Swico
Josefstrasse 218
CH-8005 Zurich

Tél. +41 44 446 90 90
www.swico.ch
info@swico.ch

Département fédéral des finances (DFF)
Unité de pilotage informatique de la Confédération (UPIC)
Direction UPIC
Monsieur Peter Fischer
Délégué au pilotage informatique de la Confédération

Par e-mail: peter.fischer@isb.admin.ch

Zurich, le lundi 18 septembre 2017 17:38:00

Prise de position de Swico sur le projet de stratégie nationale de protection de la Suisse contre les cyberrisques 2018-2022

Cher Monsieur,

Dans votre e-mail du 3 septembre 2017, vous nous avez invités à présenter notre position sur le projet d'une nouvelle stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) pour les années 2018-2022. Au nom de Swico, nous vous remercions de cette opportunité et vous remettons par la présente notre prise de position.

1. Légitimation et intérêts

Swico est l'organisation des fournisseurs du secteur des TIC en Suisse. Swico représente les intérêts de 450 fournisseurs TIC qui emploient 56'000 personnes et réalisent un chiffre d'affaires annuel de CHF 40 milliards. En tant que fournisseurs du secteur des TIC, nos membres sont particulièrement concernés par la nouvelle SNPC prévue et son application et légitiment cette prise de position de Swico.

2. Principes

Nous saluons le fait que ce projet soit soumis en amont à des organisations, associations et experts importants afin qu'ils prennent position, dans le but d'en vérifier le contenu et de fournir un large soutien à la stratégie. Le communiqué de vendredi dernier sur la découverte d'une nouvelle attaque de plusieurs serveurs de l'administration fédérale montre qu'il faut sans délai commencer à élaborer et appliquer une stratégie efficace.

Il est incompréhensible que seul le chapitre 4.8 Cyberdéfense soit rédigé en français. Nous demandons que la SNPC finale soit publiée en quatre langues (d,f,e,i) comme la stratégie précédente.

3. Prise de position sur différents champs d'action et mesures

3.1 Champ d'action Standardisation/régulation

3.1.1 Introduction de standards minimaux

La définition de directives contraignantes et vérifiables par audit doit être appuyée. Ces exigences minimales en matière de cybersécurité dans les entreprises doivent être fixées en collaboration et concertation étroites entre l'État et le secteur privé.

Demande: Il faut s'assurer que de tels standards minimaux puissent être mis en œuvre au niveau de l'entreprise moyennant un coût approprié. De plus, ces standards minimaux doivent être rendus compatibles avec les standards internationaux pertinents en usage et il faut éviter toute sorte de «touche suisse».

3.1.2 Obligation de notification des cas de cybercriminalité

Afin de réduire les cybermenaces, il faut examiner l'introduction d'une obligation de notification des cas de cybercriminalité et se prononcer sur celle-ci. Ces travaux de fond doivent être réalisés en coopération avec les administrations compétentes, le secteur privé et les associations et prendre en compte les développements internationaux dans ce domaine. Ils constituent la base pour décider l'introduction d'une obligation de notification (cf. projet p. 17).

Les données concernant les menaces actuelles et futures, l'importance des attaques et les dommages occasionnés ne sont pas accessibles de façon transparente dans l'état actuel des choses. Cela complique une gestion efficace des cyberrisques. Nous réclamons l'introduction de l'obligation de notification des cyberattaques. Le signalement doit pouvoir être anonyme. Il faut en outre insister pour que cette obligation de notification vaille aussi pour les organisations étatiques.

Demande: Il faut introduire une obligation de notification pour les cas de cybercriminalité qui peut aussi être anonyme.

3.2 Champ d'action Gestion de crise

Comme le projet le constate avec justesse, il est crucial de soutenir les cellules de crise par des connaissances techniques et une collaboration intense de tous les services compétents de la Confédération, des cantons et de l'économie. Les mesures présentées dans le projet (intégration de MELANI dans les cellules de crise, exercices en commun de gestion de crise et préparation de la communication de crise) en font partie. Il est également nécessaire de répartir et délimiter les rôles de l'État et du secteur privé:

Demande: Nous demandons une clarification et délimitation appropriées des compétences et interfaces entre l'État et le secteur privé comme mesure supplémentaire dans le champ d'action de la gestion de crise.

3.3 Champ d’action Impact à l'extérieur et sensibilisation

Sensibiliser le public aux risques de cybercriminalité (awareness)

De récents incidents, comme l’attaque des serveurs de l'administration fédérale rendue publique la semaine dernière, ont montré qu’il était plus que jamais nécessaire de sensibiliser la collectivité aux cyberrisques et d’attirer son attention sur des solutions de protection basiques. Une partie de la population ainsi que certains secteurs de l’économie n’ont pas suffisamment conscience de la menace que représentent les cyberrisques. L’application de ces mesures de base est absolument nécessaire. Les campagnes nationales de vigilance sont un outil approprié pour cela.

4. Conclusion

L’évolution importante des menaces et leur intensification depuis 2012 ainsi que la forte dynamique du développement des cyberrisques exigent une adoption rapide de la stratégie et une prompte mise en application des mesures.

Il faut également noter qu’une stratégie ne représente pas une base efficace tant qu’on ne dispose pas des compétences techniques et expertises nécessaires à sa réalisation.

Nous vous prions de bien vouloir prendre nos demandes en considération et vous en remercions au nom de tous nos membres.

Veuillez agréer nos meilleures salutations.

Swico

Christa Hofmann
Head Legal & Public Affairs