Swico
Josefstrasse 218
CH-8005 Zürich

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

Eidgenössisches Finanzdepartement EFD
Informatiksteuerungsorgan des Bundes ISB
Leitung ISB
Herr Peter Fischer
Delegierter für die Informatiksteuerung des Bundes

Per E-Mail: peter.fischer@isb.admin.ch

Zürich, 18. September 2017

**Swico Stellungnahme zum Entwurf Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018-2022**

Sehr geehrter Herr Fischer

Mit E-Mail vom 3. September 2017 haben Sie uns eingeladen, unsere Position zum Entwurf einer neuen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) für die Jahre 2018-2022 darzulegen. Namens des Swico bedanken wir uns für diese Möglichkeit und reichen hiermit gerne unsere Stellungnahme ein.

## 1. Legitimation und Betroffenheit

Swico ist der Verband der ICT-Anbieter der Schweiz. Swico vertritt die Interessen von 450 ICT-Anbieterfirmen, welche 56'000 Mitarbeitende beschäftigen und einen Umsatz von jährlich CHF 40 Milliarden erwirtschaften. Als ICT-Anbieter sind unsere Mitglieder von der geplanten neuen NCS in der Umsetzung ganz besonders betroffen und Swico zu dieser Stellungnahme legitimiert.

## 2. Grundsätzliches

Wir begrüssen, dass dieser Entwurf wichtigen Organisationen, Verbänden und Experten im Vorfeld zur Stellungnahme unterbreitet und damit bezweckt wird, den Inhalt zu verifizieren und die Strategie breit abzustützen. Wie die Mitteilung von letztem Freitag über die Entdeckung eines erneuten Angriffs auf einzelne Server der Bundesverwaltung zeigt, ist eine griffige Strategie resp. deren Umsetzung ohne Verzug in die Wege zu leiten.

Unverständlich ist, warum das Kapitel 4.8 Cyber-Abwehr als einziges in französischer Sprache abgefasst ist. Wir verlangen, dass die definitive NCS wie die Vorgängerstrategie in vier Sprachen (d,f,e,i) publiziert wird.

## 3. Stellungnahme zu einzelnen Handlungsfeldern und Massnahmen

### 3.1 Handlungsfeld Standardisierung/Regulierung

#### 3.1.1 Einführung von Minimalstandards

Die Festlegung verbindlicher und auditierbarer Richtlinien ist zu befürworten. Diese Minimalanforderungen an die Cybersecurity für Unternehmen sind in enger Zusammenarbeit und Abstimmung zwischen Staat und der Privatwirtschaft festzulegen.

Antrag: Es ist sicherzustellen, dass solche Minimalstandards mit angemessenem Aufwand in Bezug auf das einzelne Unternehmen umgesetzt werden können. Des Weiteren sind diese Minimalstandards mit relevanten, international gebräuchlichen Standards kompatibel auszugestalten und jeglicher Swiss Finish zu vermeiden.

#### 3.1.2 Meldepflicht für Cyber-Vorfälle

Zur Verbesserung des Lagebilds zu Cyber-Bedrohungen soll die Einführung einer Meldepflicht für Cyber-Vorfälle geprüft und über ihre Einführung befunden werden. Diese Grundlagearbeiten sollen in Kooperation mit den jeweils zuständigen Behörden, der Privatwirtschaft und den Verbänden durchgeführt werden und unter Berücksichtigung der internationalen Entwicklungen in diesem Bereich erfolgen. Sie bilden die Grundlage für den Entscheid über die Einführung einer Meldepflicht (vgl. Entwurf S. 17).

Daten über aktuelle und künftige Bedrohungslagen, das Ausmass von Angriffen und verursachtem Schaden sind gemäss heutigem Stand nicht transparent verfügbar. Ein wirksames Cyberrisikomanagement wird dadurch erschwert. Wir fordern, dass eine Meldepflicht von Cyber-Vorfällen eingeführt wird. Die Meldung muss anonym möglich sein. Dabei ist Wert darauf zu legen, dass diese Meldepflicht gleichermassen auch für staatliche Organisationen gilt.

Antrag: Eine Meldepflicht für Cyber-Vorfälle, die auch anonym erfolgen kann, ist einzuführen.

### 3.2 Handlungsfeld Krisenmanagement

Wie im Entwurf richtig festgestellt wird, ist bei derartigen Krisen die Unterstützung der Stäbe durch fachspezifisches Wissen und eine intensive Zusammenarbeit aller kompetenten Stellen aus Bund, Kantonen und Wirtschaft von grundlegender Wichtigkeit. Die im Entwurf aufgeführten Massnahmen (Integration von MELANI in die Krisenstäbe, gemeinsame Übungen zum Krisenmanagement und Vorbereitung der Krisenkommunikation) sind Teil davon. Zusätzlich notwendig ist die Rollenverteilung und Abgrenzung zwischen Staat und Privatwirtschaft:

Antrag: Wir fordern eine Klärung und Abgrenzung der Schnittstellen und Zuständigkeiten zwischen Staat und Privatwirtschaft als zusätzliche Massnahme innerhalb des Krisenmanagements.

### 3.3 Handlungsfeld Aussenwirkung und Sensibilisierung

**Sensibilisierung der Öffentlichkeit für Cyber-Risiken (Awareness)**

Neue Vorfälle - wie auch der letzte Woche publik gewordene Angriff auf Server der Bundesverwaltung - haben aufgezeigt, dass es mehr denn je notwendig ist, die Allgemeinheit für Cyber-Risiken zu sensibilisieren und auf grundlegende Schutzmöglichkeiten aufmerksam zu machen. In der Bevölkerung und Teilen der Wirtschaft mangelt es an hinreichendem Verständnis für die Bedrohung durch Cyber-Risiken. Die Umsetzung diesbezüglicher Grundmassnahmen ist absolut notwendig. Nationale Awareness Kampagnen sind dafür ein geeignetes Mittel.

## 4. Fazit

Die seit 2012 markant veränderte und intensivierte Bedrohungslage und die hohe Dynamik in der Entwicklung der Cyber-Risiken erfordert eine rasche Verabschiedung der Strategie und Umsetzung der Massnahmen.

Zu beachten dabei ist, dass eine Strategie als Grundlage unbrauchbar ist, solange deren Umsetzung nicht mit den notwendigen Fachkompetenzen und Skills realisiert werden kann.

Wir danken Ihnen namens unserer Mitglieder für eine Berücksichtigung unserer Anliegen.

Freundliche Grüsse

Swico

Christa Hofmann
Head Legal & Public Affairs