remarques détaillées au sujet de deux articles :

Art. 10 Soutien aux autorités
L'article manque de précision quant à la manière d'obtenir ou d'initier ce soutien. En effet, il serait opportun de préciser la procédure que les cantons devront suivre pour recevoir les conseils et les bonnes pratiques de l'OFCS, d'autant plus que l'art. 11 ne mentionne pas que la plateforme de communication pourra également être utilisée à cette fin. À savoir que le NCSC-Security-Hub permet aujourd'hui uniquement des déclarations d'incidents.

Art. 18 Cyberattaques à signaler
Il serait judicieux de modifier l'al. 1, let. a. en remplaçant le terme « interruptions » par « perturbations ». En effet, il faut permettre de signaler un problème en amont d'une interruption du système et par conséquent, dès qu'une perturbation est identifiée, elle doit pouvoir être signifiée. Dans la formulation actuelle, si une personne non autorisée s'introduit dans un système d'information pour y déposer un logiciel malveillant sans l'exploiter elle-même, par exemple dans le but de le revendre à un autre attaquant (et que l'attaque a été découverte en moins de 90 jours), le signalement ne serait pas requis puisque le système n'a pas été interrompu.

De plus, l'al. 1 manque de précision concernant le seuil à partir duquel une cyberattaque doit être signalée en fonction du nombre de collaborateurs, de collaboratrices ou d'ordinateurs affectés. Par exemple, si un collaborateur télécharge un logiciel malveillant qui interrompt uniquement le fonctionnement de son ordinateur, il n'est pas clair si le signalement serait nécessaire même s'il s'agit d'un cas isolé.

Enfin, Monsieur Hugo Sobrino, responsable de la sécurité des systèmes d'information (RSSI) (hugo.sobrino@ne.ch, 032 889 84 07) se tient volontiers à votre disposition pour toute information complémentaire.

En vous remerciant de l’attention portée au présent courrier, nous vous prions de croire, Madame la conseillère fédérale, à l’expression de notre haute considération.

Neuchâtel, le 2 septembre 2024

Au nom du Conseil d'État :

La présidente,	*La chancelière,*
F. NATER	S. DESPLAND