digitalswitzerland | Waisenhausplatz 14 | 3011 Bern

Madame la Conseillère aux Etats / Monsieur le Conseiller aux Etats
de la Commission de la politique de sécurité du Conseil des Etats

Réponse à la décision du Conseil national concernant l'objet 22.073 - Loi sur la sécurité de l'information. Modification (Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques)

Mesdames et Messieurs les Conseillers aux Etats,

La nouvelle loi sur la sécurité de l'information est un pas important pour la cybersécurité de la Suisse. Elle doit être saluée car, grâce à l'obligation d'annoncer les cyberattaques, elle permet d'obtenir une image beaucoup plus précise de la situation en Suisse.

La proposition de loi adoptée par le Conseil national le 16 mars ne doit pas être rejetée, mais complétée par les remarques suivantes. Le Conseil national souhaite que non seulement les cyberattaques, mais aussi les vulnérabilités soient déclarées. L'inclusion des vulnérabilités dans l'obligation de signalisation a toutefois pour conséquence de faire naître des questions qui nécessitent une réponse et doivent impérativement être intégrées dans le processus législatif:

1. La cybervulnérabilité est-elle définie de manière suffisamment précise pour que les acteurs concernés aient une compréhension commune des vulnérabilités à déclarer?
2. Quelles sont les vulnérabilités à signaler? Des vulnérabilités de produit ou de mise en œuvre?
3. Les vulnérabilités peuvent-elles et doivent-elles être soumises à la même logique de signalisation que les cyberattaques?

Concernant la question 1:
La définition des vulnérabilités dans le projet de loi, si elles étaient signalées, n'est pas suffisamment précise pour les distinguer des cyberincidents :

- Dans le texte actuel, une vulnérabilité peut être définie comme étant due à une erreur humaine ou à des failles dans la mise en œuvre (*cf. art. 5g vulnérabilité: une cybermenace due à des failles ou à des erreurs dans les moyens informatiques.*).
- Nous estimons que la définition de la cybervulnérabilité actuelle est imprécise et peut entraîner un nombre très élevé de signalisation de qualité variable.
- La proposition suivante est faite pour la définition des points de vulnérabilité :
    - *Art. 5 lettre g.: vulnérabilité: cybermenace résultant de faiblesses ou d'erreurs dans des composants software ou hardware.*
- Les vulnérabilités ou les erreurs dans les composants software ou hardware sont des ***vulnérabilités de produit***

Concernant la question 2:
Distinction entre les vulnérabilités de produit et les vulnérabilités de mise en œuvre:

- Une obligation de notification des vulnérabilités de produit est envisageable, mais difficile à mettre en œuvre (voir ci-dessous, logique de signalisation).
- L'obligation de signaler les vulnérabilités de configuration ou d'architecture (**vulnérabilité de mise en œuvre**) n'a, selon nous, guère de sens et conduit à une mise en danger de l'entreprise signalante sans bénéfice pour la communauté. De plus, il faut partir du principe que l'erreur de mise en œuvre serait d'abord corrigée et qu'ensuite - si jamais elle l'était - une notification serait effectuée.

Concernant la question 3:

La logique de signalisation et l'applicabilité du délai de signalisation doivent tenir compte de la distinction entre les vulnérabilités des produits et les cyberattaques.

- Dans sa forme actuelle, la loi ne tient pas suffisamment compte de la distinction entre les cyberattaques et les vulnérabilités. Les cyberattaques nécessitent une atténuation et une défense, les vulnérabilités nécessitent une prévention. En conséquence, des insuffisances apparaissent dans la signalisation et le traitement lorsque les vulnérabilités des produits sont soumises à la même logique de processus que les cyberattaques.
- Lorsqu'une entreprise suisse découvre une vulnérabilité dans un produit d'un vendeur, soit elle ne la signale pas du tout jusqu'à présent, soit elle la signale directement au fabricant lui-même.
- Il n'existe aujourd'hui aucune obligation de signalisation entre l'utilisateur et le fabricant. Mais une obligation de notification à des tiers (NCSC) est désormais introduite. Cela crée une relation de confiance ambivalente. Dans le pire des cas, il en résulte un sentiment de dénonciation.
- D'un point de vue externe, il n'est pas possible de déterminer quand une vulnérabilité a effectivement été découverte. C'est pourquoi, dans le cas des vulnérabilités, la signalisation dans les 24 heures ne peut pas être prouvée, elle devient même obsolète. Comment vérifier si une signalisation a été effectuée dans les délais?
- Pour ces raisons, nous nous joignons à la position de la minorité du Conseil National selon laquelle un délai de signalisation d'au moins 72 heures est une condition de base pour une mise en œuvre efficace de la loi.

Enfin, nous sommes d'avis qu'un rapport complet sur la loi est nécessaire. Il faudrait par exemple clarifier si:

- Une obligation de signaler les vulnérabilités, telle qu'elle est actuellement prévue, est applicable dans la pratique.
  - Existe-t-il des données provenant de pays comparables?
  - Une obligation de notification de 24 heures est-elle applicable aux petites entreprises en raison de leurs capacités ?

Nous vous remercions de votre attention. Le Comité de cybersécurité ainsi que le bureau de digitalswitzerland se tiennent 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 & Extended Management

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.