Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Informatiksteuerungsorgan des Bundes ISB

**MELANI**
Koordinationsstelle NCS

# Factsheet NCS 2014

## Die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)

Der Bundesrat hat mit der Verabschiedung der «Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)»[1] am 27. Juni 2012 und deren Umsetzungsplan am 15. Mai 2013 (Umsetzungsplan zur «Nationalen Strategie zum Schutz der Schweiz gegen Cyber-Risiken (UP NCS)»)[2] festgelegt, das Thema Internet und Sicherheit auf höchster Ebene anzusiedeln. Der schweizerische Bundesrat hat auch entschieden, dass es eine ausschliesslich zivile Cyber-Strategie sein soll, die den Kriegsfall explizit ausschließt.

**Ziele**
Die NCS verfolgt drei Hauptziele:

- Frühwarnung vor Cyber-Bedrohungen
- Stärkung der Widerstandsfähigkeit der kritischen Infrastrukturen
- Reduktion von Cyber-Risiken, insbesondere Cyber-Spionage und Cyber-Sabotage.

**Massnahmen**
Die NCS ist eine integrale Strategie, die mit ihren 16 Massnahmen einen umfassenden Ansatz verfolgt und die Schweiz gegenüber Cyber-Bedrohungen schützen soll. Die 16 Massnahmen wurden in folgende 4 Bereiche unterteilt:

- Prävention: Risiko- und Verwundbarkeitsanalysen für kritische Infrastruktur Betreiber und Bundesverwaltung,
- Reaktion: Bedrohungslage, Vorfalls-Analyse und Täterschaft Identifikation,
- Kontinuität: Kontinuitäts- und Krisenmanagement und
- unterstützende Prozesse: Forschung und Kompetenzbildung, Internationale Zusammenarbeit und Rechtsgrundlagen.

**Organisation**
Um die Umsetzung der Massnahmen innerhalb der Bundesverwaltung und in Zusammenarbeit mit den Kantonen und der Wirtschaft zu koordinieren, hat der Bundesrat einen Steuerungsausschuss NCS (STA NCS) gegründet. Dieser hat zudem die Aufgabe, die Entwicklung der Cyber-Risiken zu verfolgen und dem Bundesrat diesbezügliche Empfehlungen für die Weiterentwicklung der Strategie vorzulegen. Unter dem Vorsitz des Eidgenössischen Finanzdepartementes (EFD) sind im Steuerungsausschuss vertreten: Die Departemente mit federführender Verantwortung für die Umsetzungsmassnahmen wie auch für die Kantone der Konsultations- und Koordinationsmechanismus Sicherheitsverbund Schweiz (KKM SVS). Auf operationeller und fachlicher Ebene koordiniert die Koordinationsstelle NCS (KS NCS) die Umsetzung der Strategie. Sie ist die Geschäftsstelle des Steuerungsausschusses. Angesiedelt ist die KS NCS bei der Melde- und Analysestelle Informationssicherung (MELANI) im Informatiksteuerungsorgan des Bundes (ISB).

[1] http://www.isb.admin.ch/themen/01709/01710/index.html?lang=de
[2] http://www.isb.admin.ch/themen/01709/01711/index.html?lang=de

Die NCS-Strategie ist Risiko-basierend und verfolgt einen dezentralen Ansatz, basierend auf dem Prinzip der Eigenverantwortung. Sie reduziert Cyber-Risiken grundsätzlich im Rahmen bestehender Strukturen und Zuständigkeiten und geht davon aus, dass die Verantwortung bei den Betreibern kritischer Infrastrukturen, der Wirtschaft und der Verwaltung liegen muss. Obwohl die Verantwortung dezentral liegt, unterstützt der Bund subsidiär. MELANI ist dabei die zentrale Informationsdrehscheibe. Auch ist die NCS eine sehr flexible Strategie, die bedarfsorientiere Lösungen zulässt und die nationale Zusammenarbeit zwischen Wirtschaft und den Behörden, sowie eine internationale Kooperation fördert.

Die Umsetzungsarbeiten für die in der Strategie definierten Massnahmen haben im Mai 2013 begonnen und unterliegen einer Wirksamkeitsüberprüfung im Jahr 2017. Die NCS hat einen strategischen Umsetzungsprozess ausgelöst, der jedoch auch im Jahr 2017 nicht beendet sein wird.

## Stand der Umsetzungsarbeiten NCS 2014

Die NCS befindet sich im zweiten Jahr der Umsetzung und die Arbeiten für die meisten Massnahmen sind weit fortgeschritten. Mit allen verantwortlichen Stellen hat die Koordinationsstelle NCS die Ziele und Meilensteine für die jeweiligen Massnahmen konkret definiert und in einer Roadmap dargestellt.

Prävention: In der Prävention sind die Massnahmen der Risiko- und Verwundbarkeitsanalyse, der Überprüfung der IKT-Verwundbarkeiten auf Stufe Bund sowie der Lagedarstellung enthalten.

- Für die erste Gruppe von Teilsektoren wurden im Bundesamt für wirtschaftliche Landesversorgung (BWL) und im Bundesamt für Bevölkerungsschutz (BABS) Verwundbarkeitsanalysen durchgeführt. Abgeschlossen wurde die Erdgasversorgung (BWL, Oktober 2014). Die Arbeiten in den Teilsektoren Stromversorgung, Informationstechnologien, Strassenverkehr und Luftverkehr (Zuständigkeit BWL) sowie Parlament, Regierung, Justiz und Verwaltung, Zivilschutz, Medien, Zivilschutz, Banken, Labor, Ärztliche Betreuung und Spitäler (Zuständigkeit BABS) wurden begonnen und sind gemäss Umsetzungsplan auf Kurs.
- Die Umsetzungsarbeiten zur Erstellung eines einheitlichen Lagebildes haben begonnen und ein Prototyp zur Darstellung der Bedrohungslage wurde erstellt. Auch wurden die Bestandsaufnahme und die Überprüfung der bestehenden Prozesse zur Erstellung der Bedrohungslage, der organisatorischen Abläufe sowie der Verantwortlichkeiten erfasst.

Reaktion: Im Bereich Reaktion muss eine koordinierte Vorfall-Analyse und Nachbearbeitung erfolgen, um einen Vorfall so rasch wie möglich zu beheben. Die NCS sieht einen Ausbau der Fähigkeiten und eine Steigerung der Reaktionsfähigkeit aller beteiligten Organisationen und Akteure vor. Somit ist gewährleistet, dass Vorfälle rasch analysiert werden können, die Strafverfolgung effizient handeln kann und eine Täterschaft schneller identifiziert werden kann.

- Die Bereitschaft im GovCERT konnte gesteigert werden und die optimale Verfügbarkeit im Normalbetrieb sichergestellt werden. The GovCERT Website is operational (www.govcert.ch).
- Der Verein «Swiss Cyber Experts (SCE)» wurde gegründet. Dadurch können nun auch Experten aus dem Verein SCE beigezogen werden
- Im Bereich der Bearbeitung staatschutzrelevanter Vorfälle, wurde im NDB eine neue Einheit aufgebaut (Cyber NDB) und mit den für die Umsetzung der NCS gesprochenen Ressourcen versehen.
- Die operative Zusammenarbeit für die Bewältigung von Cyber-Vorfällen zwischen den folgenden Akteuren ist ausgebaut worden: MilCERT und Computer Network Operations (CNO) in der Führungsunterstützungsbasis (FUB), dem Cyber NDB im Nachrichtendienst des Bundes (NDB), der Cyber Defence im Militärischen Nachrichtendienst (MND) und dem CSIRT im Bundesamt für Informatik und Telekommunikation (BIT).
- Die Armee hat die eigenen Detektions- und Analysemittel verstärkt.

Kontinuität: Die gezielte Durchführung eines Krisenmanagements setzt klar definierte Führungsabläufe und -prozesse für den Cyber-Fall voraus. Das Kontinuitätsmanagement sorgt dafür, dass die Geschäfts-

prozesse auch während einer Krise verfügbar sind. Die Arbeit im Bereich Kontinuität und Krisenmanagement haben für diejenigen kritischen Teilsektoren, die bereits ihre Risiko- und Schwachstellenanalyse durchgeführt haben, am 1. Januar 2015 begonnen.

- Das BWL konnte mit Vertretern der Gaswirtschaft konkrete Schritte zur Etablierung eines Kontinuitätsmanagements einleiten. Ziel ist die Unterzeichnung einer Branchenvereinbarung, in der sich die versorgungsrelevanten Unternehmen zur gegenseitigen Unterstützung im Falle eingetretener Cyber-Risiken verpflichten.
- Das Konzept für Führungsabläufe und -prozesse zur zeitgerechten Problemlösung ist erstellt und wurde auf die Kantone erweitert.

Unterstützende Prozesse: Als Grundlagen und Prozesse für die Bewältigung der Cyber-Problematik sind internationale Kooperationen, der Austausch von Erfahrungen im Bereich Bildung und Forschung (Kompetenzbildung) sowie gegebenenfalls eine Anpassung von gesetzlichen Grundlagen notwendig.

- Im Kern der Aktivitäten 2014, als die Schweiz den OSZE Vorsitz hatte, stand die Förderung von vertrauensbildenden Massnahmen im Cyber-Raum, um die Sicherheit, Transparenz und die Vorhersehbarkeit von Cyber-Bedrohungen zu erhöhen
- Im UNO-Rahmen engagierte sich die Schweiz für den Schutz der Privatsphäre im Cyber-Raum
- Die ENISA-Studie: «Framework for Evaluating National Cyber Security Strategies» wurde veröffentlicht. Die Schweiz beteiligte sich an der ENISA «Cyber Expert Working Group», sowie an der .«Cyber Expert Working Group» der OECD.
- Auf multilateraler Ebene hat die Schweiz den Sino-European Cyber-Dialog mitgestaltet. Dieser fand einmal in Genf und einmal in Peking statt.

# Wirksamkeitsüberprüfung

Der Bundesrat hat den Steuerungsausschuss NCS (STA NCS) beauftragt, ihm bis im Frühjahr 2017 eine Wirksamkeitsüberprüfung (WiÜ) vorzulegen. Eine externe Firma wurde beauftragt, diese WiÜ durchzuführen. Die WiÜ soll aufzeigen:

- inwieweit die Massnahmen der Strategie inhaltlich und organisatorisch umgesetzt worden sind und welcher Beitrag zur Erreichung der Ziele der NCS von ihnen erwartet werden kann,
- ob seitens der Bundesverwaltung die für die Umsetzung der Strategie gesprochenen personellen und finanziellen Ressourcen genutzt worden sind und ob sich insbesondere mit Blick auf die Zukunft ein weiterer Ressourcenbedarf ergibt,
- ob sich aufgrund der Ergebnisse der Überprüfung ein Handlungsbedarf ergibt, die NCS anzupassen.

Die Arbeiten zum Detailkonzept (im Detailkonzept wird das Konzept operationalisiert) haben begonnen.

Eine ausführliche Berichterstattung zur Umsetzung der NCS ist publiziert unter:
http://www.isb.admin.ch/themen/01709/01891/index.html?lang=de