digitalswitzerland | Waisenhausplatz 14 | 3011 Bern

Madame la Conseillère aux Etats / Monsieur le Conseiller aux Etats

Zürich, le 26. Mai 2023

Loi sur la sécurité de l'information. Modification: Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques (22.073)

digitalswitzerland soutient la proposition de la minorité (Wicki, Bauer, Burkart, Français, Minder) : Approbation de la version du Conseil fédéral

Mesdames et Messieurs les Députés au Conseil des Etats,

Le 5 juin 2023, vous traiterez la loi sur la sécurité de l'information. digitalswitzerland s'est également prononcée par le passé en faveur de l'introduction d'une obligation de déclarer les cyberattaques. Nous conseillons toutefois de suivre les propositions de la minorité et de supprimer les "vulnérabilités" de l'article 74, comme le Conseil fédéral l'avait initialement proposé. Cette recommandation s'appuie sur les considérations suivantes:

1. En théorie, la logique de notification de la proposition de loi est conçue pour les cyberattaques (défense, mitigation) et non pour les cybervulnérabilités (prévention) - il s'agit conceptuellement de deux différentes circonstances.
2. Dans la pratique, la notification des vulnérabilités entraîne moins de collaboration entre les acteurs. La confiance n'est pas renforcée, mais plutôt affaiblie. Contrairement aux cyberattaques, la question de savoir *ce qui* doit être signalé aux autorités et *à quel moment* n'est pas suffisamment clarifiée dans le cas des vulnérabilités. Le *qui* n'est, selon nous, pas encore clarifié dans les deux cas.

Pour les raisons susmentionnées, la prise en compte des vulnérabilités entraîne des pièges juridiques qui ne sont pas prévisibles pour les entreprises et les autorités et qui rendent donc la loi impraticable.

Nous attirons également votre attention sur le fait que nous soutenons sans réserve la lettre et les arguments qu'elle contient de la part des opérateurs d'infrastructures critiques (énergie, mobilité, finance, télécommunications).

Explications:

Théorie:

Le traitement identique de la notification des vulnérabilités et des cyberattaques comporte des imprécisions logiques qui conduisent à des pièges juridiques:

- Les cyberattaques sont dues à des tiers, elles supposent une attaque extérieure - la réaction est la défense et la mitigation.
- Les vulnérabilités sont inconsciemment auto-infligées, il s'agit donc d'erreurs pour lesquelles la responsabilité est partagée entre le fabricant du produit et l'utilisateur, sans intervention extérieure - la recette est la prévention et la collaboration.

La prise en compte des vulnérabilités a pour conséquence que la loi n'est pas praticable, parce qu'elle traite deux situations différentes de la même manière.

La mise en pratique:
Dans la pratique, plusieurs problèmes apparaissent:

- *Ce qui est signalé:* La définition des vulnérabilités est floue. La loi ne précise pas de quelles vulnérabilités il s'agit; par exemple, des vulnérabilités de produit telles que des erreurs de logiciel, de matériel et de réseau, ou des vulnérabilités d'implémentation telles que des erreurs de configuration, des vulnérabilités physiques (par exemple, des locaux non sécurisés) ou des erreurs humaines (par exemple, un mot de passe trop faible). Le signalement de vulnérabilités d'implémentation entraîne une mise en danger de l'entreprise signalante sans bénéfice pour la collectivité.
- *Qui doit faire une notification:* Alors qu'en cas d'attaque, il y a une incitation à faire une notification, il n'est pas clair quelles et combien d'organisations sont considérées comme des exploitants d'infrastructures critiques. ***Il faudrait d'abord clarifier combien et quelles organisations sont concernées par une obligation de notification.***
- *Quand est-ce que la faille est signalée:* D'un point de vue externe, il n'est pas possible de déterminer quand une vulnérabilité quelconque a effectivement été découverte. ***Il n'est pas possible de prouver que la notification a été faite dans les délais.***
- *Comment gère-t-on aujourd'hui les vulnérabilités:* la pratique courante est la suivante: souvent, les fournisseurs TIC publient des bulletins et des avis de sécurité afin d'informer à temps les clients des vulnérabilités connues, des correctifs et des solutions de contournement pour leurs produits logiciels. Ces entreprises seraient à l'avenir concernées par les sanctions prévues par la loi. Si un utilisateur découvre aujourd'hui une faille, il le signale au fournisseur et des solutions sont recherchées bilatéralement.
- *Comment serait-il notifié à l'avenir:* La loi exige une notification à un tiers (NCSC), bien que la responsabilité de la faille et de sa correction incombe au fabricant et/ou à l'utilisateur. C'est comme si l'on répondait systématiquement "reply-all" aux signalements de défaillances par e-mail - la relation de confiance entre le client et le fournisseur serait mise à mal.

Nous vous remercions de votre attention. Le secrétariat de digitalswitzerland se tient à votre disposition pour toute question ou remarque.

Nous vous prions d'agréer, Madame, Monsieur, nos salutations distinguées,

Stefan Metzger

Managing Director digitalswitzerland

stefan@digitalswitzerland.com

Guillaume Gabus

Public Affairs & Executive Board

guillaume@digitalswitzerland.com

A propos de digitalswitzerland

digitalswitzerland est une initiative intersectorielle à l'échelle nationale qui vise à renforcer et à ancrer la Suisse en tant que leader mondial de l'innovation numérique. Sous l'égide de digitalswitzerland, plus de 200 organisations, composées de membres de l'association et de partenaires de la fondation politiquement neutres, collaborent de manière transversale à cet objectif. digitalswitzerland est un interlocuteur pour toutes les questions liées à la digitalisation et s'engage à résoudre de multiples défis.