Dachorganisation der Schweizer KMU
Organisation faîtière des PME suisses
Organizzazione mantello delle PMI svizzere
Umbrella organization of Swiss SME

Madame la Conseillère fédérale Amherd
Département fédéral de la défense,
de la protection de la population et des sports DDPS
Bundeshaus Ost
3003 Berne

ncsc@ncsc.admin.ch

Berne, le 12 septembre 2024 usam-MH/zh

Réponse à la procédure de consultation :
Adoption de l'ordonnance sur la cybersécurité (OCyS)

Madame la Conseillère fédérale Amherd,
Madame, Monsieur,

Plus grande organisation faîtière de l'économie suisse, l'Union suisse des arts et métiers usam représente plus de 230 associations et plus de 600 000 PME, soit 99,8% des entreprises de notre pays. La plus grande organisation faîtière de l'économie suisse s'engage sans répit pour l'aménagement d'un environnement économique et politique favorable au développement des petites et moyennes entreprises.

Le 22 mai 2024, le Département fédéral des finances nous a convié à prendre position dans le cadre de la procédure de consultation sur l'Adoption de l'ordonnance sur la cybersécurité (OCyS).

L'usam demande à être représentée directement dans le comité de pilotage pour la Cyberstratégie nationale. L'usam exige par ailleurs quelques précisions sur les cas de cyberattaques à annoncer, sinon les entreprises concernées resteront dans une situation d'incertitude juridique.

I. Contexte

L'ordonnance sur la cybersécurité (OCyS) a pour but de renforcer la protection des infrastructures critiques en Suisse contre les cyberattaques, en imposant notamment une obligation de signaler les incidents de cybersécurité. Elle s'inscrit dans la révision de la Loi sur la sécurité de l'information (LSI), qui a été approuvée en 2023 et qui entrera en vigueur le 1er janvier 2025. Cette révision prévoit la mise en place d'un cadre légal pour signaler les cyberattaques qui visent les infrastructures critiques, telles que l'énergie, les transports ou les services financiers.

L'Office fédéral de la cybersécurité (OFCS), créé récemment au sein du Département fédéral de la défense, de la protection de la population et des sports (DDPS), succède au Centre national pour la cybersécurité. Cet office aura pour mission de collecter et d'analyser les signalements, de faciliter l'échange d'informations entre les autorités et les entités concernées, et de fournir un soutien en cas

d'incident. Il jouera un rôle central dans la gestion des cyberattaques et des menaces à l'échelle nationale.

L'ordonnance introduit également un système de communication sécurisé pour améliorer la détection des cybermenaces et la coordination des réponses. Ce système permettra aux infrastructures critiques de recevoir des informations actualisées sur les menaces et de réagir rapidement. Un comité de pilotage pour la Cyberstratégie nationale, composé de représentants des départements fédéraux, des cantons, de l'économie et des universités, sera responsable de la mise en œuvre de la stratégie de cybersécurité.

Enfin, l'OCyS prévoit la gestion et la divulgation coordonnée des vulnérabilités dans les systèmes informatiques, en collaboration avec les fabricants et les autorités compétentes. Ces mesures visent à mieux protéger les infrastructures critiques et à renforcer la résilience du pays face aux cyberattaques.

II. Appréciation de l'usam

Pour l'usam, il est important de ne pas conduire à des sanctions des entreprises touchées, mais à trouver des solutions basées sur la coopération entre la Confédération et l'économie privée.

L'usam a ainsi deux demandes de précisions pour réduire les incertitudes dans la mise en œuvre de cette ordonnance. Il s'agit de l'art. 18, alinéas 1 et 2 ; les propositions de modification ainsi que les justifications sont visibles en vert. L'arrière-plan de l'ajustement souhaité est la crainte que la formulation actuelle n'oblige potentiellement à signaler chaque compromission d'un système.

Art. 18 Cyberattaques à signaler

1. La fonctionnalité d'une infrastructure critique est considérée comme menacée lorsque :

   1.1 . les employés ou des tiers sont affectés par des interruptions de système ; ou

   1.2. l'organisation ou l'autorité concernée ne peut plus maintenir ses activités qu'à l'aide de plans d'urgence.

Explication du rapport explicatif : *La fonctionnalité d'une infrastructure critique peut être menacée par une cyberattaque si les systèmes informatiques, réseaux ou systèmes de contrôle essentiels au fonctionnement de l'infrastructure sont compromis de telle manière qu'il en résulte des interruptions de système pour les employés et des tiers (art. 18, al. 1, let. a de cette ordonnance) ou que l'organisation ou l'autorité concernée ne peut plus maintenir ses activités qu'à l'aide de plans d'urgence (art. 18, al. 1, let. b de cette ordonnance).*
Une interruption de système se produit lorsque les employés ou des tiers ne peuvent plus exécuter des étapes importantes de leur travail en raison de l'indisponibilité des moyens informatiques nécessaires. Les plans d'urgence comprennent toutes les mesures techniques ou organisationnelles qui doivent être prises lorsque les moyens informatiques habituellement utilisés ne sont plus disponibles de manière imprévue et temporaire.

L'usam a des doutes sur ce que signifie exactement "essentiels au fonctionnement". Par exemple, le poste de travail d'un ingénieur télécom compromis par un malware entre-t-il dans le cadre de cette réglementation, dans la mesure où, pendant le nettoyage de son poste de travail, il ne pourrait plus exécuter certaines étapes importantes de son travail ?

L'usam demande de préciser cette règle, par exemple ainsi : "Les employés ou des tiers, qui sont directement responsables du fonctionnement immédiat de l'infrastructure critique, sont affectés par des interruptions de système causées par des cyberattaques, mettant ainsi directement en danger la stabilité du fonctionnement de l'infrastructure."

2. Une manipulation ou une fuite d'informations se produit lorsque :

   2.1 des informations pertinentes pour l'activité sont modifiées ou divulguées par des personnes non autorisées ; ou

   2.2 une violation de la sécurité des données au sens de l'article 24 de la loi fédérale sur la protection des données du 25 septembre 2020 se produit.

Pour l'usam, il serait nécessaire de préciser ce que l'on entend exactement par "informations pertinentes pour l'activité". Par exemple, si une application Web de l'entreprise XY, fournissant un service sans lien direct avec l'exploitation d'une infrastructure critique, est compromise, cela doit-il être signalé ?

L'usam demande d'ajouter une formulation du type : "des informations pertinentes pour l'activité, liées au fonctionnement immédiat de l'infrastructure critique".

Nous vous remercions de l'attention portée à notre prise de position et vous présentons, Madame, Monsieur, nos respectueuses salutations.

Union suisse des arts et métiers usam

Urs Furrer
Directeur

Mikael Huber
Responsable du dossier