Evaluation und Weiterentwicklung der Melde- und Analysestelle Informationssicherung Schweiz MELANI

2010

Center for Security Studies , ETH Zürich (CSS)
Autoren: Elgin Brunner, Manuel Suter
Projektleitung: Myriam Dunn Cavelty
Qualitässicherung: Victor Mauer und Andreas Wenger

CSS ETH Zurich
ETH Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Kontakt:
Center for Security Studies (CSS)
ETH Zürich
Seilergraben 45-49
CH-8092 Zürich
Schweiz
Tel.: +41-44-632 40 25
css@sipo.gess.ethz.ch

Executive Summary

Auftrag und Inhalt

Gemäss eines Auftrag des Bundesrats wurde die Melde- und Analysestelle Informationssicherung (MELANI) 2006 evaluiert. Aufgrund der positiven Ergebnisse wurde entschieden, MELANI in der bisherigen Form weiterzuführen. Seither haben sich einige wichtige Neuerungen ergeben. Deshalb hat die strategische Leitung von MELANI, das Informatikstrategieorgan Bund (ISB), das Center for Security Studies (CSS) der ETH Zürich mit einer erneuten Evaluation und dem Entwurf von Weiterentwicklungsoptionen beauftragt. Die vorliegende Studie umfasst a) die Wirksamkeitsprüfung von MELANI, b) einen Vergleich des MELANI-Modells mit anderen internationalen Modellen zur Informationssicherung sowie c) daraus abgeleitete Weiterentwicklungsoptionen und Empfehlungen.

Wirksamkeitsprüfung MELANI

Um zu erfahren, wie die Qualität der Arbeit von MELANI bewertet wird, wurden eine online-Umfrage bei allen Mitgliedern des geschlossenen Kundenkreises und Interviews mit Vertretern aus ausgewählten Sektoren durchgeführt. Das Ergebnis zeigt, dass MELANI die Erwartungen seiner Kunden in hohem Mass erfüllt. Die spezifischen Dienstleistungen von MELANI werden gut bis sehr gut bewertet. In besonderem Mass wird die Arbeit von MELANI von den Vertretern des Finanzsektors anerkannt.

Drei idealtypische Modelle zur Informationssicherung

Aus Ansätzen zur Informationssicherung in anderen Ländern lassen sich drei idealtypische Modelle mit spezifischen Stärken und Schwächen ableiten: 1) Das Modell „IT-Sicherheitsbehörde“ bezeichnet einen ausdifferenzierten und hierarchisch gegliederten Verwaltungsapparat mit umfassenden Aufgaben im Bereich der Informationssicherung; 2) Das „Blumenmodell“ hat einen Fokus auf Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor und Autonomie in den verschiedenen Sektoren (das Organigramm kann als Blume gezeichnet werden); 3) Beim „GovCERT+“ Modell stehen CERT-Dienstleistungen für die Verwaltung und die Betreiber kritischer Infrastrukturen im Vordergrund.

MELANI im internationalen Vergleich

Heute ist MELANI am ehesten mit dem Modell eines GovCERT+ vergleichbar. Als gewichtigste Schwächen des GovCERT+-Modells gelten die schwache Förderung des Informationsaustausches zwischen den Unternehmen sowie der Mangel an klaren Kriterien für die Mitgliedschaft im GK. Auch MELANI ist mit diesen Schwierigkeiten konfrontiert. Hauptstärke des GovCERT+-Modells ist, dass mit wenig Mitteln relativ viel erreicht werden kann. Jedoch sind die MELANI gegenwärtig zur Verfügung stehenden Mittel auch für ein GovCERT+-Modell äusserst knapp.

Weiterentwicklungsoptionen MELANI

In Anlehnung an die idealtypischen Modelle werden vier mögliche Zukunftsoptionen skizziert: 1) Weiterführung von MELANI bei gleichbleibenden Mitteln; 2) Konsolidierung der bisherigen Arbeit durch Ausbau der CERT-Funktion; 3) Umgestaltung von MELANI zu einer umfassenden Plattform für Informationsaustausch: 4) Pragmatische Umsetzung der dritten Option für ausgewählte Sektoren. Die Weiterentwicklungsoptionen unterscheiden sich hinsichtlich des benötigten Aufwandes, in Bezug auf die Aufgaben, für welche MELANI verantwortlich wäre und in Bezug auf die Struktur des geschlossenen Kundenkreises.

Empfehlungen

Um eine der Optionen auswählen zu können, sollte eine Strategie des Bundes zur Informationssicherung erarbeitet werden, welche den Grundauftrag und die Ziele von MELANI definiert. Als Sofortmassnahme gegen die identifizierten Schwächen sollte in Betracht gezogen werden, für ausgewählte Sektoren (insbesondere Finanzsektor) eine Plattform für den Informationsaustausch zu erstellen.

1 Einleitung

Ausgangslage

Die Informations- und Kommunikationstechnologien (IKT) sind aus dem Alltag der meisten Schweizer Firmen und Behörden nicht mehr wegzudenken. Sie ermöglichen ein vernetztes Arbeiten und vereinfachen die Kommunikation. Mit der Anwendung der neuen Technologien entstehen aber auch neue Probleme: Die zunehmende Abhängigkeit von den Informations- und Kommunikationstechnologien in den verschiedensten Tätigkeitsfeldern sowie die zuweilen zu beobachtende Sorglosigkeit bei ihrer Nutzung erhöhen die Gefahr von IKT-Pannen und Vorfällen, die das reibungslose Funktionieren von Geschäftsprozessen in der Wirtschaft und in der Verwaltung verhindern oder unter Umständen sogar die nationale Sicherheit der Schweiz gefährden könnten.

Der Staat, gemäss Bundesverfassung „der gemeinsamen Wohlfahrt" verpflichtet, hat als Anbieter des Kollektivguts Sicherheit die neuen Herausforderungen erkannt. Mehrmals hat der Bundesrat seinen Willen bekundet, die Informations- und Kommunikationsinfrastrukturen in der Schweiz vor Missbrauch, Ausfällen und Angriffen zu schützen, so etwa mit der Verabschiedung des Konzepts „Information Assurance" (Informationssicherung) vom 28. Juni 2000, der Schaffung der Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK sowie mit Beschluss vom 29. Oktober 2003 mit dem Aufbau und Betrieb der Melde- und Analysestelle Informationssicherung MELANI.

Melde- und Analysestelle Informationssicherung MELANI

MELANI ist seit Oktober 2004 operativ tätig. Ihre zentrale Aufgabe ist die Früherkennung von Problemen in der Informations- und Kommunikationsinfrastruktur. MELANI bedient dabei zwei Kundengruppen: den *„Geschlossenen Kundenkreis" (GK),* dazu gehören ausgewählte Betreiber von nationalen kritischen Infrastrukturen in der Schweiz; und den *„Offenen Kundenkreis" (OK)*, der private Computer- und Internetbenutzer sowie kleinere und mittlere Unternehmen (KMU) in der Schweiz umfasst. Dabei sind die Dienste für den GK die Hauptaufgabe von MELANI. MELANI informiert die Mitglieder des GK über neue Bedrohungen und Gefahren, unterstützt sie bei Vorfällen und bietet Workshops zu ausgewählten Themen an.

MELANI Evaluation 2006

Im Jahr 2006 wurde MELANI vom Center for Security Studies (CSS) der ETH Zürich evaluiert. Im Rahmen dieser Evaluation wurden zwei Studien erstellt:

1. Erstens wurde eine Erhebung bei 500 Unternehmen in der Schweiz durchgeführt. Ziel dieser Studie war es, eine Übersicht über das Wissen, den Mitteleinsatz und die Schutzvorkehrungen der Schweizer Wirtschaft betreffend die Informationssicherung zu erhalten.[1]
2. Zweitens wurde – ausgehend von den Resultaten der 1. Teilstudie – der Frage nachgegangen, wie MELANI a) im internationalen Vergleich dasteht; b) von anderen Bundesstellen, die eine Rolle im Bereich der Informationssicherheit spielen, eingeschätzt wird; und c) von den Grossunternehmen, die zum geschlossenen Kundenkreis von MELANI-Net gehören, bewertet wird.

Die Studien zeigten auf, dass MELANI als neutrale und vertrauenswürdige Plattform für die Kooperation aller wichtigen Partner (aus der Privatwirtschaft und der Bundesverwaltung) einen wichtigen Beitrag zur

[1] Siehe: Manuel Suter (2006), Informationssicherheit in Schweizer Unternehmen: eine Umfragestudie über Bedrohungen, Risikomanagement und Kooperationsformen, Zürich: Center for Security Studies. Online unter: http://129.132.36.135/serviceengine/Files/CRN/25402/ipublicationdocument_singledocument/67d949c7-7ee4-4616-8469-f284278a3410/de/InfosecSwissComp_dt.pdf.

Informationssicherung bei kritischen Infrastrukturen leistet. Entsprechend entschied der Bundesrat im Januar 2007, dass MELANI in der bisherigen Form weitergeführt werden soll.

MELANI Weiterentwicklung 2010

MELANI ist nun seit mehr als 5 Jahren im Einsatz, und hat sich seit der Evaluation im Jahr 2006 in zweierlei Hinsicht verändert: Erstens ist der GK stark angewachsen und umfasst heute dreimal so viele Unternehmen wie 2006 und zweitens wurde das GovCERT.ch aufgebaut.[2] Aufgrund dieser Entwicklungen hat sich die Leitung von MELANI entschieden, eine erneute Evaluation durchführen zu lassen, um zu überprüfen inwiefern sich diese Veränderungen auf die Qualität der Arbeit von MELANI ausgewirkt haben. Im Zentrum steht dabei a) die Wirksamkeitsprüfung von MELANI bzw. die Einschätzung der Dienstleistungen von MELANI durch ihre Hauptkunden, b) ein Vergleich des MELANI-Modells mit anderen internationalen Modellen zur Informationssicherung sowie c) daraus abgeleitete Weiterentwicklungsoptionen und Empfehlungen.

Struktur der Studie

Demgemäss gliedert sich die vorliegende Studie in vier Teile:

1) *Wirksamkeitsprüfung MELANI*: Es wird untersucht, wie die Mitglieder des GK die Qualität der Arbeit von MELANI heute bewerten. Zu diesem Zweck wurde eine Umfrage bei allen Mitgliedern des GK und Interviews mit Vertretern aus ausgewählten Sektoren durchgeführt. Der Fokus der Evaluation liegt dabei auf dem Zeitraum zwischen 2006 (letzte Evaluation) und Ende 2009 (Durchführung der Evaluation).
2) *Vergleich mit internationalen Modellen zur Informationssicherung*: Die Struktur und der Aufbau von MELANI werden mit anderen staatlichen Modellen zur Informationssicherung verglichen. Dies soll helfen, die Stärken und Schwächen von MELANI zu verdeutlichen und Vor- und Nachteile der verschiedenen Modelle zu identifizieren.
3) *Weiterentwicklungsoptionen MELANI*: Aufgrund der Erkenntnisse aus den Teilen 1 und 2 werden in Teil 3 mögliche Optionen für eine Weiterentwicklung von MELANI aufgezeigt und diskutiert.
4) *Empfehlungen:* Abschliessend werden Empfehlungen für das weitere Vorgehen formuliert.

Methode der Evaluation

Der Erfolg bzw. die Wirkung von MELANI kann anhand der Zufriedenheit der Mitglieder des GK in Bezug auf die Dienstleistungen und Aktivitäten von MELANI gemessen werden. Zur Erhebung der Daten für die Wirksamkeitsprüfung von MELANI wurden alle Einzelmitglieder des GK eingeladen, an einer online-Befragung teilzunehmen. Da die Unternehmen mehrere Vertreter in den GK von MELANI delegieren können, haben teilweise mehrere Personen aus der gleichen Firma an der Umfrage teilgenommen. Das Vorgehen wurde aber bewusst so gewählt, damit in den Resultaten die individuellen Bedürfnisse und nicht unbedingt eine aggregierte Unternehmenssicht abgebildet werden. Von 196 angeschriebenen Personen haben 108 den Fragebogen vollständig ausgefüllt. Das ergibt eine hohe Rücklaufquote von 55%, welche solide Rückschlüsse auf die Meinungen der Mitglieder im GK erlaubt. Um die Ergebnisse aus der Umfrage zu konsolidieren und um bei einigen Fragen zusätzliche Aspekte zu überprüfen, wurden zusätzlich drei mündliche Interviews mit Vertretern aus den Sektoren Telekommunikation, Energie und Finanz

[2] CERT steht als Abkürzung für Computer Emergency Response Team. Das GovCERT.ch ist innerhalb von MELANI für die Bewältigung von Vorfällen und deren technische Analyse zuständig. Das GovCERT.ch ist seit dem 1. April 2008 operativ.

geführt. Drei Viertel aller Mitglieder im GK stammen aus diesen drei Sektoren, weshalb ein vertiefter Eindruck über die Wahrnehmung dieser Branchen von speziellem Interesse ist.

Für den internationalen Vergleich wurde auf bestehende Literatur und bereits vorhandenes Wissen zurückgegriffen. Die verschiedenen Weiterentwicklungsoptionen wurden aus den Ergebnissen abgeleitet und mit Fachexperten diskutiert.

2 Wirkungsevaluation im geschlossenen Kundenkreis (GK)

In diesem Kapitel werden die Ergebnisse aus der online-Umfrage diskutiert, wobei die Erkenntnisse aus den Interviews direkt in die Darstellung dieser Ergebnisse einfliessen und sie in wichtigen Punkten ergänzen. Im Unterkapitel wird zuerst auf die wichtigsten Entwicklungen von MELANI und dem GK seit der letzten Evaluation von 2006 eingegangen. In einem zweiten wird die allgemeine Einschätzung von MELANI geschildert. Das dritte Unterkapitel untersucht die Bewertung der einzelnen Dienstleistungen von MELANI. Das vierte widmet sich dem Thema Informationsaustausch mit Hilfe von MELANI. Abschliessend wird umrissen, welche Wünsche die Mitglieder des GK bezüglich Weiterentwicklung von MELANI haben.

2.1 Die Entwicklung von MELANI seit 2006

Um die Ergebnisse der Befragung richtig interpretieren zu können, sollten Entwicklungen im Kundenkreis von MELANI in den letzten drei Jahren sowie Veränderungen bei MELANI (in Bezug auf die interne Organisation) in Betracht gezogen werden.

2.1.1 Mitgliedschaft im GK

Seit 2006 hat sich der GK insbesondere hinsichtlich der Anzahl der Mitglieder stark verändert. Während der GK im Jahr 2006 noch 23 Firmen und Behörden umfasste, sind es heute 73 Firmen und Behörden. Die Anzahl der vertretenen Einzelpersonen ist dadurch von ca. 60 auf über 200 gestiegen. Dieses starke Wachstum zeigt, dass MELANI auf grosses Interesse bei den Partnern aus der Privatwirtschaft stösst, stellt aber auch eine grosse Herausforderung für MELANI dar: Eine höhere Anzahl Mitglieder bedeutet nicht nur einen grösseren Aufwand in der täglichen Arbeit, sondern auch verstärkte Konfrontation mit unterschiedlichen, teilweise sogar divergierenden Erwartungen und Wünschen. Die Tabelle 1 vergleicht die Mitgliedszahlen sowie die Aufteilung auf die verschiedenen Sektoren von 2006 mit den Zahlen von heute:

Tabelle 1

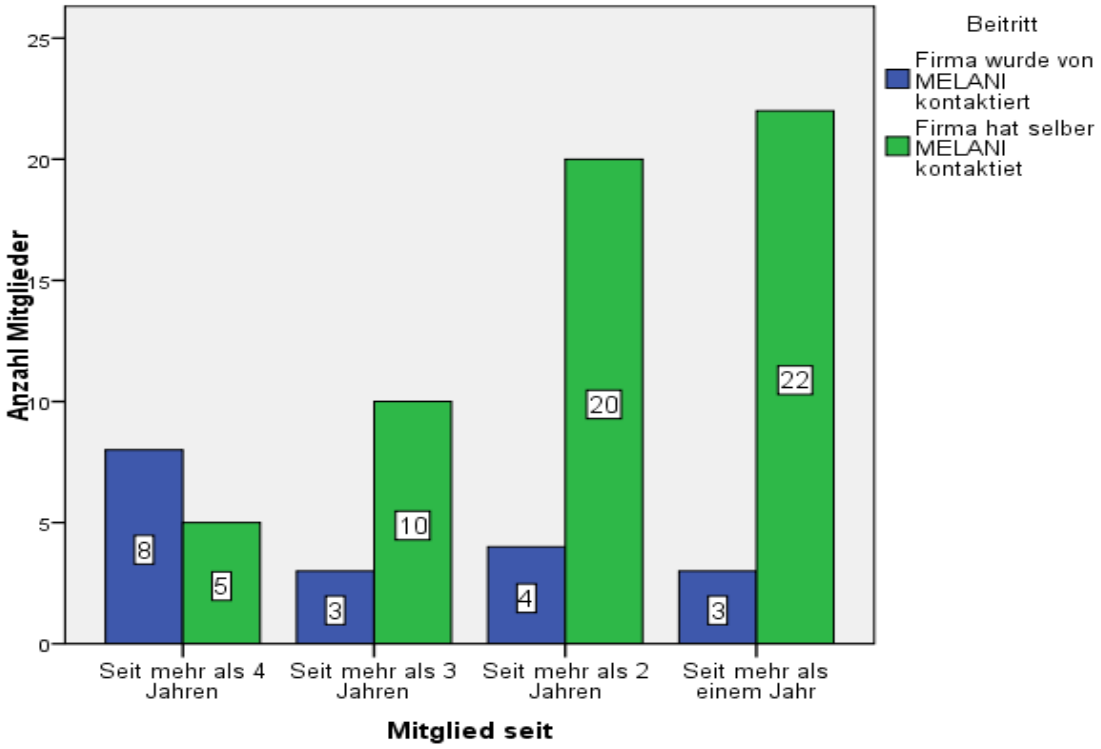
Sektoren	2006	2010
Chemie / Pharma		1
Energie	2	9
Finanzen	9	33
Versicherungen		1
Gesundheitswesen	1	4
Industrie		2
Telekommunikation	5	8
Transport / Logistik	2	5
Verwaltung	4	10
Total Firmen	23	73
Anzahl Personen	ca. 60	ca. 200

Dieser Vergleich zeigt deutlich, dass der Finanzsektor mit Abstand am stärksten gewachsen ist. Die Zahl der beteiligten Firmen aus diesem Sektor stieg von 9 auf 33. Bezüglich der Anzahl der vertretenen Firmen nimmt der Finanzsektor heute deshalb eine dominierende Rolle ein – über 50% der Mitglieder aus der Privatwirtschaft stammen aus dem Finanzsektor. Obwohl es zu berücksichtigen gilt, dass der Finanzsektor

im Vergleich zu anderen Sektoren (beispielsweise Energie oder Telekommunikation) generell mehr Firmen beinhaltet und auch darum mehr Vertreter im GK hat, kann man doch feststellen, dass er überdurchschnittlich stark vertreten ist. Diese starke Zunahme von Mitgliedern aus dem Finanzsektor lässt sich mit dem Erfolg von MELANI bei der Unterstützung der Banken im Kampf gegen Phishing und ähnliche Vorfälle erklären,[3] die die Mitgliedschaft im GK für andere Unternehmen aus dem Finanzsektor attraktiv machte. Neben dem Finanzsektor wurde auch der Energiesektor (von 2 auf 9 Firmen) ausgebaut und die Beteiligung aus der öffentlichen Verwaltung verstärkt (von 4 auf 10 öffentliche Stellen).

Angesichts des starken Ausbaus des GK interessiert, ob das Wachstum auf Rekrutierungsbemühungen von MELANI zurück zu führen ist oder ob die Firmen von sich aus den Wunsch äussern, in den GK aufgenommen zu werden. In der Evaluation wurde deshalb gefragt, auf wessen Initiative die Mitgliedschaft der Firma im GK entstanden ist. Die Antworten zu dieser Frage zeigen sich in Darstellung 1, gruppiert nach der Dauer der Mitgliedschaft.

Darstellung 1



Die Auswertung zeigt, dass relativ viele der älteren Mitglieder von MELANI rekrutiert worden sind, während sich die grosse Mehrheit der jüngeren Mitglieder selber um eine Mitgliedschaft im GK beworben hat. Dies weist darauf hin, dass MELANI bei den relevanten Unternehmen bekannt ist und wenig Überzeugungsarbeit leisten muss, um neue Mitglieder zu gewinnen. Dies heisst aber auch, dass MELANI vor der zentralen Herausforderung steht, den Mitgliederkreis im GK in Zukunft aktiv zu gestalten und – wo nötig –auch zu beschränken. Dieser Faktor spielt in den verschiedenen Weiterentwicklungsoptionen (Teil 3) eine zentrale Rolle.

[3] Vgl. Evaluationsbericht 2006.

2.1.2 Entwicklungen bei MELANI

Seit 2006 gibt es auch bei MELANI einige Veränderungen. Die erste wichtige Änderung betrifft die Gründung eines eigenen Computer Emergency Response Teams (GovCERT.ch), das im Jahr 2008 operativ wurde. Das GovCERT.ch hat die Aufgaben des SWITCH-CERTs übernommen, nachdem die Zusammenarbeit mit SWITCH beendet wurde..[4] Dieser Wechsel stellte MELANI vor grosse Herausforderungen, da das SWITCH-CERT als wichtiger Partner im MELANI Modell eine Fülle von technischem Know-how zur Verfügung gestellt hat und sowohl national als auch international stark vernetzt ist. Das GovCERT.ch ist aber erfolgreich gestartet und wurde im Februar 2010 im wichtigsten internationalen Netzwerk für CERTs, dem Forum for Incident Response and Security Teams (FIRST), als Mitglied aufgenommen. Damit hat MELANI den Zugang zu wichtigen internationalen Informationen und Kontakten wieder sicherstellen können. Der Wechsel vom SWITCH-CERT zum GovCERT.ch ist aber dennoch eine wichtige Änderung und muss deshalb bei der Evaluation beachtet werden.

Die zweite grosse Veränderung betrifft die Reorganisation der zivilen Nachrichtendienste der Schweiz. Der Dienst für Analyse und Prävention (DAP) der Bundespolizei und der Strategische Nachrichtendienst (SND) wurden per 1. Januar 2010 im neuen Nachrichtendienst des Bundes (NDB) zusammengeführt, der dem Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS)[5] angegliedert wurde. Weil der DAP für die nachrichtendienstlichen Tätigkeiten bei MELANI zuständig war, hat diese Reorganisation auch direkte Auswirkungen auf MELANI. Neu ist somit der nachrichtendienstliche Teil von MELANI über den NDB dem VBS und nicht mehr dem EJPD angegliedert. Inwiefern diese Änderung die Zusammenarbeit mit der Bundespolizei und mit den Strafverfolgungsbehörden in den Kantonen tangiert, ist gegenwärtig noch unklar. Beide Veränderungen haben einen Einfluss auf MELANI als Dienstleister und auf die Weiterentwicklungsoptionen.

2.2 Allgemeine Einschätzung von MELANI durch die Mitglieder des GK

Die Evaluation von 2006, die auf Interviews mit ausgewählten Mitgliedern des GK basierte, ergab ein sehr positives Bild von MELANI. Die Vertreter der Wirtschaft begrüssten insbesondere das Konzept der *Public-Private Partnerships* in welchem der Staat gemeinsam mit der Privatwirtschaft die Herausforderungen der Informationssicherung zu bewältigen versucht. Im folgenden Abschnitt soll untersucht werden, ob sich dieses Modell der Zusammenarbeit weiterhin bewährt (auch unter den veränderten Umständen wie in Kapitel 2.1.2 beschrieben). Konkret wird überprüft, ob es MELANI in den letzten Jahren gelungen ist, die Erwartungen der Mitglieder des GK zu erfüllen und welche Bedeutung die Mitglieder des GK MELANI für die Bewältigung der Herausforderungen im Bereich der Informationssicherheit zuschreiben.

2.2.1 Erwartungen der Mitglieder des GK

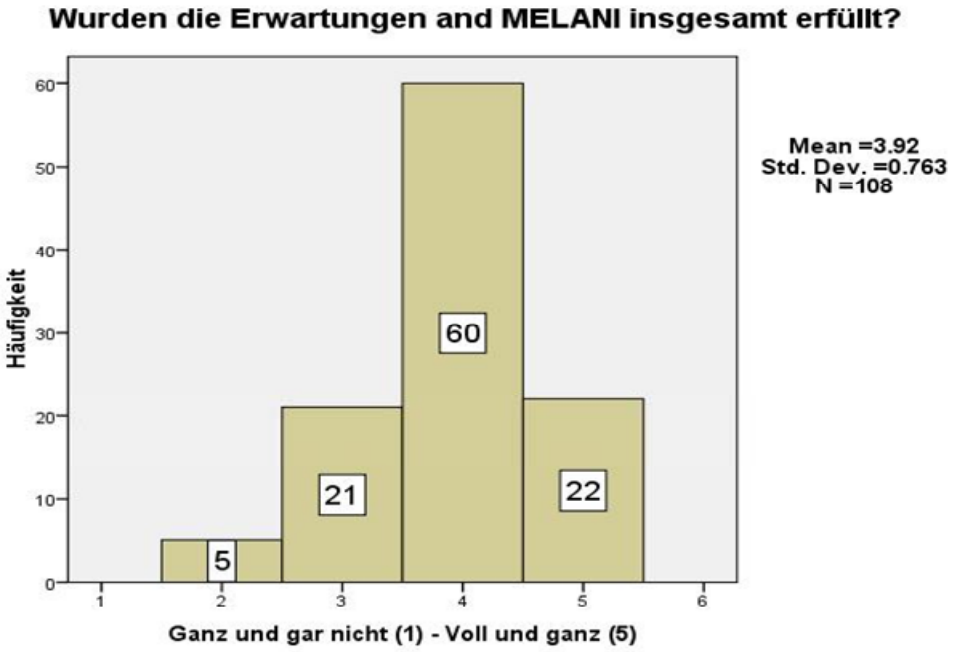
Obwohl sehr unterschiedliche Firmen im GK vertreten sind, gelingt es MELANI mehrheitlich, deren Erwartungen zu erfüllen (siehe Darstellung 2):

---

4 SWITCH-CERT war bis 2007 Kooperationspartner von MELANI. Heute bietet das SWITCH-CERT seine Dienstleistungen für einen eigenen Kundenkreis an.

5 http://www.vbs.admin.ch/internet/vbs/de/home/departement/organisation/ndb.html

Darstellung 2



22 Mitglieder des GK sehen ihre Erwartungen an MELANI voll und ganz erfüllt, und das Gesamtbild zeigt, dass die Erwartungen der Mehrheit der Befragten zum grossen Teil erfüllt werden. Besonders zufrieden mit MELANI sind die Firmen aus dem Finanzsektor. Der Mittelwert der Bewertungen von MELANI durch diese Firmen liegt bei 4.07, während der Mittelwert der übrigen Firmen bei 3.73 liegt.[6] Besonders die Kontakte zum CERT werden von den Firmen aus dem Finanzsektor wesentlich besser beurteilt als von den übrigen Firmen.[7] Aus den Interviews mit Exponenten sowohl aus dem Finanz- als auch aus dem Energiesektor geht hervor, dass das CERT für die Firmen aus dem Finanzsektor, die überdurchschnittlich häufig von Attacken auf ihre Informationssicherheit betroffen sind, eine zentrale Rolle spielt. Firmen aus anderen Sektoren (z.B. Energiesektor oder Transportsektor) verzeichnen weniger Angriffe und sind darum in ihrem täglichen Geschäft auch kaum auf das CERT von MELANI angewiesen.

Neben den Unterschieden zwischen den Sektoren wurde auch überprüft, ob es Unterschiede zwischen der Zufriedenheit von älteren und neueren Mitgliedern gibt. Es konnten aber keine signifikanten Unterschiede festgestellt werden.

2.2.2 Wichtigkeit von MELANI für die Informationssicherung

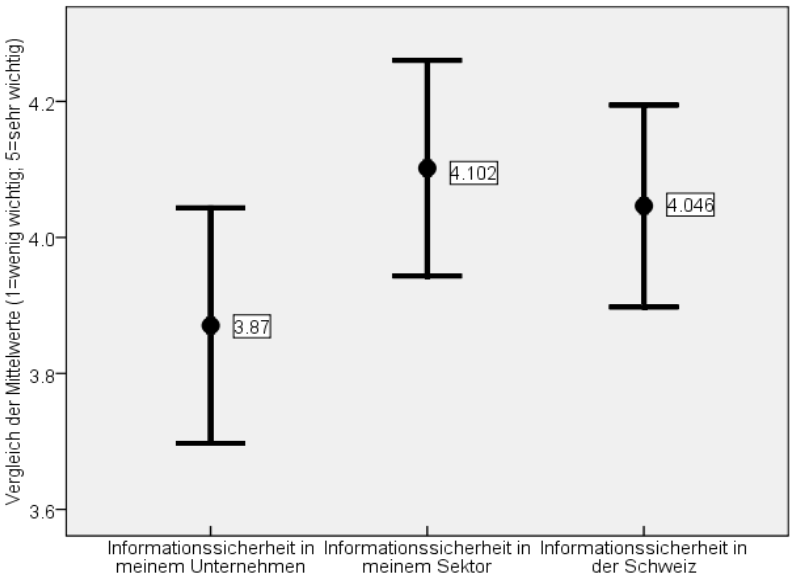
Die Teilnehmer der Befragung wurden auch gebeten einzuschätzen, wie wichtig MELANI für a) die Informationssicherheit in ihrem Unternehmen, b) die Informationssicherheit in ihrem Sektor und c) die Informationssicherheit in der Schweiz ist. Die Darstellung 3 vergleicht die Antworten zu diesen drei Fragen:

---

6 Die Differenz zwischen den Mittelwerten ist signifikant, bei einer Irrtumswahrscheinlichkeit von 2.5%.

7 Neben der Frage, ob die Erwartungen insgesamt erfüllt worden sind, wurde auch Bewertungen zu spezifischeren Erwartungen erfragt. So konnten die Befragten angeben, ob MELANI ihnen die Kontakte zu CERTS erleichtert hat. Auf einer Skala von 1 (trifft überhaupt nicht zu) bis 5 (trifft voll und ganz zu) liegen die Mittelwerte für Teilnehmer aus dem Finanzsektor bei 4.21, für Teilnehmer aus anderen Sektoren bei 3.62. Diese Differenz ist signifikant bei einer Irrtumswahrscheinlichkeit von 0.2%.

Darstellung 3



N=108; die Resultate sind für ein Konfidenzintervall von 95% dargestellt.

Die Mitglieder des GK beurteilen die Wichtigkeit von MELANI für die Informationssicherheit im Durchschnitt als eher wichtig. Auf der Skala von 1 (wenig wichtig) bis 5 (sehr wichtig) liegen die Bewertungen bei ca. 4. Dabei stufen die Befragten die Wichtigkeit für ihr eigenes Unternehmen etwas tiefer ein als die Wichtigkeit für die Informationssicherheit in ihrem Sektor oder für die Schweiz insgesamt.[8] Diese Resultate entsprechen der Grundidee von MELANI: Es ist nicht die primäre Aufgabe von MELANI, die Informationssicherheit der einzelnen Unternehmen zu verbessern (denn dies liegt in der Verantwortung der betroffenen Firmen selber). Es entspricht aber durchaus MELANIs Selbstverständnis, auf der Ebene der Sektoren oder der Schweiz insgesamt eine Rolle zu spielen, da diese Koordinationsaufgabe kaum von einem Unternehmen freiwillig übernommen wird.

Bemerkenswert in diesem Zusammenhang ist auch, dass die Wichtigkeit für den eigenen Wirtschaftssektor vor allem von Firmen aus dem Finanzsektor hoch eingeschätzt wird. 42% der Firmen aus dem Finanzsektor bezeichnen MELANI als sehr wichtig für ihren Sektor und der Mittelwert der Beurteilungen liegt mit 4.25 höher als bei den übrigen Firmen (3.92).[9] Im Gespräch mit Vertretern aus der Finanzbranche wurde bestätigt, dass im Finanzsektor die Zusammenarbeit zwischen den Unternehmen im Bereich Informationssicherung als besonders wichtig betrachtet wird. MELANI übernimmt in diesem Zusammenhang eine wichtige Funktion als Plattform für den Informationsaustausch (dazu später mehr).

2.3 Dienstleistungen von MELANI an die Mitglieder

Die insgesamt gute Beurteilung von MELANI durch die Mitglieder des GK lässt darauf schliessen, dass die Firmen mit den Dienstleistungen von MELANI im allgemeinen zufrieden sind. Dennoch ist es wichtig zu verstehen, welche Dienstleistungen für den Privatsektor besonders nützlich sind und wie sie im ein-

8 Die Differenz der Mittelwerte ist signifikant, die Irrtumswahrscheinlichkeit liegt bei 0.1% für die Differenz zwischen „Informationssicherheit in meinem Unternehmen“ und „Informationssicherheit in meinem Sektor“ und bei 3.6% für die Differenz zwischen „Informationssicherheit in meinem Unternehmen“ und „Informationssicherheit in der Schweiz“.

9 Der t-Wert des Mittelwertvergleiches beträgt 2.10, bei einer Irrtumswahrscheinlichkeit von 3.8%. Der Unterschied kann also als signifikant bezeichnet werden.

zelnen bewertet werden. Die Mitglieder des GK wurden deshalb zu den folgenden Dienstleistungen von MELANI befragt:

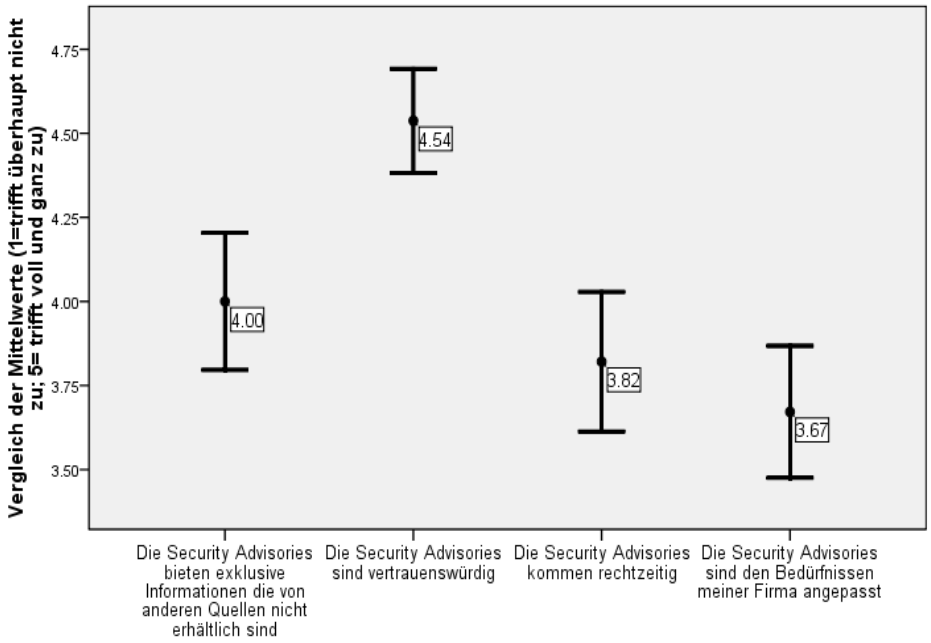
- Security Advisories
- Unterstützung bei Vorfällen
- Workshops

Konkret wurden die Mitglieder des GK gefragt, wie häufig die Dienstleistungen von MELANI genutzt werden, wie zufrieden die Vertreter der Firmen mit den Dienstleistungen sind und wo ihrer Meinung nach Verbesserungspotential besteht.

2.3.1 Bewertung der Security Advisories

Befragte, die in den letzten drei Jahren *Security Advisories* erhalten haben,[10] bewerten diese insgesamt als gut (auf einer Skala von 1= ungenügend bis 4 = sehr gut, liegt der Mittelwert bei 3.06). Die Teilnehmer der Umfrage wurden gebeten, die Qualität der *Security Advisories* anhand der Kriterien Exklusivität, Vertrauenswürdigkeit, Rechtzeitigkeit und Konformität mit den Bedürfnissen der Firmen zu beurteilen. Die Darstellung 4 vergleicht die Mittelwerte der Bewertungen mit diesen 4 Kriterien (die Skala reicht dabei von 1= Kriterium trifft überhaupt nicht zu bis 5= Kriterium trifft voll und ganz zu).

Darstellung 4: Bewertung Security Advisories



N=68; die Resultate sind für ein Konfidenzintervall von 95% dargestellt.

Deutlich am besten bewertet wird die Vertrauenswürdigkeit der Mitteilungen durch MELANI. Dies kann auf das generell hohe Vertrauen der Mitglieder in MELANI zurückgeführt werden (vgl. unten) und auf den Umstand, dass MELANI ein „neutraler" Anbieter von Warnungen und Tipps ist, d.h. im Gegensatz zu anderen Warndiensten keine kommerziellen Interessen verfolgt. Vor allem dieser letzte Aspekt wurde auch in den geführten Interviews mehrfach hervorgehoben.

Ebenfalls recht hoch bewertet wird die Exklusivität der Meldungen. Es wurde jedoch von einigen Teilnehmern der Umfrage angemerkt, dass die Exklusivität zusätzlich erhöht werden könnte, wenn MELANI mehr Informationen zur allgemeinen Gefahren- und Bedrohungslage liefern würde. Auch dieser Wunsch

[10] Insgesamt waren dies 68 Mitglieder des GK.

nach mehr Informationen zur generellen Bedrohungslage wurde in den einzelnen Interviews mehrfach geäussert. Die Rechtzeitigkeit der Informationen wird nochmals etwas tiefer bewertet. In den Kommentaren wird deutlich, dass diese Einschätzung vor allem damit zusammenhängt, dass die Firmen auch andere Informationskanäle nutzen, die teilweise schneller sind.[11] Die tiefste Bewertung erhalten die *Security Advisories* hinsichtlich ihrer Konformität mit den Bedürfnissen der Firmen. Angesichts der Diversität der Firmen im GK ist dies nicht weiter erstaunlich.

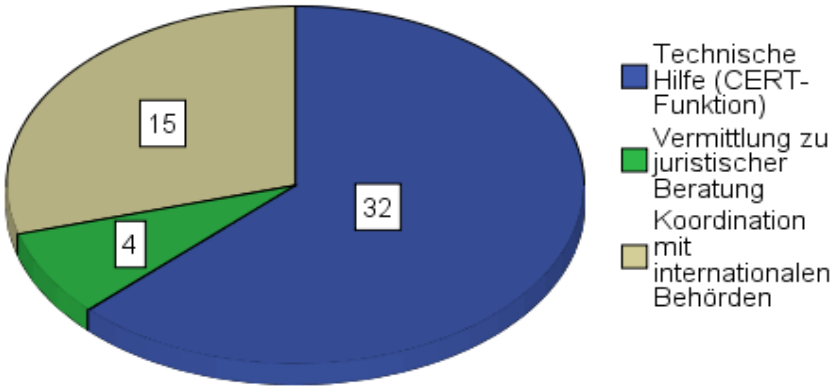
Wie verschieden die Bedürfnisse sind, zeigt auch die Beantwortung der Frage, ob mehr oder weniger *Security Advisories* gewünscht werden: die Hälfte der Befragten (50.7%) möchte häufiger *Security Advisories* erhalten, die andere Hälfte (49.3%) hält die momentane Häufigkeit für genau richtig. Niemand hingegen denkt, dass MELANI zu viele Mitteilungen verschickt.

Zusammengefasst lässt sich sagen, dass die Qualität der *Security Advisories* als gut befunden wird, dass sich die Firmen aber noch mehr qualifizierte und möglichst spezifische Einschätzungen wünschen. In den Kommentaren aus der Befragung und in den Gesprächen mit Vertretern aus verschiedenen Sektoren wurde mehrfach darauf hingewiesen, dass Informationen aus nicht-öffentlichen Quellen über die allgemeine Bedrohungslage in der Schweiz und im Ausland für die Firmen von besonderem Interesse wären. Daraus lässt sich ableiten, dass der Wert der *Security Advisories* zusätzlich gesteigert werden könnte, wenn es MELANI gelänge, vermehrt solche Informationen zu gewinnen und den Mitgliedern des GK zur Verfügung zu stellen.

2.3.2 Unterstützung bei Vorfällen

Die Bewertung der Hilfe bei Vorfällen fällt insgesamt sehr positiv aus. Glücklicherweise sind grössere Störungen der Informationssicherheit in den meisten Firmen aber selten; die CERT-Dienstleistungen von MELANI mussten deshalb längst nicht von allen Befragten in Anspruch genommen werden. Insgesamt gaben 38 Befragte an, in den letzten drei Jahren Hilfe von MELANI bei einem Vorfall beansprucht zu haben. Von diesen 38 stammen 23 aus dem Finanzsektor, was wiederum verdeutlicht, dass dieser Sektor besonders für Angriffe auf die Informationsinfrastruktur exponiert ist. Die Art der Hilfe, die betroffene Unternehmen von MELANI erhalten haben, sind in Darstellung 5 abgebildet:

Darstellung 5



Technische Hilfe wurde am häufigsten genannt, aber auch die Koordination mit internationalen Behörden scheint ein wichtiger Bestandteil der Hilfeleistungen zu sein. Betont wurde auch, dass MELANI eine wichtige Rolle bei der Vermittlung von Kontakten zu nationalen und internationalen *Internet Service Pro-*

[11] Als Beispiele werden abuse.ch oder heise.de genannt.

viders (ISPs) spielen kann. In diesem Zusammenhang bedauerten einige der Befragten, dass das CERT der Stiftung SWITCH nicht mehr Teil von MELANI ist. Für MELANI wird es in Zukunft wichtig sein, eine möglichst gute Zusammenarbeit mit dem SWITCH-CERT (und anderen Organisationen mit technischem Know-how im Bereich Informationssicherung) anzustreben, so dass auch auf externes Wissen zurückgegriffen werden kann.

Die Tatsache, dass nur ein Drittel der Befragten Hilfe beansprucht hat, sollte nicht dazu verleiten, die CERT-Funktion von MELANI zu unterschätzen. Bei der Vorfallbekämpfung kann MELANI seinen Mitgliedern aus der Privatwirtschaft einen teilweise grossen Mehrwert bieten: 26 der 38 Mitglieder, die Hilfe beansprucht haben, bezeichnen die Unterstützung durch MELANI bei der Bekämpfung des Vorfalls als entscheidend.[12] Die Wichtigkeit der Unterstützung durch das GovCERT bei Vorfällen wurde auch im Gespräch mit Vertretern aus dem Finanzsektor klar hervorgehoben. Für den Erfolg von MELANI als Partnerschaft sind solche Ergebnisse sehr wichtig. Wenn MELANI in entscheidenden Situationen ihre Mitglieder wesentliche Hilfe anbieten kann, sind die Mitglieder umgekehrt auch bereit, zum Erfolg von MELANI beizutragen (indem sie beispielsweise Informationen mit anderen Mitgliedern teilen). Das starke Wachstum des GK im Bereich des Finanzssektors nach der erfolgreichen Unterstützung einiger Finanzinstitute während der Phishing-Attacken von 2005/2006 zeigt, dass solche Erfolge auch eine starke Signalwirkung haben können und wesentlich zur Etablierung von MELANI in der Privatwirtschaft beigetragen haben.

Von den 38 Mitgliedern, die Hilfe in Anspruch genommen haben, bewerten 34 die Hilfe als schnell und effizient.[13] Besonders bei der Vorfallbekämpfung ist die Qualität der Dienstleistung absolut zentral. Sobald die Hilfe von MELANI nicht mehr rasch und effizient erfolgt, ist sie für die Mitglieder des GK nicht mehr von Nutzen. Darum muss verhindert werden, dass es beim CERT zu Überlastungen kommt. Da Vorfälle häufig mehrere Kunden gleichzeitig betreffen und der GK stark gewachsen ist, sind die Herausforderungen im Bereich der Vorfallbekämpfung gross.

2.3.3 Workshops

Als weitere Dienstleistung bietet MELANI den Kunden des GK auch die Organisation von Trainings und Workshops an, in welchen spezifische Themen im Bereich der Informationssicherung diskutiert und „best practices“ vorgestellt werden. Obwohl das Angebot an solchen Veranstaltungen im Bereich der Informationssicherheit bereits relativ gross ist, sind diese doch meist eher allgemein gehalten und richten sich an ein breites Publikum. Das kommerzielle Interesse der privaten Veranstalter solcher Workshops beeinträchtigt zudem manchmal deren Unabhängigkeit und Vertrauenswürdigkeit. Die Workshops von MELANI hingegen, sind auf die Mitglieder des GK beschränkt und da MELANI keine kommerziellen Interessen verfolgt ist die Vertrauenswürdigkeit der vermittelten Informationen hoch. Dies wurde auch in den Gesprächen mit den Vertretern aus dem Finanz-, Energie- und Telekommunikationssektor bestätigt.

Insgesamt veranstaltet MELANI aber relativ wenige Workshops. Nur 48 der 108 Befragten gaben an, in den letzten drei Jahren einen Workshop von MELANI besucht zu haben. Diese eher tiefe Anzahl dürfte

---

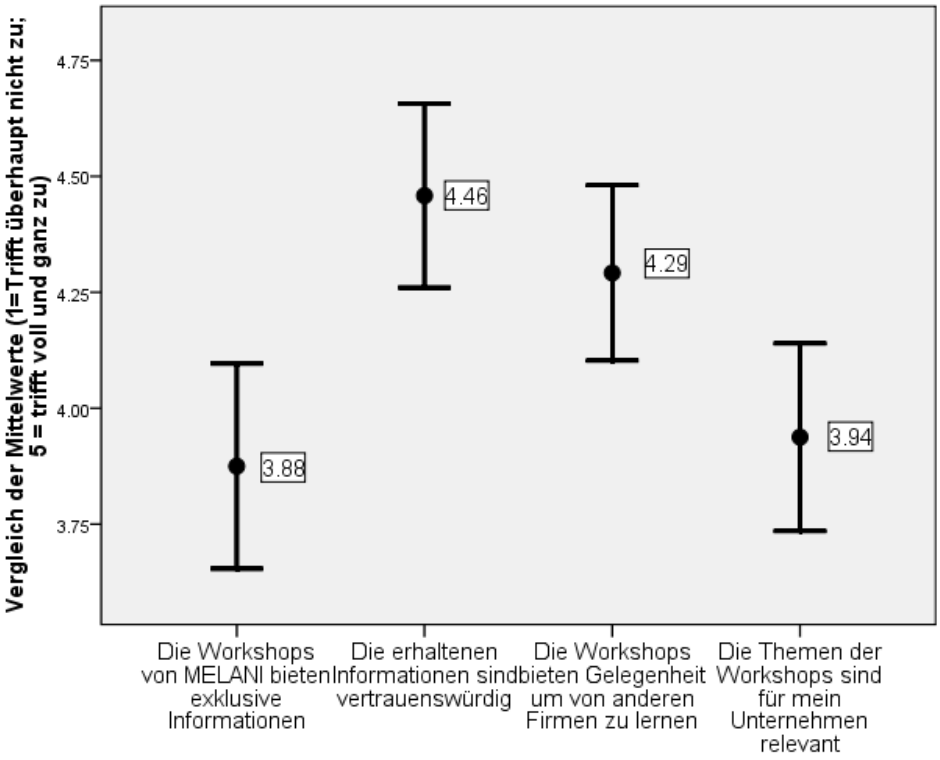
[12] Die Teilnehmer wurden gebeten, die Aussage „die Hilfe von MELANI war bei der Vorfallbekämpfung entscheidend“ zu beurteilen. 8 stimmten voll und ganz zu und weitere 18 stimmten eher zu. Für nur 2 der Befragten war die Hilfe eher nicht entscheidend („trifft eher nicht zu“) und 10 Befragte wählten die Antwortoption „weder noch“.

[13] Die Befragten konnten die Aussage „der Vorfall wurde schnell und effizient bekämpft“ auf einer Skala von 1= trifft überhaupt nicht zu bis 5=trifft voll und ganz zu bewerten. Ein Mitglied des GK beurteilte die Hilfe eher kritisch („trifft eher nicht zu“), 3 wählten die Option „weder noch“, 18 antworteten mit „trifft eher zu“ und 8 mit „trifft voll und ganz zu“.

weniger auf ein mangelndes Interesse der Mitglieder des GK zurückzuführen sein,[14] als auf den Umstand, dass MELANI zu wenig Mittel zur Verfügung hat, um solche Veranstaltungen durchzuführen. Deshalb ist es umso wichtiger zu wissen, was von den Teilnehmern von Workshops besonders geschätzt wird und welche Wünsche es zu berücksichtigen gilt. Aus diesem Grund werden die Antworten jener Mitglieder des GK analysiert, die in den letzten drei Jahren mindestens an einem Workshop teilgenommen haben.

Die generelle Qualität der Workshops wird von den Teilnehmer als gut beurteilt (der Mittelwert liegt bei 3.96, auf einer Skala von 1=ungenügend bis 5=sehr gut). Die Darstellung 6 zeigt zudem auf, welche Qualitäten besonders geschätzt werden:

Darstellung 6



N=48; die Resultate sind für ein Konfidenzintervall von 95% dargestellt.

Die Vertrauenswürdigkeit der vermittelten Informationen wird besonders geschätzt, was auch in den Gesprächen mit den Vertretern aus dem Finanz-, Energie- und Telekommunikationssektor betont wurde. Denn obwohl das Angebot an Veranstaltungen im Bereich der Informationssicherheit gross ist, beeinträchtigt das kommerzielle Interesse der privaten Veranstalter tendenziell auch deren Unabhängigkeit und Vertrauenswürdigkeit. Die Workshops von MELANI hingegen sind auf die Mitglieder des GK beschränkt, und es besteht keinerlei kommerzielles Interesse.

Wichtig ist den Teilnehmern auch, dass gute Kontakte zu anderen Firmen geknüpft werden können. Dank der beschränkten Anzahl der Mitglieder im GK bieten sich an den Workshops von MELANI gute Gelegenheiten für den gegenseitigen Austausch zwischen Verantwortlichen in ähnlichen Positionen. Solche Möglichkeiten werden von den Teilnehmern an Workshops offensichtlich sehr geschätzt. Im folgenden Abschnitt wird auf die Bedeutung des gegenseitigen Informationsaustausches eingegangen und dabei auch nochmals untersucht, inwiefern Workshops zu einem solchen beitragen.

[14] Nur 19% der Befragten würden es nicht begrüssen, wenn MELANI mehr Workshops veranstalten würde, während 59% diese Frage bejaht. Der relativ hohe Anteil der Antworten „weiss nicht“ zu dieser Frage (22%) deutet jedoch darauf hin, dass die Teilnahmebereitschaft stark von der Qualität der Workshops abhängt.

Etwas weniger positiv wird die Exklusivität und die Relevanz der erhaltenen Informationen beurteilt. Hinsichtlich der Kriterien der Exklusivität, der Vertrauenswürdigkeit und der Relevanz für die Unternehmen zeigt sich somit ein sehr ähnliches Bild wie bei der Einschätzung der Qualität der *Security Advisories*. Während die Vertrauenswürdigkeit der Dienstleistungen von MELANI sehr hoch eingeschätzt wird, liegen die Bewertungen für die Exklusivität der Informationen und die Relevanz etwas tiefer. Daraus lässt sich ableiten, dass MELANI wo immer möglich versuchen sollte, die Dienstleistungen noch etwas besser auf die entsprechenden Zielgruppen zu fokussieren und sich auf diejenigen Services zu konzentrieren, die die Unternehmen nirgendwo sonst beziehen können. In den Gesprächen wurde seitens des Energiesektors diesbezüglich die Anregung geäussert, MELANI könnte zur Vermittlung von spezifischem Fachwissen an themenorientierten Workshops vermehrt auch externe Spezialisten engagieren.

2.4 MELANI als Plattform für Informationsaustausch

Der Austausch von Informationen über Bedrohungen, neue Gefahren und mögliche Schutzmassnahmen zwischen allen beteiligten Akteuren ist ein zentraler Bestandteil der Informationssicherung. Nur durch einen solchen Erfahrungs- und Wissensaustausch können neue Risiken rechtzeitig erkannt und Sicherheitslücken rechtzeitig geschlossen werden. Neben der Früherkennung ist der gegenseitige Informationsaustausch aber auch wichtig für die Prävention. Weil viele Unternehmen mit ähnlichen Problemen konfrontiert sind, können sie viel voneinander lernen und einander helfen, ihre Systeme sicherer zu machen und die Abläufe zu optimieren.

Es ist darum erklärtes Ziel von MELANI, diese Art der Selbsthilfe zwischen den Firmen zu fördern. Zudem ist es für MELANI als Behörde wichtig, sich selber an diesem Informationsaustausch zu beteiligen: Um die Lage in der Informationssicherung korrekt einschätzen zu können, ist MELANI einerseits auf Informationen aus der Privatwirtschaft angewiesen, andererseits möchten die Unternehmen eine staatliche Anlaufstelle beim Staat haben, der sie Vorfälle melden und von der wenn nötig Unterstützung angefordert werden kann. In diesem Abschnitt wird deshalb analysiert, wie MELANI als Plattform für den Informationsaustausch funktioniert. Es wird untersucht, wie viele Mitglieder des GK dem Personal von MELANI oder anderen Mitgliedern vertrauliche Informationen weitergegeben haben, welche Voraussetzungen dazu gegeben sein müssen und welche Rolle das MELANI-Net beim Austausch von vertraulichen Informationen spielt.

2.4.1 Der Informationsaustausch im GK

Angesichts der Wichtigkeit von Informations- und Erfahrungsaustausch für die Informationssicherung ist es bemerkenswert, dass nur die Hälfte (54 von 108) der befragten Mitglieder des GK angibt, in den letzten drei Jahren vertrauliche Informationen mit dem Personal von MELANI oder mit anderen Mitgliedern des GK ausgetauscht zu haben. Dieses Resultat muss aber etwas relativiert werden: Nur ein Teil der Befragten ist am direkten Informationsaustausch beteiligt. Pro Firma sind teilweise mehrere Personen im GK vertreten; Informationen werden aber meist nur von einer Person weitergegeben. Zweitens wurde in der Befragung nicht weiter spezifiziert, was unter vertraulicher Information verstanden werden soll. Es ist also durchaus möglich, dass Firmen wichtige Informationen weitergegeben haben, diese aber nicht als vertraulich einstuften.

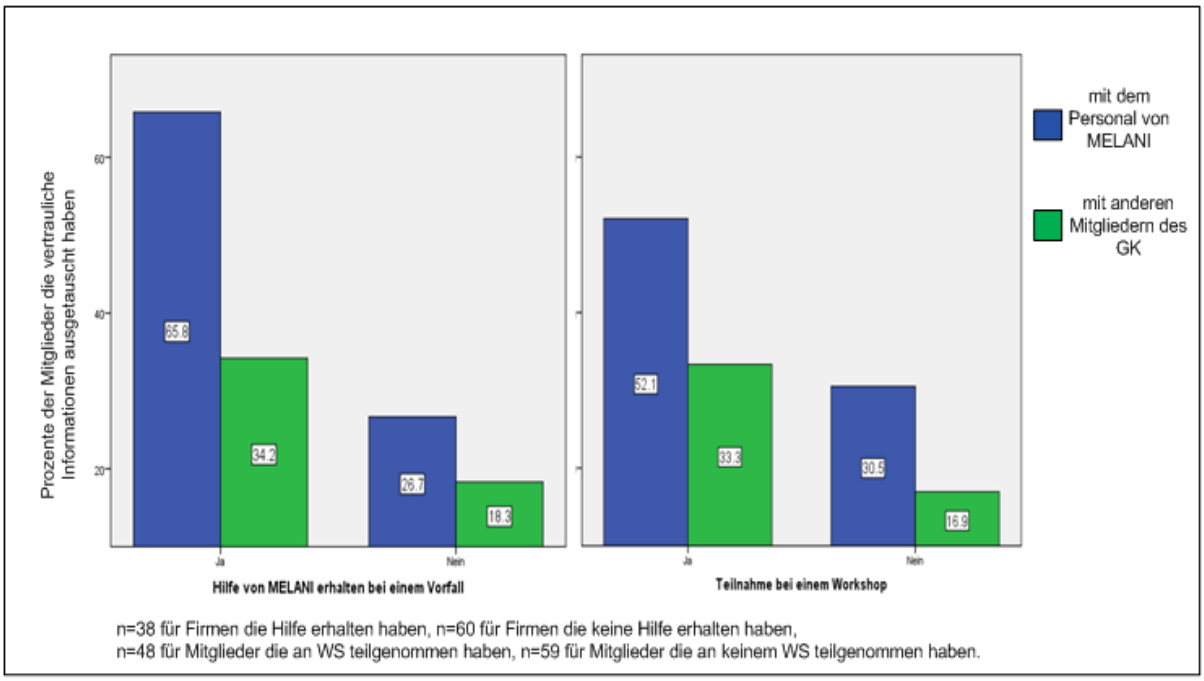
Doch obschon die Ergebnisse vorsichtig zu interpretieren sind, sind einige interessante Resultate feststellbar. Zunächst ist es aufschlussreich, dass der Informationsaustausch vor allem zwischen den Mitgliedern des GK und MELANI stattfindet (und nicht zwischen den Firmen). 43 Mitglieder des GK gaben an, dass sie in den letzten drei Jahren mit dem Personal von MELANI vertrauliche Informationen ausge-

tauscht haben. 26 Mitglieder haben sich mit Unternehmen aus dem gleichen Sektor ausgetauscht und nur zwei Mitglieder haben mit Unternehmen aus einem anderen Sektor Informationen ausgetauscht.[15]

Dieses Ergebnis ist weitgehend mit der Struktur des GK zu erklären. Im Normalfall werden Informationen zuerst dem Personal von MELANI übermittelt, woraufhin bestimmt wird, ob die Information über das MELANI-Net anderen Mitgliedern des GK zugänglich gemacht werden soll. Dieser „Zentralismus" führt dazu, dass wenig Informationsaustausch zwischen den Mitgliedern selber stattfindet. Zudem sind viele Sektoren schlicht zu klein, als dass ein aktiver Austausch zwischen den Mitgliedern desselben Sektors stattfinden könnte. Bezeichnenderweise stammen von den 26 Mitgliedern, die sich mit Firmen aus dem gleichen Sektor ausgetauscht haben, 21 aus dem Finanzsektor.

Als nächstes wurde untersucht, ob der Austausch von vertraulichen Informationen mit a) Hilfe bei Vorfällen und b) den von MELANI organisierten Workshops zusammenhängt (Darstellung 7). Informationsaustausch bei Vorfällen ist für das Funktionieren von MELANI zentral, denn nur durch die Kommunikation von Vorfällen kann MELANI sich ein Bild über die allgemeine Verwundbarkeit machen. Zudem kann ohne einen gewissen Informationsaustausch über einen Vorfall auch nicht die richtige Hilfe geboten werden.

Darstellung 7



Tatsächlich gehen Unterstützung bei Vorfällen und Workshops mit einem deutlich höheren Anteil an Informationsaustausch einher. Knapp zwei Drittel der Mitglieder, die Hilfe bei einem Vorfall erhalten haben, haben mit dem Personal von MELANI vertrauliche Informationen ausgetauscht, während es bei jenen Mitgliedern, die keine Hilfe erhalten haben, nur etwas mehr als ein Viertel war. Interessanterweise haben die Mitglieder, die Hilfe erhalten haben, auch häufiger Informationen mit anderen Mitgliedern ausgetauscht (34% zu 18%). Dieses Resultat verdeutlicht nochmals die Bedeutung der Hilfe bei Vorfällen. Durch diese Dienstleistung wird der Austausch der Informationen deutlich erhöht und es gelingt MELANI, Wissen über aktuelle Bedrohungen und Risiken zu gewinnen. Zudem scheint die Hilfe bei Vorfällen auch zu bewirken, dass mehr Informationen mit anderen Mitgliedern des GK ausgetauscht werden, wodurch wiederum der GK als Ganzes profitiert.

[15] N=108.

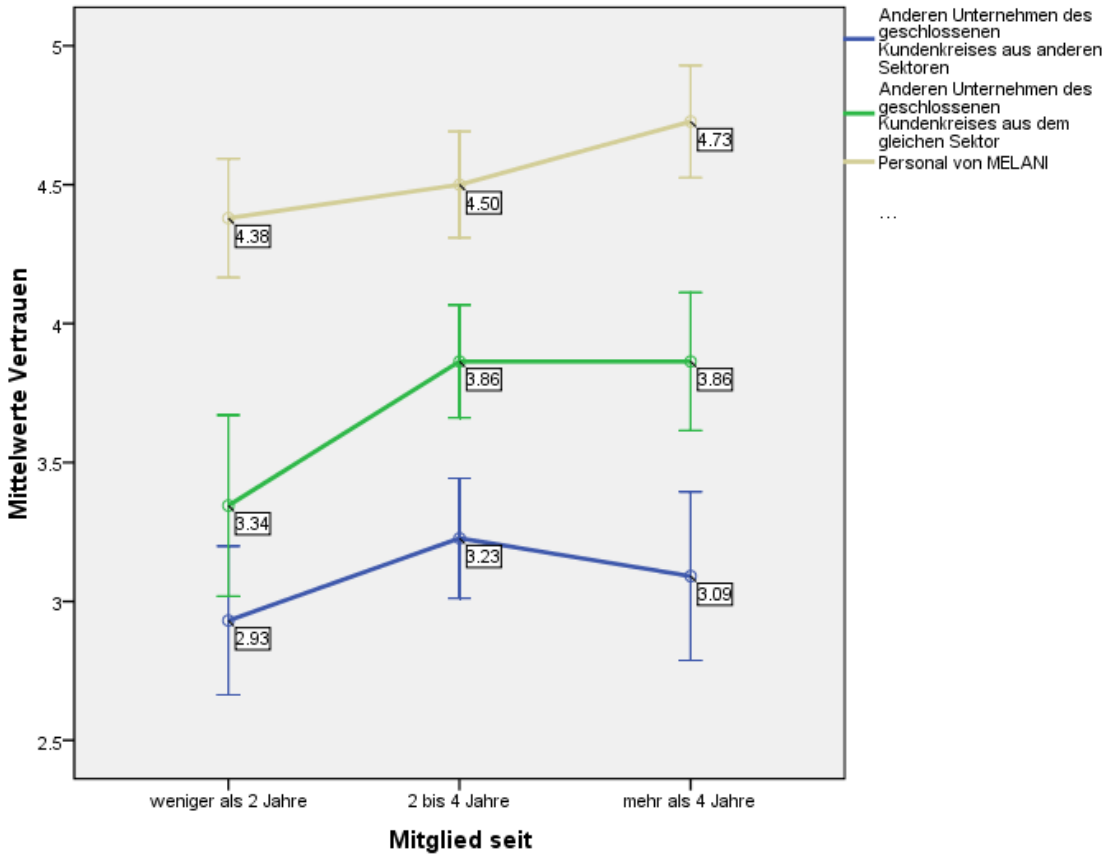
Auch unter den Teilnehmern an Workshops hat mehr als die Hälfte mit dem Personal von MELANI vertrauliche Informationen ausgetauscht und ein Drittel hat dies mit anderen Mitgliedern getan. Im Vergleich dazu liegen die Anteile für Mitglieder, die nicht an Workshops teilgenommen haben, bei 31% für den Austausch mit dem Personal von MELANI und bei 17% für den Austausch mit anderen Mitgliedern. Die Veranstaltung von Workshops erhöht also den Anteil des Informationsaustausches deutlich und erfüllt damit einen wichtigen Zweck. Dies entspricht der oben gezeigten Wichtigkeit der Workshops für das gegenseitige Lernen.

2.4.2 Das Vertrauen der Mitglieder des GK zu MELANI und zu anderen Mitgliedern

Als Grundvoraussetzung für den Austausch von Informationen im Bereich der Informationssicherheit wird oft ein starkes gegenseitiges Vertrauen genannt. Aus diesem Grund wurden die Teilnehmer zur Stärke ihres Vertrauens a) zum Personal von MELANI, b) zu anderen Unternehmen aus dem gleichen Sektor und c) zu anderen Unternehmen aus anderen Sektoren befragt. Es wird zunächst untersucht, wie die Mitglieder des GK diese Fragen beantwortet haben, wobei insbesondere überprüft wird, ob das Ausmass des Vertrauens mit der Zeit zunimmt, d.h. ob ältere Mitglieder stärkeres Vertrauen in MELANI und in andere Unternehmen haben als jüngere. Danach wird diskutiert, welche Rolle das gegenseitige Vertrauen für den Informationsaustausch spielt.

Die Skala der vorgegebenen Antworten zu den Fragen nach dem gegenseitigen Vertrauen reichte dabei von 1= sehr schwach bis 5= sehr stark für alle drei verschiedenen Arten des Vertrauens. Die Darstellung 8 zeigt die Resultate für alle drei Fragen, aufgeteilt nach der Anzahl Jahre der Mitgliedschaft im GK.

Darstellung 8



Die Fehlerbalken sind für ein Konfidenzintervall von 95% angegeben

Die Graphik verdeutlicht, dass das Vertrauen in das Personal von MELANI bereits anfangs sehr gross ist, es über die Jahre aber sogar noch weiter zunimmt.[16] Von den 108 Befragten geben 102 an, MELANI stark oder sehr stark zu vertrauen, nur sechs stufen ihr Vertrauen in MELANI als „mittel" ein, kein einziges Mitglied als „schwach" oder „sehr schwach". Es ist zu vermuten, dass ein hohes Grundvertrauen in MELANI eine Voraussetzung dafür ist, dass Firmen überhaupt in den GK eintreten. Die Tatsache, dass dieses Vertrauen über die Jahre gefestigt wird und weiter wächst, zeigt, dass MELANI tatsächlich ein vertrauenswürdiger Partner für die Firmen ist. Auch in den Gesprächen mit den verschiedenen Sektorvertretern wurde dies bestätigt. Angesichts der grossen Bedeutung des Vertrauens für eine funktionierende Partnerschaft ist dies ein wichtiger Erfolg von MELANI.

Das Vertrauen in andere Unternehmen aus dem gleichen Sektor ist deutlich weniger hoch bei jüngeren Mitgliedern, wächst dann aber relativ stark an.[17] Durch die Mitgliedschaft im GK scheint auch das Vertrauen in andere Unternehmen des gleichen Sektors gesteigert zu werden. Auch ersichtlich ist jedoch, dass es zwischen den Mitgliedern, die 2-4 Jahre im GK sind, und jenen, die schon mehr als vier Jahre dabei sind, keine Unterschiede mehr gibt. Das Vertrauen in andere Unternehmen aus dem gleichen Sektor wird also am Anfang stark gefördert, stagniert dann aber mit der Zeit. MELANI trägt zwar dazu bei, dass eine anfängliche Skepsis überwunden werden kann, es stellt sich aber die Frage, ob und wie das gegenseitige Vertrauen zwischen den Unternehmen aus dem gleichen Sektore mit gezielten Massnahmen noch stärker gefördert werden könnte. Teilnahme an gemeinsamen Workshops zum Beispiel scheint das Vertrauen zu stärken: Mitglieder, die an Workshops teilgenommen haben, vertrauen anderen Unternehmen aus dem gleichen Sektor stärker, als solche, die noch nie an einem Workshop teilgenommen haben.[18]

Das Vertrauen in andere Unternehmen aus anderen Sektoren ist von Anfang an vergleichsweise tief und ist auch bei langjährigen Mitgliedern des GK nur unwesentlich höher. Dies ist erklärbar mit der Tatsache, dass innerhalb des GK nur sehr wenige sektorübergreifende Aktivitäten stattfinden. Mitglieder aus verschiedenen Sektoren treten nur selten in Kontakt miteinander und so verstärkt sich auch das gegenseitige Vertrauen kaum.

Gegenseitiges Vertrauen hat auch eine hohe Bedeutung für den Informationsaustausch. Ein Mindestmass an gegenseitigem Vertrauen scheint auch eine Voraussetzung für den Austausch von Informationen zwischen Unternehmen aus dem gleichen Sektor zu sein. Von den 26 Befragten, die vertrauliche Informationen mit anderen Unternehmen aus dem gleichen Sektor ausgetauscht haben, haben 17 ein starkes oder sehr starkes und 9 ein mittleres Vertrauen in die anderen Mitglieder aus dem gleichen Sektor. Aufgrund der relativ tiefen Anzahl Mitglieder, die mit anderen Mitgliedern aus dem gleichen Sektor Informationen austauschen, kann nicht abschliessend beurteilt werden, ob stärkeres Vertrauen wirklich zu mehr Informationsaustausch führt. Schlussendlich ist aber vor allem die Einsicht zentral, dass für jeden Informationsaustausch eine Vertrauensbasis vorhanden sein muss und dass diese zwischen den Mitgliedern des GK und dem Personal von MELANI sicher in grösserem Ausmass vorhanden ist als zwischen den verschiedenen Mitgliedern des GK.

---

16 Der Korrelationskoeffizient für die Beziehung zwischen dem Vertrauen in das Personal von MELANI und der Anzahl Jahre der Mitgliedschaft beträgt 0.26 auf dem Signifikanzniveau von <0.05.

17 Der Korrelationskoeffizient für die Beziehung zwischen dem Vertrauen in andere Unternehmen aus dem gleichen Sektor und der Anzahl der Jahre der Mitgliedschaft beträgt 0.27 auf dem Signifikanzniveau von >0.01.

18 Die Mittelwerte betragen 3.88 für Mitglieder die an Workshops teilgenommen haben und 3.51 für solche, die noch nie an einem Workshop teilgenommen haben (die Irrtumswahrscheinlichkeit für die Differenz dieser Mittelwerte beträgt 0.9%).

2.4.3 MELANI-Net als Instrument für den Informationsaustausch

Mit dem MELANI-Net bietet MELANI den Mitgliedern des GK eine geschützte online-Plattform, auf der vertrauliche Informationen ausgetauscht werden können. Im Abschnitt über die Qualität der *Security Advisories* wurde bereits erläutert, wie die Mitglieder die Informationen bewerten, die sie über diese Plattform erhalten. In der Befragung wurde aber auch deutlich, dass sich viele Mitglieder des GK wünschen, dass das MELANI-Net vermehrt für den Informationsaustausch zwischen Mitgliedern benutzt werden könnte. Wie bereits erwähnt, besteht aktuell ein gewisser Zentralismus beim Informationsaustausch innerhalb des GK: Die Mitglieder teilen die Informationen zunächst dem Personal von MELANI mit, und dieses wiederum macht die Informationen über MELANI-Net anderen Mitgliedern zugänglich (natürlich nur, wenn das Mitglied, von welchem die Informationen stammen, mit diesem Vorgehen einverstanden ist). Dieser Ablauf verhindert das Verbreiten redundanter, irrelevanter oder gar sachlich umstrittener Informationen über MELANI-Net. Dafür ist diese Art des Informationsaustausches relativ umständlich, und interaktive Diskussionen sind nicht möglich.

Genau solche Diskussionen scheinen aber bei relativ vielen Mitgliedern des GK ein Bedürfnis zu sein. Sowohl in der Befragung als auch in den Gesprächen wurde mehrfach der Wunsch nach einem Diskussionsforum auf MELANI-Net geäussert. Ein solches Forum würde den Mitgliedern Gelegenheit geben, sich direkt untereinander auszutauschen und würde damit das gegenseitige Lernen fördern. In eine ähnliche Richtung zielt der ebenfalls mehrfach geäusserte Wunsch nach Mailing-Listen für die Mitglieder des GK. Durch eine solche Liste könnten ausgewählte Mitglieder einfacher von anderen Mitgliedern kontaktiert werden.

Sowohl ein Diskussionsforum als auch Mailing-Listen müssten aber vom Personal von MELANI betreut werden, um die Qualität der Diskussionen sicherzustellen. Zudem hängt der Erfolg eines solchen Forums stark vom Engagement der einzelnen Mitglieder ab. Um den Meinungsaustausch zu fördern, wird es kaum genügen, den Mitgliedern ein Forum oder Mailing-Listen zur Verfügung zu stellen, da sich viele erst dann an Diskussionen beteiligen, wenn sie den anderen Teilnehmern stark vertrauen und auch davon ausgehen, dass sie von ihnen etwas lernen können. Zusätzliche (technische) Instrumente für den Informationsaustausch sind deshalb nur dann sinnvoll, wenn ein vermehrter Informationsaustausch zwischen Mitgliedern aktiv gefördert wird. Dies würde bedeuten, dass häufiger Anlässe wie Workshops durchgeführt werden müssen, an welchen sich die verschiedenen Mitglieder auch persönlich kennenlernen.

2.5 Weiterentwicklung des GK aus Sicht der Mitglieder

Wie oben erwähnt, ist der GK von MELANI in den letzten drei Jahren stark gewachsen. In einigen Sektoren kamen sehr viele neue Mitglieder hinzu und mit Chemie / Pharma, Versicherungen und Industrie sind auch drei neue Sektoren vertreten. Es stellt sich deshalb die Frage, ob MELANI nun die Grenzen erreicht hat, oder ob es noch weiter wachsen soll.

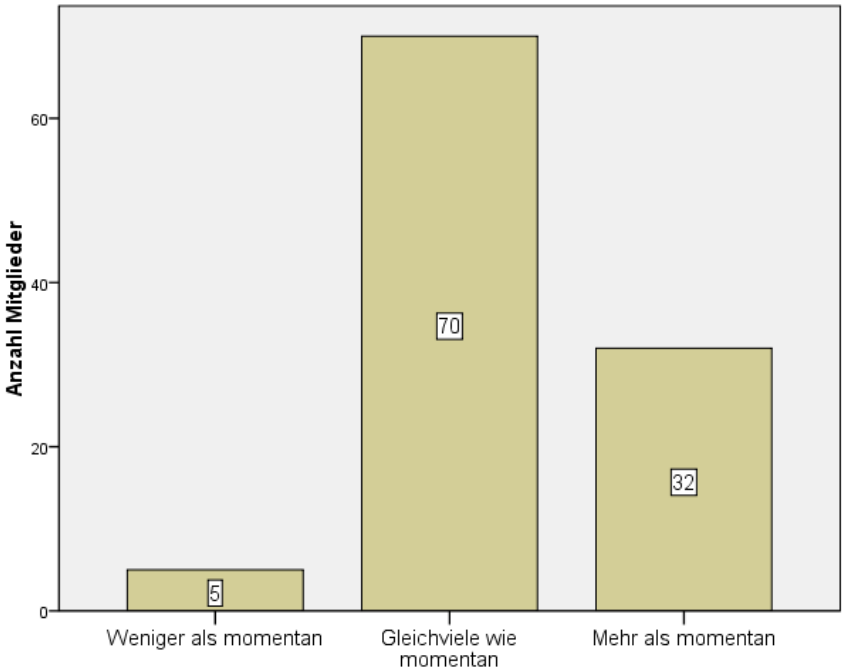
In der Umfrage konnten die Mitglieder des GK beurteilen, wie viele Unternehmen ihrer Meinung nach in Zukunft im GK vertreten sein sollten, unabhängig von den bestehenden bzw. zukünftigen Ressourcen von MELANI. Es handelt sich dabei also um einen Wunsch und nicht um eine Einschätzung des Machbaren.

Die Mehrheit der Mitglieder des GK hält die momentane Anzahl Mitglieder für genau richtig, aber immerhin mehr als ein Drittel der Befragten wünscht sich noch mehr Mitglieder (siehe Darstellung 9). Wenig überraschend ist, dass die Mitglieder jener Sektoren, in welchen bereits relativ viele Firmen vertreten sind, weniger häufig ein weiteres Wachstum des GK wünschen. Nur 14 von 59 Mitgliedern aus dem Finanzsektor wollen ein weiteres Wachstum des GK, und von den neun Vertretern aus dem Sektor Tele-

kommunikation (in welchem auch bereits die meisten wichtigen Unternehmen vertreten sind) wünscht sich kein einziger eine Vergrösserung des GK.

Umgekehrt erhoffen sich Sektoren mit relativ wenigen Mitgliedernein weiteres Wachstum speziell in ihrem Sektor. Die Antworten auf die Frage, wie viele Unternehmen aus dem eigenen Sektor in Zukunft im GK vertreten sein sollen, zeigen dies deutlich. So denken beispielsweise vier von fünf Mitgliedern aus dem Industriesektor, dass in ihrem Sektor mehr Unternehmen vertreten sein sollten. Auch die Vertreter des Energiesektors wünschen sich Mehrheitlich ein weiteres Wachstum ihres Sektors (sieben von elf sind der Meinung, es brauche in ihrem Sektor mehr Mitglieder).

Darstellung 9



Schliesslich wurden die Mitglieder des GK auch gefragt, ob noch weitere Sektoren in den GK integriert werden sollten. Während hier keine konkreten Sektoren genannt wurden, erwähnten zwei Teilnehmer die Problematik, dass kleine und mittlere Unternehmen (KMUs) keinen Zugang zum GK haben, gleichzeitig aber relativ häufig mit Problemen der Informationssicherung konfrontiert sind. Auch in den Gesprächen mit Vertretern aus dem GK wurde deutlich, dass vom Bund eine stärkere Rolle im Bereich der Informationssicherung für KMUs und Privatanwender gewünscht würde. Aus Sicht einiger Vertreter des GK besteht ein Bedarf an verstärkter Öffentlichkeitsarbeit und an besserer Unterstützung für KMUs. Ob und wie sich der Bund hier engagieren soll und kann und inwiefern MELANI dabei involviert sein soll, sind aber Fragen, die bei der Weiterentwicklung von MELANI unbedingt beachtet werden müssen.

3 Internationaler Vergleich

In diesem Kapitel sollen Informationssicherungsmodelle in den umliegenden und für die Schweiz relevanten Ländern dargestellt werden. Daraus können drei idealtypische Modelle abgeleitet und deren Stärken und Schwächen diskutiert werden. Dies wird im nächsten Kapitel helfen, die Stärken und Schwächen von MELANI zu kontextualisieren.

3.1 Ausgewählte Modelle zur Informationssicherung

Die Lösungsansätze in den untersuchten Ländern (Österreich, Deutschland, Grossbritannien, Italien, die Niederlande und Schweden) sind nicht nur in ihrer Logik sehr unterschiedlich, sie befinden sich auch in verschiedenen Phasen der Umsetzung bzw. Konsolidierung. Ein direkter Vergleich zwischen den einzelnen Modellen ist deshalb nicht möglich. Die kurzen Darstellungen von Aufbau und Zielen hilft aber, die wichtigsten Bausteine zu identifizieren, aus denen die Modelle im Kapitel 3.2 gebaut werden.

3.1.1 Österreich

Die Strukturen zur Informationssicherung sind in Österreich dreistufig gegliedert:

1) Als übergeordnetes Koordinations- und Strategiegremium der Bundesregierung für E-Government dient die Plattform Digitales Österreich[19]. Oberste Priorität auf dieser Stufe hat die Einbindung aller Bürgerinnen und Bürger, der Datenschutz und die Kundenorientierung.
2) Die zweite Stufe der Informationssicherung wird gewährleistet durch das nationale Computer Emergency Response Team, CERT.at[20]. Dieses fungiert als Ansprechpartner für IT-Sicherheit im nationalen Umfeld: Es vernetzt andere CERTs und CSIRTs (Computer Security Incident Response Teams) aus den Bereichen kritische Infrastruktur, Informations- und Kommunikationstechnik und gibt Warnungen, Alerts und Tipps für kleine und mittlere Unternehmen (KMU) heraus.
3) Seit April 2008 agiert das sogenannte GovCERT[21] auf der dritten Stufe. Es wird vom Bundeskanzleramt in Kooperation mit CERT.at betrieben, zur Verhinderung von Sicherheitsvorfällen im Bereich Information und Kommunikationstechnologien für die öffentliche Verwaltung und die kritische Informations-Infrastruktur in Österreich.

Auf nationaler Ebene ist es die Aufgabe von GovCERT, eine Koordinationsfunktion zwischen den einzelnen Stellen der öffentlichen Verwaltung und den Betreibern der kritischen Infrastruktur einzunehmen. Dabei geht es vor allem darum, Informationen über Vorfälle aus dem operativen Informations- und Kommunikationstechnologie (IKT)-Betrieb der Bundes-, Landes-, Städte- und Gemeindeverwaltungen zu sammeln und zu bewerten, die Gegenmassnahmen zu koordinieren und Nachrichten aus öffentlich und nicht-öffentlich zugänglichen Quellen zu beschaffen und zu bewerten.

GovCERT hat einen zweigliedrigen Teilnehmerkreis. Zum einen schliesst dieser den Behördenbereich (Bundesministerien, Landesverwaltungen oder Städte- und Gemeindeverwaltungen) mit ein, zum andern sind die Betreiber von kritischen Infrastrukturen teilnahmeberechtigt. Die Liste der kritischen Sektoren wird derzeit im Bundeskanzleramt erarbeitet. In Zukunft müssen die individuellen Mitglieder des Teil-

[19] http://www.digitales.oesterreich.gv.at/

[20] http://www.cert.at/

[21] http://www.digitales.oesterreich.gv.at/site/6828/default.aspx

nehmerkreises durch die jeweilige Behörde beziehungsweise den Infrastruktur-Betreibern offiziell nominiert und abgesegnet werden.

Die Teilnahme in diesem GovCERT-Modell ist an klare Auflagen geknüpft: Die Teilnehmer sind angehalten, Informationen zu IT-sicherheitsrelevanten Kenndaten und Vorfällen aktiv bereitzustellen, bei der sicherheitsrelevanten Themenaufarbeitung mitzuwirken, Knowhow auszutauschen und das Krisenmanagement bei IT-sicherheitsrelevanten Vorfällen sicherzustellen. In Gegenzug werden den Teilnehmenden folgende Dienstleistungen zur Verfügung gestellt:

- statistische Zusammenfassungen von Vorfällen innerhalb des Benutzerkreises,
- die Unterstützung durch den GovCERT-Expertenpool bei Vorfällen,
- den Zugriff auf einschlägige (auch klassifizierte) Dokumente,
- die Teilnahme am so genannten GovCERT-Wiki, in dem Dokumente zu bestimmten Themen gemeinsam erarbeitet und weiterentwickelt werden und
- die Partizipation an Workshops, Schulungen und Security-„Stammtischen".

3.1.2 Deutschland

In Deutschland ist das Bundesamt für Sicherheit in der Informationstechnik (BSI)[22] das Hauptorgan für den Schutz kritischer Informationsinfrastrukturen. Es gehört dem Bundesministerium des Innern (BMI)[23] an und versteht sich als der zentrale IT-Sicherheitsdienstleister des Bundes. Mit seinem sehr breiten Angebot wendet es sich an Privatanwender und an die Nutzer und Hersteller von Informationstechnik in der öffentlichen Verwaltung und in der Privatwirtschaft.

Das BSI ist stark zentralisiert und mit einem breiten Aufgabenspektrum zum Schutz kritischer Informationsinfrastrukturen betraut. Es übernimmt Aufgaben in den vier Kernbereichen Information, Beratung, Entwicklung und Zertifizierung. Es informiert über Risiken und Gefahren beim Einsatz der Informationstechnik und ist gleichzeitig, um Lösungen bemüht, z.B. durch die Prüfung und Bewertung der Sicherheit von IT-Systemen, einschliesslich deren Entwicklung in Kooperation mit der Industrie. Im BSI werden auch Störungen oder Ausfälle in kritischen Infrastrukturen untersucht, die im Zusammenhang mit (absichtlich herbeigeführten) Fehlfunktionen der Informationstechnik stehen. Mit den beiden Internet-Services „BSI für Bürger" und dem „Bürger-CERT" werden darüber hinaus in leicht verständlicher Sprache Hintergrundinformationen für ein breites Publikum zu Informationssicherheit angeboten.

Ebenfalls in den Aufgabenbereich des BSI[24] fällt der CERT-Bund. CERT-Bund hat zum einen die Aufgabe, präventiv Sicherheitslücken in den Computersystemen des Bundes zu finden und zu schliessen und andererseits rund um die Uhr auf mögliche Gefährdungen oder Angriffe zu reagieren und kurzfristige Gegenmassnahmen zu ergreifen. CERT-Bund ist Teil des CERT-Verbunds, der Allianz deutscher Sicherheits- und Computer-Notfallteams aus dem Privatsektor, dessen Ziel es ist, den Schutz der nationalen Netze der Informationstechnik sicherzustellen und dazu bei auftretenden Sicherheitsvorkommnissen gemeinsam und schnell zu reagieren. Die Leitlinien des CERT-Verbundes schliessen u.a. die Freiwilligkeit der Kooperation, die absolute Priorität von Vertraulichkeit und den wechselseitigen und permanenten Informationsaustausch mit ein.[25]

---

22 https://www.bsi.bund.de/cln_134/DE/Home/home_node.html

23 http://www.bmi.bund.de/cln_173/DE/Home/startseite_node.html

24 Übersicht BSI-Themen mit links: https://www.bsi.bund.de/cln_134/DE/Themen/themen_node.html

25 Leitlinien umfassend: http://www.cert-verbund.de/coc.html

3.1.3 Grossbritannien

In Grossbritannien ist der Schutz der kritischen (Informations-)Infrastruktur Aufgabe des Centre for the Protection of the National Infrastructure (CPNI)[26]. Mit dem Auftrag, die nationale Sicherheit zu gewährleisten, wendet sich das CPNI an die Betreiber der nationalen Infrastruktur und bietet Beratung und Hilfe bei der Vernetzung an. Diese Unterstützung ist eine Kombination aus dem Bereitstellen wichtiger Information und aus personeller und physischer Unterstützung.

Das CPNI ist eine interdepartementale Organisation, die versucht, die Ressourcen aus der Industrie, der Wissenschaft und aus verschiedenen Regierungs- und Administrationsbereichen zusammenzuführen. Dieser Ansatz basiert auf der Annahme einer effektiven Dreierbeziehung zwischen Sicherheitsexperten, Regierungsvertretern und den privaten Betreibern von kritischen Infrastrukturen. Die verschiedenen Infrastruktursektoren werden durch verschiedene Regierungsdepartemente betreut. So sind zahlreiche sektorspezifische Informationsaustauschgruppen entstanden, die von CPNI unterhalten werden. Das Ziel dieser Gruppen ist es, den Informationsaustausch über Sicherheitsvorfälle und IT-Schwachstellen zu fördern, zum einen innerhalb von spezifischen Sektoren, zum anderen zwischen den Infrastrukturbetreibern und der Regierung. Dafür ist laut CPNI der Aufbau und die Pflege von Vertrauen zwischen den Mitgliedern der Sektorgruppen zentral. Um dieses herzustellen, gibt es klare Regeln sowohl für die Mitgliedschaft als auch für den Informationsaustausch.

3.1.4 Italien

Das italienische System der Informationssicherung ist zweigliedrig:

1) Zum einen unterhält der italienische Staat eine sogenannte Post- und Fernmeldewesenpolizei (Polizia Postale e delle Comunicazioni). Diese ist betraut mit der Überwachung des Einhaltens von Gesetzen und Regelungen im Bereich der Telekommunikation. Es gehört in ihren Aufgabenbereich, Kinderpornographie im Internet zu bekämpfen, Angriffe auf EDV-Systeme und Verstösse gegen das Urheberrecht zu ahnden und allgemein gegen Computerkriminalität vorzugehen. Ebenfalls zu ihrem Aufgabenbereich gehört der Schutz der nationalen Informationsinfrastruktur gegen Cybercrime-Anschläge. Um dieser Aufgabe nachzukommen, wurde das nationale Anti-Cybercrime Zentrum zum Schutz kritischer Infrastrukturen (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche CNAIPIC) eingerichtet.[27]
2) Zum anderen unterhält das Ministerium für öffentliche Administration und Innovation (Ministerio per la pubblica amministrazione et l'innovazione) ein nationales Zentrum für Information in der öffentlichen Administration (Centro Nazionale per l'informatica nelle pubblica amministrazione, CNIPA). Die Aufgabe dieses Zentrums ist es, die Anwendung von modernen Technologien in der öffentlichen Verwaltung zu fördern, Sicherheitsprobleme zu behandeln und Empfehlungen und technische Regelungen für den IT Bereich des öffentlichen Sektors zu erarbeiten.

Des Weiteren unterhält das CNIPA auch das CERT des öffentlichen Sektors, das CERT-SPC (Computer Emergency Response Team Sistema Pubblico di Connettività), dessen Aufgabe es ist, das Sicherheitsniveau der öffentlichen Informationssysteme zu verbessern und Frühwarnungen für Bedrohungen von und durch ebendiese(n) Systeme(n) bereitzustellen.

---

[26] http://www.cpni.gov.uk/default.aspx

[27] Brunner, E. and Suter, M. (2008), International CIIP Handbook 2008/2009. An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies, Center for Security Studies, ETH Zurich.

3.1.5 Niederlande

Das niederländische Modell zur Informationssicherung ist jenem von Grossbritanien nachempfunden. Mit dem sogenannten ‚Cybercrime Information-Sharing Model' wird auf das vom CPNI entwickelte Modell der Zusammenarbeit zwischen privaten Infrastrukturbetreibern und öffenlichem Sektor zurückgegriffen.

Die Informationsaustausch-Funktion, die vom holländischen National Infrastructure against Cybercrime (NICC) Programm betrieben wird, kann – wie auch das von Grossbritannien – als Blume dargestellt werden.[28] In deren Zentrum befinden sich jene Regierungsagenturen, welche für die verschiedenen Aspekte von Information Assurance und Cybercrime-Bekämpfung verantwortlich sind; so die Polizei, die Geheimdienste, das CERT der Regierung, und das NICC selbst. Darum herum sind die verschiedenen Sektoren in einzelnen Informations-Austausch-Gruppen angeordnet. Der Informationsaustauch innerhalb der Sektoren ist vertraulich, weitgehend strukturiert und reguliert. Von Fall zu Fall kann entschieden werden, ob und welche Information anderen Sektoren oder gar der Öffentlichkeit zur Verfügung gestellt wird.[29]

Das Computer Emergency Response Team im Dienste der Regierungsdepartemente ist das GOVCERT.NL[30]. Es arbeitet unter der Federführung des Innenministeriums und in enger Zusammenarbeit mit dem ‚Waarschuwingsdienst.nl'[31], dem Alert Service, der von Wirtschaftsministerium und dem Generaldirektorium für Energie und Telekommunikation zur Verfügung gestellt wird und malware-Warnungen und Hinweise zu Viren und Trojaner für Kleine und Mittlere Unternehmen herausgibt. Auch die allgemeine Öffentlichkeit kann sich über Email oder SMS über diese Warnungen informieren.

3.1.6 Schweden

Die neueste Situationsanalyse zur Informationssicherheit in Schweden[32] zeichnet das Bild einer weitverzweigten und den verschiedensten Akteuren zugeteilten Verantwortung für die Informationssicherung. Es ist die übergeordnete Aufgabe der im Januar 2009 aus drei Vorgängeragenturen (der Swedish Emergency Management Agency, der Swedish Rescue Services Agency und des National Board of Psychological Defense) neu gebildeten Civil Contingencies Agency, die Arbeiten zur Informationssicherung zu koordinieren und Entwicklungen in diesem Bereich zu analysieren und zu bewerten.

Des weiteren ist seit 2002 die Schwedische Nationale Post und Telekommunkationsagentur damit beauftragt, das Schwedische IT Incident Centre (SITIC)[33] zu betreiben mit dem Ziel, den öffentlichen Sektor beim Schutz vor IT Vorfällen zu unterstützen. Dazu baut das SITIC ein Informationsaustauschsystem zu IT Vorfällen zwischen dem Zentrum und öffentlichen Organisationen auf. Des weiteren soll das SITIC die Öffentlichkeit schnell auf sicherheitsrelevante Probleme im IT Bereich aufmerksam machen, über Gegenmassnahmen informieren, Daten erheben und Dokumentationen bereitstellen, welche die Prävention von Vorfällen erleichtern.

---

28 http://www.samentegencybercrime.nl/UserFiles/File/Leaflet_NICC.pdf

29 http://www.samentegencybercrime.nl/UserFiles/File/NICC%20brochure_uk.pdf

30 http://www.govcert.nl/render.html?it=41

31 http://www.waarschuwingsdienst.nl/render.html?cid=106

32 Swedish Civil Contingencies Agency, Information Security in Sweden. Situational Assessment 2009. Zugriff: http://www2.msb.se/Shopping/pdf//upload/Publikationsservice/MSB/0119_09_Information_security_in_Sweden.pdf

33 http://www.sitic.se/

3.2 Drei idealtypische Modelle

Inspiriert durch die oben dargestellten länderspezifischen Ansätze (v.a. Österreich, Deutschland, Niederlande und Grossbritannien) lassen sich drei idealtypische Modelle ableiten, die im folgenden unter den Namen „IT-Sicherheitsbehörde“, „Blumenmodell“ und „GovCERT+“ vorgestellt werden. Die Abstrahierung der tatsächlich vorhandenen Formen in Idealtypen hilft, wichtige Vor- und Nachteile der verschiedenen Ansätze hervorzuheben.

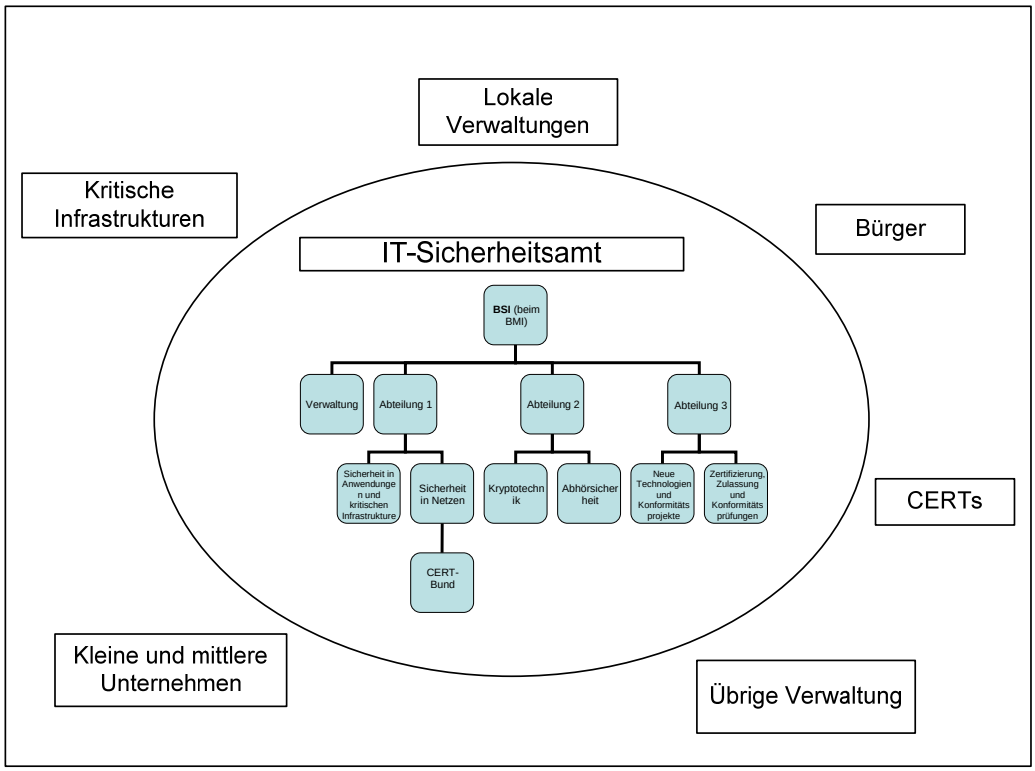
3.2.1 IT-Sicherheitsbehörde

Das Model „IT-Sicherheitsbehörde“ bezeichnet einen ausdifferenzierten und hierarchisch gegliederten Verwaltungsapparat. Von den untersuchten Ländern folgt Deutschland am ehesten einem solchen Modell.

Das wesentliche Merkmal des Modells „IT-Sicherheitsbehörde“ ist die Zentralisierung der Aufgaben. Die IT-Sicherheitsbehörde ist grundsätzlich für alle Aufgaben im Bereich der Informationssicherung verantwortlich. Das bedeutet, dass sich eine solche Behörde nicht auf eine bestimmte Zielgruppe fokussiert, sondern im Bereich der Informationssicherung zugleich für die Anliegen der Bürger, die der Infrastrukturbetreiber und die der verschiedenen Verwaltungseinheiten zuständig ist.

Innerhalb der Behörde werden die verschiedenen Aufgaben entsprechenden Abteilungen und Unterabteilungen zugeordnet. Beispielsweise kann eine Abteilung für den Schutz kritischer Informationsinfrastrukturen zuständig sein, während sich eine andere um die CERT-Aufgaben für die Verwaltung kümmert. Je nach Zuständigkeit sind es die einzelnen Abteilungen, die in ihrem spezifischen Bereich mit den geeigneten Partnern aus der Privatwirtschaft kooperieren; diese Kooperation ist aber nicht integraler Bestandteil der Behörde.

Ein Idealtypus dieses Modells kann folgendermassen dargestellt werden:



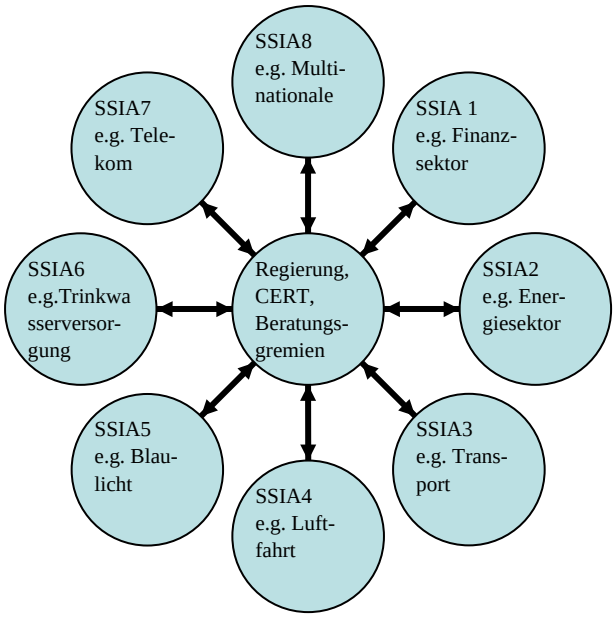
Die starke Zentralisierung aller Aufgaben im Bereich der Informationssicherung bringt einige Vorteile. Die Verantwortung für alle Aufgaben im Bereich der Informationssicherung liegt bei einer Behörde, was eine klare Rechenschaftszuordnung ermöglicht. Dies kann insbesondere die Öffentlichkeitsarbeit erleichtern, weil stets klar ist, wer für Fragen der Informationssicherung zuständig ist. Zudem garantiert die Schaffung einer IT-Sicherheitsbehörde eine gewisse Kontinuität und Stabilität der Strukturen und verhindert Doppelspurigkeit.

Die grosse Schwäche dieses Modells ist der hohe Aufwand, der auf staatlicher Seite betrieben werden muss. Weil Informationssicherung viele verschiedene Aufgaben umfasst, müssen zahlreiche Abteilungen geschaffen werden, was ein grosser Bedarf an Personal bedeutet. Das Modell der IT-Sicherheitsbehörde ist daher sehr ressourcenintensiv. Eine weitere Schwäche besteht darin, dass die Zusammenarbeit mit dem privaten Sektor in diesem Modell nur eine marginale Rolle spielt und wenn überhaupt, dann nur auf untergeordneter Stufe stattfindet. Diese fehlende Institutionalisierung der Zusammenarbeit erschwert den Zugang der einzelnen Abteilungen zu potentiell wertvollen Informationen aus dem Privatsektor. Angesichts einer starken, zentralen Behörde für Informationssicherung besteht auch die Gefahr, dass der Privatsektor die Verantwortung für die Aufgaben in diesem Bereich an den Staat auszulagern versucht.

3.2.2 Blumenmodell

Das „Blumenmodell“ ist der Idealtyp des britischen Modells zur Informationssicherung, das auch jenes der Niederlande inspiriert hat. Im Blumenmodell liegt der Fokus nicht auf der Zentralisierung der Aufgaben, sondern auf der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor. Im Gegensatz zum Modell der IT-Sicherheitsbehörde, ist das Blumenmodell deshalb auch nicht funktional, sondern sektoriell gegliedert. Konkret heisst das, dass die Zusammenarbeit nach Wirtschaftssektoren strukturiert ist. Berücksichtigt werden dabei all jene Sektoren, welche zu den kritischen Infrastrukturen zählen.

Aus der sektoralen Gliederung ergibt sich die Blumenstruktur des Modells. Die folgende Darstellung verdeutlicht diese Struktur:



SSIA: Sektorspezifischer Informationsaustausch

Die Blütenblätter repräsentieren dabei die kritischen Sektoren. Innerhalb dieser Blütenblätter findet der Informationsaustausch zwischen den einzelnen Unternehmen statt. Das Ziel ist es, die Informationssicherung innerhalb der Sektoren zu stärken, indem die Unternehmen sich gegenseitig über relevante Ereignisse (beispielsweise über neue Risiken und Bedrohungen oder über Sicherheitsvorfälle) informieren. Die Grundlage für einen solchen Informationsaustausch ist natürlich ein starkes Vertrauen zwischen den einzelnen Firmen. Darum wird den Sektoren auch eine gewisse Autonomie bei der internen Organisation zugestanden. So können sie beispielsweise selber definieren, welche Aufnahmekriterien für ihren Sektor gelten sollen.

Koordiniert wird dieser sektorspezifische Informationsaustausch durch Vertreter der Behörden. Diese stellen auch den Zugang zum Zentrum der Blume sicher, in welchem sowohl das CERT angesiedelt ist als auch sektorübergreifende Beratungsgremien. Das Ziel ist nicht nur, dass der Informationsaustausch zwischen Unternehmen vor allem innerhalb der Sektoren gefördert wird, sondern auch, dass alle Beteiligten auf die zentralen Dienstleistungen des CERTs zurückgreifen können.

Die Stärke dieses Modells liegt in der klaren Struktur für den Informationsaustausch. Durch den konstanten Austausch zwischen Unternehmen aus dem gleichen Sektor kann gegenseitiges Vertrauen aufgebaut werden. Lücken und Gefahren werden von den Betreibern entdeckt und diese Information mit den anderen Betreibern geteilt. Die Behörden übernehmen in diesem Modell vor allem die Funktion eines Koordinatoren für den sektorspezifischen Austausch. Dank dieser Aufgabe haben die Behörden einen direkten Zugang zu den Betreibern von kritischen Infrastrukturen. Dieser Zugang kann für die Sensibilisierung gegenüber aufkommenden neuen oder sich verändernden Bedrohungsszenarien genutzt werden.

Für die Betreiber der Infrastrukturen ist dieses Modell attraktiv, weil sie einerseits in einem geschützten Rahmen Informationen mit anderen Unternehmen mit ähnlichen Problemen austauschen können und gleichzeitig einen privilegierten Zugang zu den für sie wichtigen Dienstleistungen und Informationen des CERTs erhalten. Ein solches Modell ist zudem relativ flexibel, da zusätzliche Sektoren einfach integriert werden können. Im Vergleich mit dem Modell der IT-Sicherheitsbehörde ist es zudem weniger ressourcenintensiv.

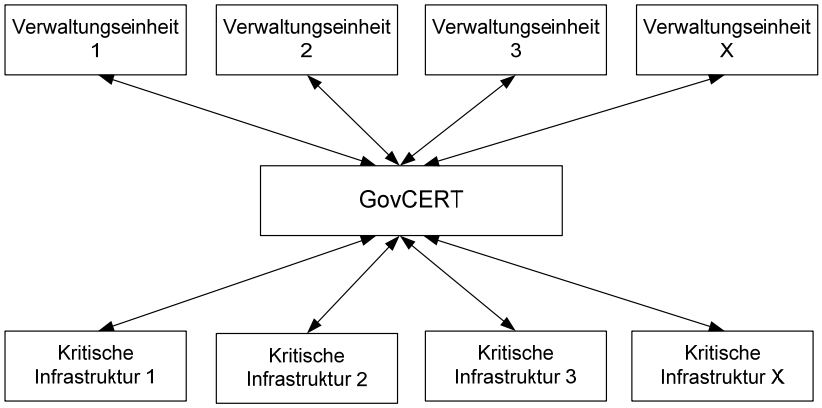
Dennoch ist der Koordinationsaufwand, der für die staatlichen Betreiber der Kooperationsplattform besteht, nicht zu unterschätzen. Um eine funktionierende Zusammenarbeit in den verschiedenen Sektoren zu etablieren, braucht es ein intensives Engagement der Behörden. Zudem besteht die Gefahr der Bildung von sogenannten Silos, d.h. von ausschliesslich sektorspezifischem Austausch und ebensolcher Koordination. Dem kann der Plattformbetreiber jedoch entgegenwirken, indem periodisch Veranstaltungen von sektorübergreifender Relevanz organisiert werden, was aber wiederum mit einem beträchtlichen Aufwand verbunden ist. Eine letzte eventuelle Schwäche dieses Modells ist die Dezentralisierung von Verantwortlichkeiten. Weil für jeden Sektor der jeweilige Sektor-Koordinator verantwortlich ist, kann es zu uneinheitlichen Vorgehensweisen und Unklarheiten zwischen den Sektoren kommen.

3.2.3 GovCERT+

Das Modell „GovCERT+“ lässt sich von den Beispielen aus Ländern wie Österreich oder Schweden ableiten. Im Vergleich zu den beiden bisher diskutierten Modellen, stehen beim GovCERT+-Modell die eigentlichen CERT-Dienstleistungen im Vordergrund. Weder wird wie beim Blumenmodell der Informationsaustausch in den kritischen Sektoren gezielt gefördert, noch wird wie beim Modell der IT-Sicherheitsbehörde versucht, eine umfassende Agentur zur Informationssicherung zu schaffen. Stattdessen basiert das GovCERT+-Modell auf der relativ einfachen Grundidee, dass die CERT-Dienstleistungen (beispielsweise technische Hilfe bei Vorfällen oder Warnungen über neue Gefahren), welche der Verwaltung zur Verfügung stehen, auch für die Informationssicherung von Betreibern kritischer Infrastrukturen

von Nutzen sein können. Deshalb wird der Kundenkreis des GovCERTs auf diese Betreiber kritischer Infrastrukturen ausgeweitet.

Das GovCERT+-Modell kann darum wie folgt dargestellt werden:



Die Graphik veranschaulicht, dass in diesem Modell die direkten Beziehungen zwischen dem CERT und den einzelnen Kunden (Verwaltungseinheiten oder Betreiber kritischer Infrastrukturen) wichtig sind. Dies ist ein wesentlicher Unterschied zum Blumenmodell, in welchem das CERT nur im Fall der Vorfallbekämpfung direkten Kontakt zu den Betreibern von kritischen Infrastrukturen hat. Während im Blumenmodell Aufgaben wie die Durchführung von Workshops, die Verbreitung von sektorspezifischen Warnungen oder die Organisation des Informationsaustausches durch einen Sektor-Koordinator wahrgenommen werden, ist es im GovCERT+-Modell eine zentrale Stelle, welche diese Aufgaben für alle Kunden übernimmt. Der Name GovCERT+ bezieht sich darum nicht nur auf den ausgeweiteten Kundenkreis (respektive die Tatsache, dass das Verwaltungs-CERT sich auch um die Anliegen der Betreiber kritischer Infrastrukturen kümmert), sondern auch auf die Ausweitung der Aufgaben. Die Organisation, die hier als GovCERT+ bezeichnet wird, leistet mehr als die klassische CERT-Funktion der Vorfallbekämpfung. Sie fördert auch den Informationsaustausch, organisiert Workshops und warnt die Kunden vor neuen Bedrohungen.

Die Stärke dieses Modells liegt denn auch in den direkten Beziehungen zwischen der GovCERT+-Organisation und den Kunden. Dadurch kann gut auf die Bedürfnisse der Betreiber von kritischen Infrastrukturen eingegangen werden. Als Stärke kann sicher auch erwähnt werden, dass mit einem solches Modell mit relativ wenig Ressourcen viel erreicht wird, weil sich die Dienstleistungen aufs Wesentliche beschränken. Umgekehrt ist es eine Schwäche des Modells, dass viele zusätzliche Bedürfnisse nicht abgedeckt werden: Der Informationsaustausch zwischen den Betreibern von Infrastrukturen wird kaum gefördert, da die Unternehmen nur mit dem GovCERT+ direkt kommunizieren, und die Warnungen und Workshops können nicht auf die spezifischen Bedürfnisse einzelner Sektoren angepasst werden. Eine weitere grosse Schwierigkeit ist die Definition des Kundenkreises. Dieser darf einerseits nicht zu gross sein, weil sonst das GovCERT+ an seine Kapazitätsgrenzen stösst, andererseits ist es sehr schwierig, klare Kriterien für die Kritikalität von Infrastrukturen zu erarbeiten, was dazu führen kann, dass Beitrittsbegehren von Unternehmen nur schwer abgelehnt werden können.

3.2.4 Stärken und Schwächen der drei Modelle

Die folgende Tabelle fasst die Stärken und Schwächen der drei oben identifizierten IA/CIIP Modelle zusammen:

	Stärken	Schwächen
IT Sicherheitsamt	• Zentralisierung /stabile Strukturen • Kontinuität • Klare Rechenschaftsordnungen und Verantwortlichkeiten • Einfachere Öffentlichkeitsarbeit und Sensibilisierung • Keine Doppelspurigkeiten	• Ressourcenintensiv • Keinen direkten/institutionalisierten Zugang zum privaten Sektor und den relevanten Informationen • Tendenz: der Privatsektor lager die IT-Sicherheitsaufgaben an den Staat aus • Inflexibel
Blumenmodell	• klar strukturierter und gut funktionierender Informationsaustausch • Relativ einfache Vertrauensbildung zwischen Unternehmen und zwischen privatem und öffentlichem Sektor • Gegenseitig privilegierter Zugang zwischen den Behörden und den Betreibern von kritischen Infrastrukturen • Hohe Flexibilität	• Erheblicher Koordinationsaufwand für die Behörden • Risiko von Silos – kein sektor-übergreifender Informationsaustausch • Dezentrale Verantwortlichkeiten
GovCERT+	• Direkte Beziehung GovCert zu Kunden • Ressourceneffektiv / Beschränkung aufs Wesentliche	• Kein Informationsaustausch zwischen Betreibern von kritischen Infrastrukturen • Schwierige Definition der Kritikalität der Sektoren

4 Evaluation von und Weiterentwicklungsoptionen für MELANI

Basierend auf der Umfrage im geschlossenen Kundenkreis, den ergänzenden Interviews und dem Vergleich mit internationalen Modellen zur Informationssicherung, werden in diesem Kapitel die Stärken und Schwächen von MELANI identifiziert. Darauf aufbauend werden verschiedene Optionen für die Weiterentwicklung von MELANI vorgestellt und auch deren Stärken und Schwächen abgewogen. Abschliessend werden Empfehlungen für die nächsten Schritte bei der Weiterentwicklung von MELANI formuliert.

4.1 Fazit der Evaluation

4.1.1 Evaluation durch die Mitglieder des GK

Die Ergebnisse aus der Befragung der Mitglieder des GK können in zwei Unterkapitel gegliedert werden. Erstens wird zusammengefasst, wie die Mitglieder des GK die aktuelle Arbeit von MELANI wahrnehmen und bewerten (IST-Zustand). Zweitens wird gezeigt, welche Erwartungen und Wünsche die Mitglieder des GK an MELANI haben (SOLL-Zustand aus Sicht der Mitglieder).

IST-Zustand: die Einschätzung der laufenden Arbeiten
Es darf festgestellt werden, dass MELANI die Erwartungen der Mitglieder des geschlossenen Kundenkreises in hohem Mass erfüllt. Die Mitglieder haben grossmehrheitlich ihre Zufriedenheit mit der Arbeit von MELANI geäussert und schätzen MELANI als Anlauf- und Analysestelle für Informationssicherheit. Auch wird das Geleistete als wichtig erachtet.

Die spezifischen Dienstleistungen von MELANI werden im Grossen und Ganzen gut bis sehr gut bewertet. Dabei wird von seitens der Mitglieder des GK insbesondere die Vertrauenswürdigkeit von MELANI-Produkten hervorgehoben. Sowohl die *Security Advisories* als auch die Workshops werden auf dieser Dimension am besten bewertet. Das heisst, dass MELANI im Vergleich zu privaten Anbietern, die ähnliche Dienstleistungen anbieten, hier für den geschlossenen Kundenkreis einen Mehrwert zu leisten vermag. Dies steht im Zusammenhang mit dem Vorteil der Nicht-Kommerzialität von MELANI. Es wurde mehrfach betont, dass dies zu einem Vertrauensvorschuss seitens der Mitglieder gegenüber MELANI führe. Diesem Vertrauensvorschuss wird MELANI offensichtlich gerecht. Die Unterstützung bei der Vorfallbekämpfung durch MELANI wird vor allem vom Finanzsektor beansprucht, geschätzt und grossmehrheitlich als entscheidend bewertet. Es zeigt sich, dass die Hilfe bei der Bewältigung von Vorfällen zwar nicht von allen Mitgliedern häufig genutzt wird, aber dennoch eine zentrale Funktion von MELANI bleibt.

Daneben ist die Förderung des Informationsaustausches ein weiterer wichtiger Aspekt. Es wurde festgestellt, dass der Informationsaustausch zwischen den Unternehmen auf Grund der Struktur des GK von MELANI sehr gering ausfällt. Der Informationsaustausch ist bei MELANI so angelegt, dass er über MELANI als Mittler läuft (‚Zentralismus').

In Bezug auf die Mitgliederzahl von MELANI, hält die Mehrheit der Mitglieder des GK die momentane Anzahl Mitglieder für genau richtig. Es sind aber immerhin mehr als ein Drittel der Befragten, die sich mehr Mitglieder wünschten. Dies trifft insbesondere auf jene Sektoren mit wenigen Mitgliedern zu.

SOLL-Zustand: die Bedürfnisse der Mitglieder des GK
Das wichtigste Bedürfnis der Mitglieder des GK sind qualifizierte und spezifische Informationen. MELANI sollte demgemäss Einschätzungen liefern, die den Unternehmen helfen, die Bedrohungslage zu verstehen und Risiken einzuordnen. Dies können technische Analysen des CERT sein, aber auch Informationen aus dem Nachrichtendienst, die den Mitgliedern des GK weitergegeben werden können. Allgemein sollten

die Dienstleistungen von MELANI so spezifisch wie möglich auf die Bedürfnisse der Unternehmen angepasst sein. Dies ist eine grosse Herausforderung, da diese Bedürfnisse sehr unterschiedlich sind. Es ist darum entscheidend, dass MELANI seine Kunden gut kennt und in einem ständigen Dialog mit ihnen steht.

Ein häufig geäussertes Bedürfnis ist auch eine Erleichterung des Informationsaustausches innerhalb des GK. Dies kann über eine Anpassung der Strukturen geschehen (siehe unten) oder auch durch das Einführen von neuen Kommunikationsmöglichkeiten auf MELANI-Net. So wird beispielsweise in der Kundenbefragung von verschiedenen Mitgliedern die Errichtung eines Online-Diskussionsforums oder einer internen Mailing-Liste angeregt. Solche zusätzlichen Möglichkeiten würden den „Eindruck einer Einbahn-Kommunikation“[34] mildern.

Wichtig ist auch eine klare Kommunikation seitens MELANI über neue interne Entwicklungen. So herrscht bei einigen Mitgliedern noch immer Unklarheit darüber, ob das SWITCH-CERT noch Teil von MELANI ist. Personelle Wechsel bei MELANI sollten ebenfalls sorgfältig kommuniziert werden, da die Kunden MELANI nicht zuletzt aufgrund von guten persönlichen Kontakten vertrauen.

Schliesslich weisen verschiedene Unternehmen darauf hin, dass im Bereich der Informationssicherung generell immer noch ein grosser Handlungsbedarf besteht. MELANI leistet zwar wertvolle Arbeit im Bereich des GK, für die kleinen und mittleren Unternehmen, ebenso wie für die breite Bevölkerung, scheint aber keine Institution auf Bundesebene verantwortlich zu sein. In der Befragung wurde darauf hingewiesen, dass diese Lücke wegen der starken Vernetzung der Informations- und Kommunikationstechnologien zu einem unzureichenden Schutz führt. Aus Sicht der Unternehmen wäre es darum wünschenswert, wenn MELANI auch in diesem Bereich eine aktivere Rolle spielen würde.

4.1.2 MELANI im internationalen Vergleich

Auch der Vergleich mit anderen staatlichen Modellen zur Informationssicherung kann dazu beitragen, Klarheit über die spezifischen Stärken und Schwächen von MELANI zu erhalten. In diesem Abschnitt soll deshalb versucht werden, MELANI mit den drei in Kapitel 3.2 vorgestellten generischen Modellen zu vergleichen.

MELANI ist nicht mit dem Modell einer IT-Sicherheitsbehörde vergleichbar: die Unterschiede in der Art und Weise, wie die Informationssicherung gewährleistet wird, sind zu gross. Eine IT-Sicherheitsbehörde ist aufgrund der zahlreichen Aspekte des kritischen Informationsinfrastrukturschutzes, mit dem sie beauftragt ist, zwingend gross und dementsprechend mit beträchtlichen Mitteln personeller und finanzieller Art ausstattet. Mit MELANI hat der Bundesrat aber eine verhältnismässig kleine Stelle zur Informationssicherung geschaffen.

Dem gegenüber ist jedoch ein Vergleich von MELANI sowohl mit dem GovCERT+ als auch mit dem Blumenmodell möglich. Zum jetzigen Zeitpunkt (und insbesondere seit dem Aufbau des GovCERT.ch) ist MELANI am ehesten mit dem Modell eines GovCERT+ vergleichbar. MELANI hat den Auftrag, die Informationssicherung innerhalb der Verwaltung und bei den Betreibern der kritischen Infrastrukturen zu fördern. Entsprechend ist auch der GK aus Vertretern der Verwaltung und der kritischen Sektoren zusammengesetzt. Ebenfalls analog zum GovCERT+-Modell ist der Informationsaustausch bei MELANI zentralistisch strukturiert, d.h. die Mitglieder des GK teilen die Informationen zunächst MELANI mit, bevor diese dann je nach Relevanz (und natürlich nur mit Erlaubnis des Informanten) von MELANI an die übrigen Mitglieder des GK weitergegeben werden.

Bei aller Ähnlichkeit zum GovCERT+-Modell sind aber auch Elemente von MELANI identifizierbar, die eher dem Blumenmodell entsprechen. So ist der GK nach Sektoren unterteilt und viele Aktivitäten,

[34] Zitat aus einer Äusserung eines Mitgliedes des GK.

wie beispielsweise die Veranstaltung von Workshops, sind gezielt auf die Bedürfnisse gewisser Sektoren ausgerichtet. Besonders in Sektoren, in welchen viele Unternehmen vertreten sind (vor allem im Finanzsektor, aber auch beispielsweise im Energiesektor, oder im Telekommunikationssektor), könnten mehr sektorspezifische Aktivitäten, wie sie in Grossbritannien und in den Niederlanden umgesetzt werden, sinnvoll sein.

Als Schwäche des GovCERT+-Modells wurde die schwache Förderung des Informationsaustausches zwischen den Unternehmen erwähnt, so wie die Schwierigkeiten, die Aktivitäten an die jeweils sehr verschiedenen Bedürfnisse aus den unterschiedlichen Sektoren anzupassen. Mit beiden Schwierigkeiten ist auch MELANI konfrontiert, begegnet dem aber wie erwähnt zum Teil mit der Durchführung von sektorspezifischen Aktivitäten. Schwerwiegender ist der Mangel an klaren Kriterien für die Mitgliedschaft im GK. Während der Entscheid über die Mitgliedschaft von Unternehmen im Ermessen von MELANI liegt, sieht beispielsweise das Modell von Österreich (das auch am ehesten ein GovCERT+-Modell umsetzt) vor, dass dieser Entscheid auf einer politischen Ebene (im Bundeskanzleramt) vorgenommen wird. Dies hat den Vorteil, dass die strategische von der operativen Ebene klar getrennt ist.

Ein sehr wichtiger Punkt ist die Frage nach den notwendigen Ressourcen. Es ist eine der Hauptstärken des GovCERT+-Modells, dass mit wenig Mitteln relativ viel erreicht werden kann. Jedoch sind die MELANI gegenwärtig zur Verfügung stehenden Mittel auch für ein GovCERT+-Modell äusserst knapp. Gerade um mehr sektorspezifische Aktivitäten durchführen zu können oder um den Informationsaustausch zwischen den anderen Unternehmen zu fördern, wären unbedingt mehr Mittel notwendig.

4.1.3 Stärken und Schwächen von MELANI

Aus der Wirkungsevaluation im GK und dem Vergleich von MELANI mit internationalen Modellen für die Informationssicherung, lassen sich die spezifischen Stärken und Schwächen von MELANI identifizieren:

Stärken:
• Die Erwartungen der Mitglieder des GK in MELANI werden insgesamt gut erfüllt, bemerkenswert ist insbesondere das hohe Vertrauen der Unternehmen in das Personal von MELANI • MELANI hat mit sehr wenigen Ressourcen viel erreicht, insbesondere bei der Vorfallbekämpfung • Der GK von MELANI konnte in den letzten drei Jahren ausgebaut werden. Heute ist ein Grossteil der Betreiber kritischer Infrastrukturen im GK vertreten
Schwächen:
• Die Ressourcen von MELANI sind äusserst knapp bemessen • Durch das starke Wachstum im GK hat MELANI seine Kapazitätsgrenzen erreicht • Es fehlen eindeutige Aufnahmekriterien für neue Mitglieder im GK • Der Informationsaustausch zwischen den Unternehmen wird kaum gefördert • Es fehlt eine klare Strategie für die Weiterentwicklung von MELANI hinsichtlich des Grundauftrages und der Ziele

Die identifizierten Schwächen sind teilweise miteinander verknüpft bzw. verstärken einander. Aus ihnen lassen sich folgende zentralen Herausforderungen ableiten:

- *Ressourcen:* Die MELANI gegenwärtig zur Verfügung stehenden Mittel sind im internationalen Vergleich sehr knapp. Das Problem dürfte sich in Zukunft noch verschärfen: Obwohl sich die Anzahl Kunden mehr als verdoppelt hat, operiert MELANI immer noch mit den gleichen personellen und finanziellen Mittel wie 2006. Die Ressourcenfrage bestimmt massgebend, wie MELANI weiterentwickelt werden kann.

- *Kundenkreis:* MELANI braucht klare Aufnahmekriterien für neue Mitglieder im GK, unabhängig davon, wie viele Ressourcen in Zukunft zur Verfügung stehen. Nur mit Hilfe klarer Kriterien ist eine strukturierte und zielgerichtete Weiterentwicklung des GK möglich. Diese Kriterien müssen in einem Strategieprozess definiert werden, in welchem auch bestimmt wird, welche Unternehmen zur Zielgruppe von MELANI gehören.
- *Dienstleistungen:* Es wird nicht möglich sein, bei gleichbleibenden Mitteln in Zukunft zusätzliche Dienstleistungen anzubieten (vgl. Wünsche des GK). Bei gleichbleibenden Ressourcen müssten die Dienstleistungen gekürzt und besser fokussiert werden. Dem Informationsaustausch ist dabei besondere Bedeutung zuzumessen. Die Ausgestaltung der Dienstleistungspalette müsste ebenfalls an eine klare Strategie für die Weiterentwicklung geknüpft werden.
- *Strategie für die Weiterentwicklung von MELANI*: Alle Herausforderungen sind mit der strategischen Ausrichtung von MELANI verknüpft. Der Grundauftrag von MELANI muss eindeutig definiert werden, damit sich MELANI gegenüber den Partnern aus dem Privatsektor und innerhalb der Bundesverwaltung klar positionieren kann.

4.2 Zukunftsoptionen

Es gibt verschiedene Möglichkeiten, wie diesen Herausforderungen begegnet werden kann. Ausgehend von den identifizierten Stärken und Schwächen und in Anlehnung an die idealtypischen Modelle werden in diesem Kapitel deshalb vier mögliche (d.h. umsetzbare) Zukunftsoptionen für MELANI skizziert[35]

1) Weiterführung von MELANI bei gleichbleibenden Mitteln
2) Konsolidierung der bisherigen Arbeit durch Ausbau des GovCERT+
3) Umgestaltung von MELANI zu einer Plattform für Informationsaustausch
4) Pragmatische Umsetzung des Blumenmodells

Die Optionen unterscheiden sich hinsichtlich des benötigten Aufwandes, aber auch in Bezug auf die Aufgaben, für welche MELANI verantwortlich wäre. Jede Option hat einen spezifischen Einfluss auf die folgenden oben identifizierten Kategorien:

- die benötigten Ressourcen,
- den Kundenkreis (Ausgestaltung/Grösse),
- die Dienstleistungen (Art/Menge),
- mögliche Kooperationspartner und
- die organisatorische Einbettung von MELANI in der Bundesverwaltung.

4.2.1 Weiterführung von MELANI bei gleichbleibenden Mitteln

Option eins ist die Weiterführung von MELANI mit gleichbleibenden Mitteln. Diese Option scheint angesichts der guten Bewertungen der bisherigen Arbeit von MELANI durch die Mitglieder des GK auf den ersten Blick attraktiv. Sie muss aber skeptisch beurteilt werden, da zu bezweifeln ist, ob es mit gleichbleibenden Mitteln gelingen kann, die Dienstleistungen auch weiterhin in ähnlicher Qualität anzubieten. Weil der GK in den letzten Jahren stark gewachsen ist und weil die Informationssicherung in Zukunft vermutlich weiter an Bedeutung gewinnen wird, droht MELANI eine Überlastung, wenn versucht wird, die gleichen Dienstleistungen ohne zusätzlichen Mitteleinsatz weiterzuführen. Darüber hinaus besteht die

35 Die Option IT-Sicherheitsbehörde erachten wir als nicht umsetzbar. Deshalb wird sie nicht diskutiert.

Gefahr, dass eine Verringerung der Dienstleistungen (oder deren Qualität) das Partnerschaftsmodell – und damit die Grundidee von MELANI – gefährden könnte.

Diese Option hätte die folgenden Auswirkungen:

- *Personal/Ressourcen:* MELANI erhält keine weiteren Ressourcen zugesprochen.
- *Kundenkreis:* Der GK kann nicht mehr weiter ausgebaut werden, weil MELANI an Kapazitätsgrenzen stösst. MELANI muss sich sogar überlegen, den GK zu verkleinern, um dadurch die Qualität der Dienstleistungen für die verbliebenen Mitglieder sicherzustellen.
- *Kooperationen:* MELANI ist stark darauf angewiesen, Kooperationspartner zu finden, die einen Teil der Aufgaben übernehmen. Innerhalb der Bundesverwaltung könnten beispielsweise Kapazitäten des MilCERTs genutzt werden. Auch eine Zusammenarbeit mit CERTs aus dem Privatsektor sollte verstärkt angestrebt werden (gemäss Beispiel CERT-Verbund in Deutschland).
- *Dienstleistungen:* Die Anzahl und Art der Dienstleistungen wird überprüft. MELANI muss sich auf das Minimum beschränken, was vor allem ein Fokus auf die klassischen CERT-Aufgaben bedeutet. Die Förderung des Informationsaustausches und die Durchführung von Workshops müssen reduziert werden. Um den bestehenden hohen Erwartungen entgegenzuwirken, muss MELANI klar kommunizieren, welche Dienstleistungen noch angeboten werden können und welche Services nicht mehr zum Zuständigkeitsbereich von MELANI gehören.
- *Organisatorische Einbettung*: Die wenigen Mittel werden konzentriert und alle Untereinheiten von MELANI werden in einem Departement zusammengefasst. Eine konsolidierte Zusammenarbeit mit anderen Bundesstellen (z.B. MilCERT, CSIRT BIT, ZEO usw.) wäre zu prüfen.

Stärken der Option:
• Keine zusätzlichen Ressourcen nötig
Schwächen der Option:
• Auftrag Informationssicherung kann nur noch teilweise erfüllt werden • Eine Reduktion des Angebotes birgt das Risiko, dass wichtige Unternehmen ihr Interesse an einer Zusammenarbeit verlieren • Der Fokus auf die Aufgaben als CERT birgt das Risiko, dass wichtige Informationen aus dem Privatsektor MELANI nicht mehr mitgeteilt werden

4.2.2 Konsolidierung der bisherigen Arbeit durch Ausbau des GovCERT+

Wie oben erwähnt, ist MELANI heute am ehesten dem GovCERT+-Modell vergleichbar. Eine relativ einfach umsetzbare Option ist deshalb der Ausbau der Aktivitäten gemäss diesem Modell. Das Ausmass des Ausbaus hängt stark von den Ressourcen ab, welche MELANI in Zukunft zur Verfügung stehen. Ein gewisser Mehraufwand wird aber in jedem Fall nötig sein. Ein GovCERT+-Modell ist für die Kunden aus dem Privatsektor nur dann attraktiv, wenn ihnen mit geeigneten Dienstleistungen ein echter Mehrwert geboten wird.

Diese Option hätte die folgenden Auswirkungen:

- *Personal/Ressourcen*: Das Personal wird aufgestockt. Vor allem das GovCERT muss verstärkt werden, weil es in dieser Option eine Schlüsselrolle einnimmt. Insgesamt ist diese Option in Bezug auf den Aufwand aber recht flexibel: Je nach Ambitionen in Bezug auf die Dienstleistungen und Grösse des Kundenkreises, entsteht ein grösserer oder kleinerer Bedarf an zusätzlichen Ressourcen.

- *Kundenkreis:* Nur noch Betreiber kritischer Infrastrukturen haben Zugang zum GK von MELANI. Der Entscheid, welche Unternehmen kritische Infrastrukturen sind und welche nicht, ist in der Praxis aber oft sehr schwer zu treffen, weil Informationsinfrastrukturen sehr verschiedene Unternehmen miteinander vernetzen. Die Beschränkung des GK ist darum eine schwierige Herausforderung.
- *Kooperationen:* Die Zusammenarbeit mit CERTs aus der Bundesverwaltung und aus der Privatwirtschaft wird verstärkt. Um der Problematik der Beschränkung des GK zu begegnen, werden mit anderen Partnern Aktivitäten für jene Unternehmen durchgeführt, die keinen Zugang zum GK erhalten. Zum Beispiel kann MELANI ihr Engagement in der Stiftung Infosurance (die die Informationssicherung in KMUs zu fördern sucht) verstärken.
- *Dienstleistungen:* MELANI muss den Betreibern kritischer Infrastrukturen einen wirklichen Mehrwert bieten; die Kunden sind an exklusiven (normalerweise nicht zugänglichen) und spezialisierten Informationen und Workshops interessiert. Die verschiedenen Bedürfnisse der einzelnen Kunden bleiben eine grosse Herausforderung.
- *Organisatorisch*: Das GovCERT ist zentral wichtig. Alle in der Bundesverwaltung vorhandenen Stellen mit CERT-ähnlichen Aufgaben werden zusammengeführt. Mittelfristig gewinnt das GovCERT dadurch an Kapazitäten. Das GovCERT wird dadurch bedeutend grösser und müsste eventuell unter eine eigene Leitung gestellt werden.

Stärken der Option:
• Einfach umsetzbar, da auf bestehenden Strukturen aufgebaut wird • Kann flexibel angepasst werden und ermöglicht dadurch ein langsames Wachstum • Klarer Fokus auf den Grundauftrag der Informationssicherung im Bereich kritischer Infrastrukturen
Schwächen der Option:
• Die Grösse des GK muss beschränkt bleiben – es ist schwierig zu definieren, welche Unternehmen dazu gehören sollen • Die unterschiedlichen Bedürfnisse der Unternehmen können nur schwer alle gleichzeitig berücksichtigt werden • Der Informationsaustausch zwischen den Unternehmen wird nicht gefördert

4.2.3 Umgestaltung von MELANI zu einer Plattform für den Informationsaustausch

Option drei besteht in der Umgestaltung des GK in Richtung eines Blumenmodells. Wenn davon ausgegangen wird, dass der GK weiter wächst, muss versucht werden, diesen besser zu strukturieren und den Informationsaustausch zwischen den Unternehmen unabhängig vom CERT zu fördern. Bei dieser Option finden die Aktivitäten von MELANI vor allem in den verschiedenen Sektoren statt. MELANI wird verstärkt zu einer Plattform für den Informationsaustausch. Die CERT Funktion bleibt zwar erhalten, ist aber nur noch ein Teil des Aufgabengebietes und nicht mehr die Hauptaufgabe. Eine solche Neuausrichtung bringt erhebliche Veränderungen mit sich.

Diese Option hätte die folgenden Auswirkungen:

- *Personal/Ressourcen:* Die personellen Ressourcen von MELANI werden stark vergrössert, da es in jedem Sektor einen Sektor-Koordinator braucht. Zwar können einzelne Mitarbeiter mehrere Sektoren betreuen, aber es ergibt sich ein beträchtlicher Mehraufwand, weil die CERT-Funktionen gleichzeitig beibehalten werden.

- *Kundenkreis:* Insgesamt wird der GK vergrössert, da eine sektorielle Organisation nur dann Sinn macht, wenn in den einzelnen Sektoren auch genügend Unternehmen vertreten sind. Besonders in den Sektoren, die heute nur wenige Unternehmen umfassen, müssen aktiv neue Mitglieder rekrutiert werden. Weil die meisten Aktivitäten innerhalb des Sektors stattfinden, wird es den Sektoren (in Abstimmung mit den von MELANI gestellten Sektor-Koordinatoren) überlassen, welche Kriterien für die Mitgliedschaft im GK ihres Sektors gelten.
- *Kooperationen:* Die übergeordnete Gesamtsicht bezüglich Schutz kritischer Infrastrukturen rückt ins Zentrum. Das Bundesamt für Bevölkerungsschutz (BABS), das mit der Ausarbeitung einer SKI Strategie beauftragt ist, ist daher ein wichtiger Partner. Auch mit dem Bundesamt für Wirtschaftliche Landesversorgung, das ebenfalls aktiv den Informationsaustausch zwischen Unternehmen fördert, entstehen verschiedene Synergien. Für die Arbeit in den einzelnen Sektoren werden diverse Partner in passenden Departementen gesucht.
- *Dienstleistungen:* Die sektor-spezifischen Aktivitäten werden durch Sektor-Koordinatoren ausgeführt. Diese werden von MELANI oder von Kooperationspartnern gestellt. Wichtig bleiben aber die CERT-Dienstleistungen und die Bedrohungsanalysen von MELANI, weil der Zugang zu effizienter Vorfallbekämpfung und zu exklusiven Warnungen und Informationen einen wesentlichen Anreiz für die Unternehmen bieten, beim Informationsaustausch mitzumachen.
- *Organisatorisch*: Diverse Kooperationen mit Partnern aus der Bundesverwaltung sind möglich und sinnvoll. Die Arbeit im GK, die den Austausch von Informationen zwischen Unternehmen zum Ziel hat, wird zu einem breit abgestützten Programm innerhalb der Bundesverwaltung, das in die Strategie für den Schutz kritischer Infrastrukturen eingebunden ist. MELANI übernimmt dabei ein Teil dieses Programms und konzentriert sich auf die Aspekte der Informationssicherung.

Stärken der Option:

- Der Informationsaustausch zwischen den Unternehmen wird gestärkt
- Das Blumenmodell lässt sich gut in eine breite Strategie zum Schutz kritischer Infrastrukturen einbetten
- Der GK kann erweitert werden, ohne dass eine Überlastung droht, da der Grossteil der Aktivitäten in den Sektoren stattfindet

Schwächen der Option:

- Eine Grundlegende Änderung der gewachsenen Strukturen von MELANI kann zu Unklarheiten führen
- Die Option ist vergleichsweise ressourcenintensiv, auch wenn Kooperationspartner gefunden werden
- Die Strategie für den Schutz kritischer Infrastrukturen (SKI) ist erst in Entwicklung. Dadurch kann die Option momentan noch nicht als Teil einer breiteren Strategie für SKI umgesetzt werden.

4.2.4 Pragmatische Umsetzung des Blumenmodell

Neben den Optionen GovCERT+ und derjenigen der Umgestaltung von MELANI hin zu einer Informationsaustauschplattform gemäss Blumenmodell, gibt es auch die Möglichkeit, diese beiden Optionen zu kombinieren. Diese Option wird als pragmatische Umsetzung des Blumenmodells bezeichnet, da die Struktur des Kundenkreises zwar wie beim Blumenmodell sektoriell gegliedert ist, aber nicht in allen kritischen Sektoren eine sektorspezifische Austauschplattform etabliert wird. Solche sollen nur in Sektoren umgesetzt werden, die schon über viele Mitglieder verfügen und in welchen ein grosses Bedürfnis seitens der Unternehmen besteht, sich gegenseitig auszutauschen. Im Falle von MELANI wären dies zum jetzigen Zeitpunkt der Finanzsektor und eventuell der Energiesektor. Bei den übrigen Sektoren könnte man die weitere Entwicklung abwarten und je nach Bedürfnis und Wachstum auch erst später sektorspezifische Austauschplattformen kreieren. Bis dahin würde in diesen Sektoren die bisherige Struktur der direkten

Beziehung zwischen MELANI und den einzelnen Unternehmen analog dem GovCERT+-Modell beibehalten.

Diese Option hätte die folgenden Auswirkungen:

- *Personal/Ressourcen:* Für die Koordination der Aktivitäten in den Sektoren mit vielen Mitgliedern werden zusätzliche Stellen geschaffen. Die Aktivitäten in den Sektoren, für die eine Austauschplattform etabliert wird, führt aber gleichzeitig zu einer Entlastung im CERT (beispielsweise durch eine Bündelung der Anfragen).
- *Kundenkreis:* Die grossen Unterschiede zwischen den Sektoren können berücksichtigt werden. Beispielsweise im Finanzsektor, wo bereits mehr als 30 Firmen vertreten sind, werden die sektorspezifischen Aktivitäten verstärkt. Dadurch wird sichergestellt, dass die Qualität der Dienstleistungen für diesen Sektor auch bei einem weiteren Wachstum erhalten bleibt. In anderen Sektoren, wie beispielsweise im Sektor Industrie, wo erst zwei Firmen vertreten sind, werden die direkten Kontakte zwischen MELANI und den Kunden aufrechterhalten, da so am besten auf die individuellen Bedürfnisse dieser Unternehmen eingegangen werden kann.
- *Kooperationen:* Die Etablierung von sektor-spezifischen Austauschplattformen bietet Raum für Kooperationen mit anderen Akteuren aus der Bundesverwaltung. Teile der Koordinationsaufgaben werden delegiert. Es wird kein umfassendes Modell zum Schutz kritischer Infrastrukturen geschaffen; dennoch wird die Entwicklung von Austauschplattformen mit jenen Bundesämtern abgestimmt, welche im Bereich SKI tätig sind (BABS, BWL), um eine spätere Integration der Plattformen in SKI-Programme zu ermöglichen.
- *Dienstleistungen:* Durch die Auslagerung der Aktivitäten in Sektoren mit vielen Mitgliedern an einen Sektor-Koordinator werden Kapazitäten frei, die für die direkte Betreuung von Firmen aus Sektoren mit weniger Unternehmen genutzt werden können. So kann verhindert werden, dass die Aktivitäten von MELANI zu stark von den Bedürfnissen eines stark wachsenden Sektors bestimmt werden.
- *Organisatorisch*: Es bestehen verschiedene Möglichkeiten für die organisatorische Einbettung von MELANI. Wenn vermehrt Aufgaben übernommen werden, die im Bereich der Bekämpfung von Cyber-Kriminalität liegen (was vor allem für den Finanzsektor wichtig wäre), müsste eine bessere Anbindung ans Justiz und Polizei Departement angestrebt werden.

Stärken der Option:
• Basiert auf der momentanen Zusammensetzung des GK und kann darum relativ leicht umgesetzt werden • Berücksichtigt die unterschiedlichen Bedürfnisse und unterschiedliche Grösse der verschiedenen Sektoren • Verhindert eine Überlastung von MELANI und eine Dominanz durch einen Sektor
Schwächen der Option:
• Braucht zusätzliches Personal zur Koordination mit anderen Sektoren • Keinen eindeutigen Fokus auf den Schutz kritischer Infrastrukturen

5 Schlussfolgerung und Empfehlungen

Die vier in Kapitel 4.2 beschriebenen Weiterentwicklungsoptionen unterscheiden sich hinsichtlich des benötigten Aufwandes, in Bezug auf die Aufgaben, für welche MELANI verantwortlich wäre und in Bezug auf die benötigten Ressourcen. Um eine der Optionen auswählen zu können, braucht es in erster Linie Klarheit über den Grundauftrag und die Ziele von MELANI in der Zukunft. Darüber hinaus können Empfehlungen in Bezug auf Sofortmassnahmen gemacht werden, die einige der identifizierten Schwächen beheben könnten.

Strategie

Das einzige aktuell verfügbare strategische Dokument zur Informationssicherung und der Rolle von MELANI ist der Bericht „Verletzliche Informationsgesellschaft: Herausforderung Informationssicherung" aus dem Jahr 2003. Dieser Bericht definiert die Funktionen von MELANI in erster Linie als Lagezentrum mit der Aufgabe der Frühwarnung im Bereich Informationssicherung und als Koordinationsstelle für den Fall einer Krise. Während MELANI diese Funktionen immer noch wahrnimmt, hat sich in den letzten Jahren gezeigt, dass gezielte, mit krimineller Absicht ausgeführte Angriffe auf Firmen viel häufiger vorkommen als Attacken auf das gesamte Netzwerk. Ein grosser Teil der Arbeit die MELANI heute verrichtet, liegt deshalb häufig unterhalb der „Krisenschwelle". Das Beispiel des Finanzsektors zeigt, dass MELANI einen wichtigen Beitrag zur Koordination des Kampfes gegen Cyber-Kriminalität leisten kann. Zugleich lassen sich diese Aktivitäten aber nicht mehr direkt auf den Auftrag zur Informationssicherung von kritischen Infrastrukturen zurückführen. Um definieren zu können, für welche Bereiche der Informationssicherung MELANI verantwortlich ist und wo die Prioritäten liegen sollen, muss darum eine Strategie zur Informationssicherung formuliert werden.

Empfehlung 1: Die Weiterführung von MELANI sollte auf einer Strategie zur Informationssicherung abgestützt sein, die Grundauftrag und die Ziele von MELANI definiert und Klarheit schafft, für welche Aufgaben MELANI zuständig ist.

Eine Strategie umfasst den Prozess des Zurückblickens und des Identifizierens der möglichen Wege in die Zukunft. Sie zeigt auf, wie die Zukunftsvision im Rahmen gegebener Werte, Mittel und Möglichkeiten verwirklicht werden kann. Aus einer solchen Strategie leiten sich daher die benötigten Ressourcen ab. Dabei gilt es zu beachten, dass die Resultate aus der Umfrage und die Gespräche mit Vertretern aus dem GK Hinweise dafür geliefert haben, dass MELANI heute an die Leistungsgrenzen gestossen ist. Aus Sicht der Privatwirtschaft leistet MELANI zwar wichtige Arbeit, müsste aber verschiedene Bereiche ausbauen, um weiterhin einen relevanten Beitrag zur Informationssicherung leisten zu können. Die Mitglieder des GK wünschen sich von MELANI Dienstleistungen und Informationen, welche sie nirgendwo anders erhalten können. Um solche exklusiven Services bieten zu können, muss MELANI mit mehr Ressourcen ausgestattet werden. Die Option der Weiterführung mit gleichbleibenden Mitteln ist daher klar nicht zu empfehlen. Die strategische Ausrichtung wird die Wahl zwischen Option 2, 3 und 4 ermöglichen.

Sofortmassnahmen

Ein Strategiefindungsprozess ist aber normalerweise ein relativ zeitintensiver Prozess und es sollte verhindert werden, dass MELANIs Weiterentwicklung dadurch blockiert wird. Die vorliegende Evaluation zeigt einige mögliche Sofortmassnahmen auf, die umgesetzt werden könnten. Die Analyse des GK hat gezeigt, dass vor allem der Finanzsektor eine Sonderstellung innehat. Einerseits ist diese Sonderstellung durch die

grosse Anzahl Mitglieder bedingt, andererseits aber auch dadurch, dass die Informationssicherung in diesem Sektor eine wichtigere Stellung einnimmt als in anderen Sektoren. MELANI könnte relativ leicht eine separate Austauschplattform für den Finanzsektor errichten und dadurch Kapazitäten freimachen für die Betreuung der Unternehmen aus anderen Sektoren. Je nach Bedürfnis können solche Austauschplattformen dann auch für den Energiesektor oder andere Sektoren erstellt werden. Auf Grund dieser Überlegungen kann folgende Empfehlung gemacht werden:

Empfehlung 2: Bei der Weiterentwicklung des GK sollten die grossen Unterschiede zwischen den Sektoren beachtet werden. Deshalb sollte überprüft werden, für ausgewählte Sektoren sektorspezifische Plattformen für den Informationsaustausch zu erstellen. Es wird empfohlen, den GK gemäss der oben beschriebenen Option „pragmatische Umsetzung des Blumenmodells" weiter zu entwickeln.

Eine Entwicklung hin zu einer stärkeren sektoriellen Gliederung des GK von MELANI würde es auch ermöglichen, die Dienstleistungen spezifischer auf die Bedürfnisse der Firmen aus den verschiedenen Sektoren anzupassen. Generell können aus den Ergebnissen der Wirkungsevaluation der Aktivitäten im GK die folgenden drei Empfehlungen für die Weiterentwicklung der Dienstleistungen abgegeben werden:

1) MELANI soll, wenn immer möglich, erhaltene Informationen durch eigene Analysen ergänzen und aufwerten.
2) Die Warnungen und Informationen von MELANI sind für die Mitglieder des GK vor allem dann wertvoll, wenn sie aus Quellen stammen, die den Unternehmen sonst nicht zugänglich sind. MELANI soll darum vermehrt solche Informationen weiterzugeben.
3) Der Austausch zwischen den Unternehmen soll erleichtert werden. Dafür könnte auf MELANI-Net ein Diskussionsforum eingerichtet werden oder eine interne Mailing-Liste erstellt werden.

CSS
ETH Zurich

Das **Center for Security Studies der ETH Zürich** wurde 1986 gegründet und befasst sich in Lehre, Forschung und Dienstleistung mit Fragen der schweizerischen und internationalen Sicherheitspolitik. Zu den Forschungsschwerpunkten gehören neue Risiken, europäische und transatlantische Sicherheitspolitik, Strategie und Doktrin, Staatenzerfall und Staatenaufbau sowie schweizerische Aussen- und Sicherheitspolitik. Das CSS leitet das International Relations and Security Network (ISN). Es verfügt über ein breites Netzwerk aus nationalen und internationalen Partnerorganisationen und ist Mitglied des Center for Comparative and International Studies (CIS) der ETH und der Universität Zürich.