SUISSEDIGITAL
ASSOCIATION DES RESEAUX DE COMMUNICATION

CONNECTE
NOTRE PAYS

BILLET DE SESSION MARS 2023

EDITORIAL

Mesdames et Messieurs,

J'ai le grand plaisir de vous convier à notre manifestation d'information de la session du printemps 2023 consacrée aux questions sur les mondes virtuels « Métavers ». Concrètement, nous nous pencherons sur le thème **« Métavers – pertinence pour la société, l'économie et la politique ».**

La manifestation se déroulera à la date suivante :

le mercredi 8 mars 2023, de 19h00 à 21h00, à l'hôtel Bellevue Palace, Berne, salon « Orangerie »

Qu'est-ce que le métavers ? Quels développements se profilent ? Dans quelle mesure ces développements sont-ils pertinents pour la société, l'économie et la politique ? Nous aimerions aborder avec vous ces questions et bien d'autres lors de la manifestation de session.

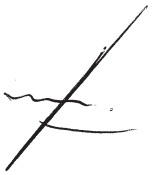
Programme :

Dès 19h00	**Apéritif et buffet**
19h55	**Allocution de bienvenue et introduction** Pierre Kohler, Président de SUISSEDIGITAL
20h00	**Métavers – pertinence pour la société, l'économie et la politique** Fabian Wicki, propriétaire de Gestalt Kommunikation (www.gestalt.ch) et chargé de cours à la Fachhochschule Nordwestschweiz FHNW
21h00	**Discussion autour d'un café et d'un dessert**

Nous serions ravis que vous puissiez vous joindre à nous le 8 mars 2023. Nous nous ferons un plaisir de prendre note de votre inscription par e-mail à l'adresse info@suissedigital.ch ou par téléphone au 031 328 27 28.

Enfin, j'aimerais attirer votre attention sur notre prise de position concernant l'introduction d'une obligation de signaler les cyberattaques contre les infrastructures critiques (modification de la loi sur la sécurité de l'information, projet 22.073), à la page 2 du présent billet de session.

Je vous souhaite une lecture enrichissante et une session de printemps couronnée de succès.



Pierre Kohler
Président de SUISSEDIGITAL

AFFAIRES EN COURS

22.073 : Loi sur la sécurité de l'information. Modification (inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques)
CN, le jeudi 16 mars 2023

SUISSEDIGITAL salue l'orientation de la proposition d'amendement. Toutefois, étant donné qu'il est prévu d'introduire une obligation de signaler les cyberattaques qui, si elle n'est pas respectée, peut même entraîner une condamnation pénale de la personne responsable au sein de l'entreprise, la loi devrait indiquer clairement quelles entreprises sont concernées par cette obligation et quand un signalement doit obligatoirement être fait au Centre national pour la cybersécurité (NCSC). Le projet de loi ne répond pas encore à cette exigence :

- Le **cercle des destinataires** de l'obligation de signaler pour les prestations informatiques et d'information n'est pas suffisamment précis et délimité par rapport à la criticité des réseaux et services exploités. => Le cercle des destinataires doit être précisé.

- Les **exceptions au cercle des destinataires** de l'obligation de signaler devraient déjà être clairement désignées au niveau de la loi. On ne peut pas exiger des petits fournisseurs de services de télécommunication qui sont victimes d'une cyberattaque qu'ils vérifient encore, dans cette situation exceptionnelle, si une déclaration au NCSC est obligatoire pour eux. On ne peut pas non plus exiger qu'ils se renseignent au préalable sur une éventuelle obligation de signaler auprès du NCSC. Il faudrait avant tout miser sur la coopération volontaire et l'encourager par un travail de relations publiques et d'information approprié de la part du NSCS. => Il faut prévoir dans la loi un régime d'exception généreusement délimité.

- Les **cas déclencheurs** définis pour le signalement obligatoire au NCSC sont décrits de manière trop vague pour pouvoir délimiter à l'avance de manière fiable quand un signalement au NCSC doit être effectué dans un cas particulier en présence d'une obligation de signaler personnelle. Lors de la mise en œuvre du processus de signalement au NCSC dans l'organisation de l'entreprise, des critères clairs sont toutefois nécessaires pour déterminer quand un signalement au NCSC par la personne compétente est obligatoire. Il faudrait en outre préciser que les attaques contre les clients finaux, leurs terminaux et leurs propres éléments d'infrastructure (p. ex. réseau domestique) ne déclenchent pas d'obligation de signaler. => Les cas déclencheurs doivent être décrits plus précisément.

SUISSEDIGITAL rejette en particulier la responsabilité pénale personnelle prévue pour la personne responsable au sein de l'entreprise en cas de non-respect de l'obligation de signaler ; une éventuelle amende infligée à l'entreprise est suffisante.

Enfin, SUISSEDIGITAL estime qu'il est problématique de devoir remplir diverses obligations de signaler vis-à-vis des autorités dans des situations extraordinaires, par exemple en cas de pannes de réseaux ou de systèmes qui pourraient être dues à une cyberattaque. Un point de contact central devrait, selon les besoins, informer automatiquement d'autres services.

Synthèse : Rejetez la modification de la loi pour l'améliorer.