

Département fédéral des finances
Bundesgasse 3
3003 Berne

ncsc@gs-efd.admin.ch

Berne, le 30 mars 2022 usam-MH/cp

Réponse à la consultation

Obligation de signaler les cyberattaques contre des infrastructures critiques

Monsieur le Conseiller fédéral Maurer,
Madame, Monsieur,

Plus grande organisation faïtière de l'économie suisse, l'Union suisse des arts et métiers usam représente plus de 230 associations et quelque 500 000 PME, soit 99,8% des entreprises de notre pays. La plus grande organisation faïtière 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.

L'usam est d'avis que des mesures rapides et efficaces sont nécessaires pour réduire les multiplications des cyberattaques notamment contre les infrastructures critiques, mais aussi contre les PME. Après une cyberattaque leur existence est menacée. Raison pour laquelle l'usam ne s'oppose pas à soutenir la possibilité de signaler des cyberattaques contre des infrastructures critiques. L'avant-projet manque toutefois de clarté pour la définition des domaines concernés sous l'expression « infrastructures critiques ».

I. Point de situation

Les cyberattaques sur les PME représentent un thème important pour l'usam. Les PME devraient également avoir la liberté d'annoncer les cyberattaques auprès du centre national pour la cybersécurité de la Confédération et d'être prises en considération. De fait, la Confédération pourrait mieux estimer l'étendue du problème et proposer des solutions et des campagnes de sensibilisation pour assurer la sécurité sur les réseaux Internet.

La numérisation progresse rapidement et des processus entiers sont aujourd'hui numérisés. Si une cyberattaque se produit et que les données ne peuvent pas être récupérées, l'existence d'une PME peut être menacée. C'est pourquoi la possibilité d'annonce est nécessaire, également dans l'optique de l'exigence selon laquelle d'autres PME doivent être informées et sensibilisées aux cyberattaques. Les PME restent une cible privilégiée des cyberattaques, les effets néfastes augmenter également largement et risquent, à long terme, de péjorer l'ensemble de l'économie. Les cyberattaques sur les

infrastructures critiques sont plus évidentes, car elles touchent à des points névralgiques de notre société et économie. Il est urgent pour l'usam que la Confédération veille tout particulièrement à instaurer des mesures de protections et de préventions des infrastructures critiques et des PME.

II. Appréciation générale

L'usam est d'avis que pour travailler raisonnablement et efficacement avec l'économie privée, il faudrait instaurer une coopération entre les autorités publiques et les entreprises privées représentant ou comportant des infrastructures critiques. Il n'y a aucune raison d'imposer une obligation de plus aux entreprises. Celles-ci sont responsables de leurs affaires et savent parfaitement à quel moment demander de l'aide aux autorités publiques en cas de cyberattaque. La coopération est importante pour que cet outil de détection précoce puisse fonctionner au niveau national.

La signalisation des cyberattaques contre les infrastructures critiques ne devrait également représenter aucune charge administrative inutile pour les PME. Les entreprises aimeraient y trouver un service qui peut aider dans le cas de cyberattaque et non une charge administrative supplémentaire.

L'usam demande à clarifier ce qui est sous-entendu par « infrastructures critiques ». Dans les termes présentés, il est fort probable qu'on veuille imposer une signalisation des cyberattaques à des secteurs de l'économie qui ignorent encore être concernés. La définition « infrastructures critiques » ne doit pas faire laisser planer de doutes pour les entreprises impliquées.

Autant l'obligation est exagérée, autant la menace de sanction est totalement déplacée. Les entreprises privées sont responsables de leurs affaires. Dans le domaine de la numérisation et de l'IT, la culture de l'erreur possible est indispensable pour développer de nouveaux modèles d'affaires. Raison pour laquelle, l'introduction d'une culture de la sanction dans ce domaine serait absolument contre-productive. L'usam s'oppose fermement à toute sanction ou mesure de contrainte envers l'économie privée.

Si le signalement des cyberattaques peut se faire sur une base de coopération, l'usam demande que le signalement des cyberattaques puisse se faire très simplement, de manière *user-friendly*. La signalisation de ces attaques doit être faite en ligne avec un concept clair et une procédure *user-friendly* qui soit pensée comme une procédure d'accompagnement des entreprises victimes et non comme une punition administrative.

III. Conclusion

L'usam constate que le projet impose trop de restrictions à l'économie privée. Une possibilité d'annoncer suffirait, et cela devrait aussi être ouvert aux PME. En revanche, il est hors de questions d'imposer des obligations accompagnées de sanctions dans le domaine de la signalisation des cyberattaques contre les infrastructures critiques. La Confédération devrait développer un service d'accompagnement des entreprises victimes de cyberattaques sans en faire une énième procédure administrative contraignante pour des entreprises d'ores-et-déjà fragilisées.

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

Union suisse des arts et métiers usam



Hans-Ulrich Bigler
Directeur



Mikael Huber
Responsable du dossier