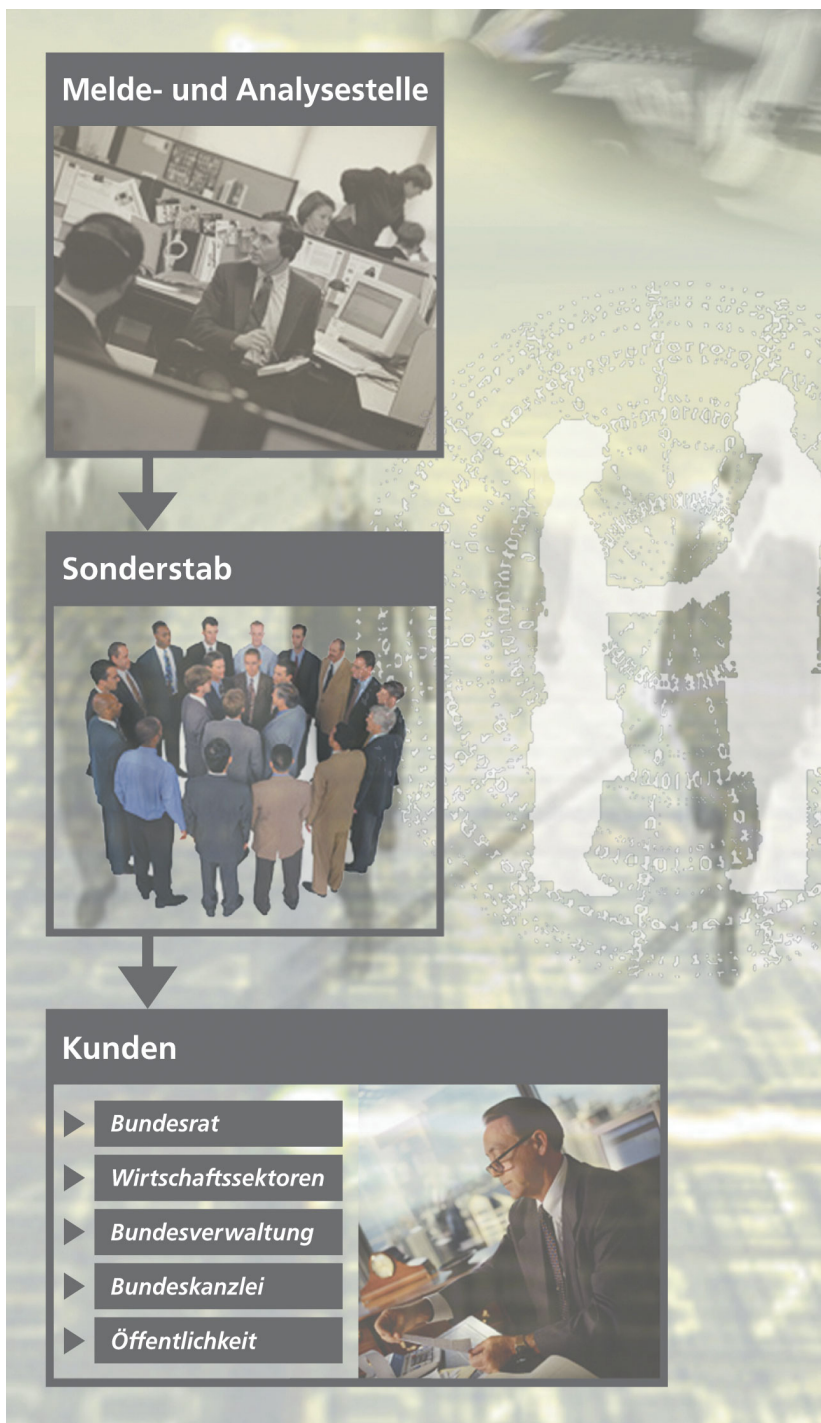


Einsatzkonzept Information Assurance Schweiz

Melde- und Analysestelle Informationssicherheit (MELANI)
Sonderstab Information Assurance (SONIA)

Schlussbericht vom 30. November 2001



Ernst **Basler + Partner** AG

FACHHOCHSCHULE
ZENTRALSCHWEIZ

HTA

HOCHSCHULE FÜR
TECHNIK+ARCHITEKTUR
LUZERN

Vorwort

Das vorliegende Einsatzkonzept „Information Assurance Schweiz“ wurde im Auftrag des Informatikstrategieorgans Bund (ISB) erstellt. Die Bearbeitung erfolgte im Zeitraum von November 2000 bis November 2001 durch die Firma Ernst Basler + Partner AG, Zollikon, Schweiz. Das Konzept berücksichtigt den Stand der Diskussion bis November 2001.

Die Ausführungen zu den Einsatzkriterien wurden durch die Hochschule für Technik und Architektur (HTA) in Luzern erstellt.

Dieses Konzept richtet sich an die Personen und Organisationen, die für die Umsetzung der Einsatzorgane Information Assurance zuständig sind. Es wurde daher auf eine Zusammenfassung des Berichts verzichtet.

Allgemein verwendete Literatur ist im Literaturverzeichnis aufgeführt. Auf punktuelle Ergänzungen wird in den Fussnoten hingewiesen.

Die Autoren danken Dr. Ruedi Rytz vom Informatikstrategieorgan Bund für das Bereitstellen von Texten und Abbildungen, die für diesen Bericht verwendet wurden.

Zollikon, 30. November 2001

Inhaltsverzeichnis

1	Einleitung.....	1
1.1	Auftrag.....	1
1.2	Vorgehen.....	2
1.3	Situationsanalyse.....	4
1.4	Konsequenzen.....	11
2	Melde- und Analysestelle Informationssicherheit.....	13
2.1	Kundenbedürfnisse.....	13
2.2	Aufgaben.....	17
2.3	Produkte.....	18
2.4	Informationsfluss MELANI.....	19
2.5	Funktionen und Verantwortlichkeiten.....	22
2.6	Organisationsmodell.....	24
2.7	Kostenschätzung.....	26
3	Sonderstab Information Assurance.....	28
3.1	Aufgaben vor und nach der Krise.....	28
3.2	Aufgaben in der Krise.....	29
3.3	Organisationsmodell.....	32
3.4	Ausbildung und Training.....	36
3.5	Kostenschätzung.....	38
4	Verbundsystem.....	40
4.1	Zusammenarbeit.....	40
4.2	Kunden und Partner.....	43
4.3	Einsatzkriterien für SONIA.....	45
5	Ausblick und Empfehlungen.....	56

Anhänge

- A1 Szenarien zur Gefährdung der Informationsinfrastruktur
- A2 Basisinformationen zu Melde- und Analysestellen weltweit
- A3 Fragebogen Sonderstab Informationssicherheit
- A4 Fragebogen für ausländische Melde- und Analysestellen
- A5 Fragebogen Kundenbedürfnisse einer Melde- und Analysestelle
- A6 Einsatzszenarien Sonderstab Information Assurance (HTA Luzern)

1 Einleitung

1.1 Auftrag

Informationssicherheit als
zentrales Thema

Die Notwendigkeit des Schutzes der schweizerischen Informationsinfrastrukturen und damit auch der Bundesverwaltung wurde sowohl als Schlussfolgerung der Strategischen Führungsübung 97 als auch im sicherheitspolitischen Bericht 2000 klar festgehalten.

Strategie
Informationsgesellschaft Schweiz

Am 18. Februar 1998 verabschiedete der Bundesrat die Strategie für die Informationsgesellschaft Schweiz. Neben Massnahmen im Ausbildungsbereich und aus wirtschaftlicher und gesetzgeberischer Sicht wurde insbesondere auch auf die Aspekte Sicherheit und Verfügbarkeit hingewiesen.

Politischer Auftrag

Mit Beschluss vom 22. Juni 2000 genehmigte der Bundesrat das Konzept „Information Assurance“. Neben der Unterstützung der Stiftung InfoSure als gemeinsames Organ von Privatwirtschaft und Verwaltung und der Neugründung des Milizamts für „Informations- und Kommunikationsinfrastruktur“ der wirtschaftlichen Landesversorgung wurde darin das Informatikstrategieorgan Bund (ISB) des EFD beauftragt, einen Sonderstab Information Assurance zu gründen.¹⁾ Die Übung INFORMO 2001 der Strategischen Führungsausbildung zeigte zudem die Notwendigkeit einer permanenten Melde- und Analysestelle Informationssicherheit (im Folgenden kurz: MELANI) in Ergänzung zum Sonderstab Information Assurance (im Folgenden kurz: SONIA) für ein erfolgreiches Krisenmanagement.²⁾

Ziel: Einsatzorganisation
Information Assurance

Zur Lagebeobachtung, der Analyse von Meldungen und zur Alarmierung von SONIA ist eine permanente MELANI zu schaffen. Sie muss in ein enges nationales und internationales Netzwerk mit IT-Betreibern in Wirtschaft und Verwaltung und anderen Stellen mit vergleichbarem Aufgabenspektrum eingebunden sein.

Mit der Bildung des SONIA soll ein Organ für die Bewältigung von Krisen im Bereich Informationssicherheit geschaffen werden. SONIA soll zur Beratung der politischen Führung und der Schaffung einer Plattform zum Austausch in Krisensituationen dienen. Durch den Einbezug von geeigneten

1) Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung vom 23. Februar 2000 (BinfV), Art. 7 Abs. 3 auch: Eidgenössisches Finanzdepartement, Informationsnotiz an den Bundesrat: Informatiksicherheit in der Schweiz "Information Assurance", Stand am 30. November 2000.

2) Zur Verwendung der Begriffe: Sonderstab Information Assurance (SONIA), Melde- und Analysestelle Informationssicherheit (MELANI)

Stellen ausserhalb der Bundesverwaltung soll er im Weiteren ein Bindeglied zwischen Verwaltung und Wirtschaft darstellen.

Auftrag und Inhalt dieses Berichtes	Aufgrund dieser Ausgangslage hat das Informatikstrategieorgan des Bundes (ISB) der Firma Ernst Basler + Partner AG den Auftrag erteilt, ein Konzept für MELANI und SONIA zu erarbeiten. Dabei sollen neben einer Situationsanalyse die grundlegenden Fragen zu Auftrag und Einsatz und Organisation dieser Organe diskutiert werden. Das ursprüngliche Konzept SONIA wurde zwischen November 2000 und Februar 2001 erarbeitet. Die Überarbeitung aufgrund der Erkenntnisse u.a. aus INFORMO 2001 sowie die Arbeiten für MELANI wurden von August bis November 2001 durchgeführt.
Adressat	Der vorliegende Bericht richtet sich an die für die Umsetzung verantwortlichen Institutionen des Auftraggebers. Das entsprechende Hintergrundwissen wird daher vorausgesetzt.

1.2 Vorgehen

Erarbeitung des Konzepts	Die Erarbeitung des vorliegenden Konzepts verlief im Wesentlichen in acht Schritten, die im Folgenden kurz erläutert werden:
--------------------------	--

Erarbeitung des Konzepts SONIA

1. Sichten der wichtigsten Unterlagen	Der erste Schritt umfasst das Sichten und Analysieren der wichtigsten Grundlagen und Daten sowie die Identifikation der betroffenen Stellen und Organisationseinheiten. Im Zentrum stehen dabei die Unterlagen, die im Rahmen der Strategischen Führungsübung 97 erstellt worden sind sowie Konzepte und Studien, die im Zusammenhang mit der Bildung der Stiftung InfoSurance entstanden sind.
2. Analyse von bestehenden Organisationen im Inland...	Verschiedene staatliche oder private Stellen sind bei Fragen der Informationssicherheit Schweiz involviert (Bundesamt für wirtschaftliche Landesversorgung, Stiftung InfoSurance, SFA etc.) und sollten entsprechend vernetzt werden, um Synergien zu nutzen resp. Kompetenzprobleme und Doppelspurigkeiten zu vermeiden. Dabei sind auch Erfahrungen mit anderen Sonderstäben des Bundes resp. Einsatzorganisationen miteinzubeziehen. Als Beispiel sei auf die Verordnung über den Sonderstab Geiselnahme und Erpressung resp. die Einsatzorganisation bei erhöhter Radioaktivität hingewiesen. ³⁾

3) Vgl. Verordnung über den Sonderstab Geiselnahme und Erpressung (SR 172.213.80) und Verordnung über die Einsatzorganisation bei erhöhter Radioaktivität VEOR (SR 732.32).

-
- ... und im Ausland Ein kritischer Punkt ist die Frage, in welchen Situationen SONIA eingesetzt werden soll. Dabei kann auf Erfahrungen aus ähnlichen Organisationen in der Privatwirtschaft resp. auf Vergleiche mit anderen nationalen und internationalen Gremien (CERT, KRITIS, NIPC, FedCIRC, CIAO etc.) aufgebaut werden.
3. Schriftliche Befragung unter Experten Für die weiteren Arbeiten wurden verschiedene Experten aus dem Bereich Krisenmanagement und Informationssicherheit zur Bildung von SONIA befragt:⁴⁾ Die Rückmeldung der Befragten zu Einsatzspektrum, Aufgaben und Organisation des Stabes wurden in das vorliegende Konzept eingearbeitet.
- Überarbeitung Konzept SONIA und Erarbeitung Konzept MELANI**
4. Erkenntnisse aus INFORMO 2001 führen zur Anpassung des Konzepts SONIA Die Übung INFORMO 2001 der Strategischen Führungsausbildung bestätigte im Juni 2001 wesentliche Elemente des Konzepts für SONIA. Die genaue Ausrichtung und das Training der Führungstätigkeit konnten weiter vorangetrieben und in diesem Konzept integriert werden. Szenarien dienen zur Klärung der Frage, wann SONIA zum Einsatz kommt.
5. Grundlagen für MELANI Unbestritten war die Forderung aus INFORMO 2001, dass innerhalb des Gesamtsystems Information Assurance eine MELANI notwendig ist. Die Grundlagen dazu wurden mit einer Analyse ausländischer Modelle, der Diskussion mit Verwaltungstellen und der Wirtschaft sowie einer Befragung von potentiellen Kunden erarbeitet.⁵⁾
6. Produkte und Prozesse MELANI Aus den Erkenntnissen resultiert ein Konzept MELANI. Dieses umfasst Produkte und Prozesse, die kundengerecht, effektiv und effizient ausgestaltet werden. Daraus ergeben sich Randbedingungen, die eine entsprechende Stelle erfüllen muss.
7. Organisation MELANI Die definierten Anforderungen können organisatorisch verschieden umgesetzt werden. Vorgeschlagen wird innerhalb dieses Konzepts eine mögliche Organisationsvariante für MELANI.
8. Ausblick und Empfehlungen Aufgrund der Erkenntnisse aus der Erarbeitung des vorliegenden Einsatzkonzepts Information Assurance werden weitere wichtige Aspekte der Information Assurance Landschaft Schweiz im Sinne eines Ausblickes aufgenommen. Mögliche Schwerpunkte werden mittels Empfehlungen dargestellt.

4) Der Fragebogen und die Liste der Befragten befindet sich in Anhang A3.

5) Der Fragebogen und die Liste der Befragten befindet sich in Anhang A4 und A5.

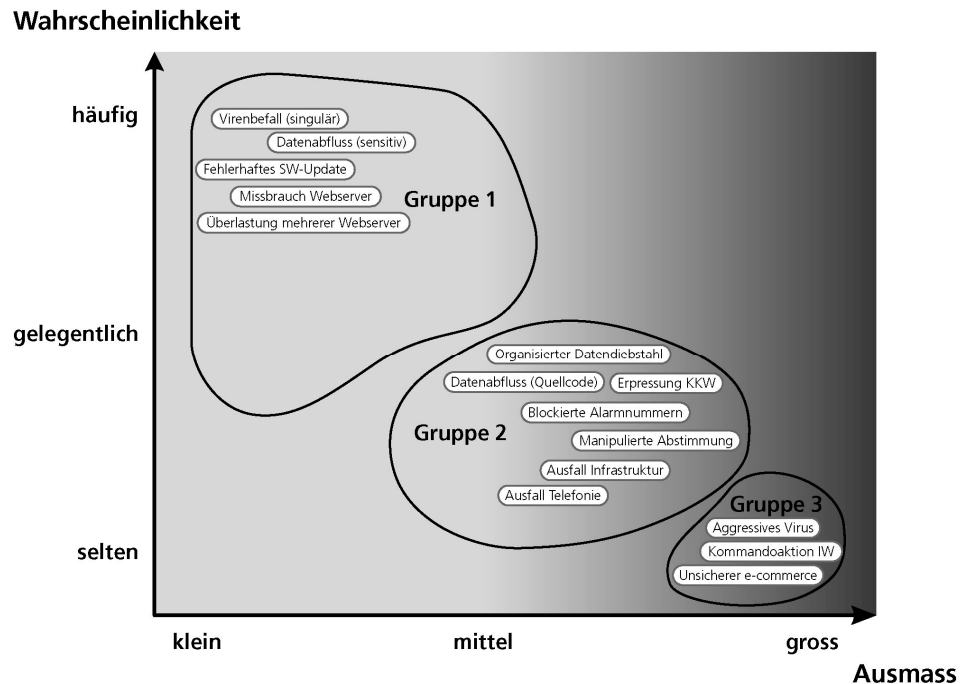
1.3 Situationsanalyse

1.3.1 Gefährdungsanalyse

Zunehmende Bedeutung der Informationsinfrastruktur	Die zunehmende Verflechtung und Bedeutung der Informationsinfrastruktur in der heutigen Gesellschaft führt zu neuartigen Gefährdungen. Im Vergleich zu anderen Gefährdungen wie beispielsweise Naturkatastrophen kann hier jedoch nur beschränkt auf Erfahrungswerte zur Risikoabschätzung zurückgegriffen werden.
Szenarien als Spektrum möglicher Gefährdungen	Aufgrund bisheriger Ereignisse und Überlegungen zu potenziellen Gefährdungen der Informationsinfrastruktur der Schweiz lässt sich ein Satz von stellvertretenden Szenarien generieren, der mögliche Gefährdungen aufzeigt. Dieser kann keinen Anspruch auf Vollständigkeit erheben, soll aber einen Überblick verschaffen und dabei helfen, Einsatz und Abgrenzung von SONIA von weiteren Organisationen (z.B. Stiftung InfoSurance, wirtschaftliche Landesversorgung, Armee) festzulegen.
Auswahl von möglichen Szenarien	Im Folgenden ist eine Auswahl von stellvertretenden Szenarien zusammengestellt, die einen relativ breiten Fächer abdecken. Die Szenarien und die Methodik zur Abschätzung von Wahrscheinlichkeit und Ausmass sind ausführlich in Anhang A1 beschrieben. Für jedes Szenario wurden mit Bezug auf das System Schweiz eine Wahrscheinlichkeit des Eintretens und ein mögliches Schadensausmass abgeschätzt und in der Abbildung 1 aufgetragen. Die Szenarien lassen sich mit Blick auf das Gesamtsystem Schweiz in drei Gruppen einteilen:
Eher unkritische Szenarien (Gruppe 1):	<p><i>Bei diesen Szenarien ist die Verfügbarkeit von einzelnen, unkritischen Systemen eingeschränkt und die Integrität von Daten betroffen.</i></p> <ol style="list-style-type: none"> 1. Virenbefall von PCs in der Verwaltung und Privatwirtschaft 2. Abfluss sensitiver Daten I (persönliche Daten) 3. Fehlerhaftes Software-Update in kritischem Sektor (z.B. Energie) 4. Propagandamissbrauch des Webservers der Bundesverwaltung 5. Überlastung mehrerer Webserver der Privatwirtschaft
Gelegentliche Szenarien mit mittlerem bis grossem Schadensausmass (Gruppe 2):	<p><i>Die Vertraulichkeit von Informationen und Daten sowie die Verfügbarkeit von Systemen von grossem öffentlichen Interesse ist bei diesen Szenarien eingeschränkt. Die kritischen Sektoren sind teilweise nicht verfügbar.</i></p> <ol style="list-style-type: none"> 6. Organisierter und koordinierter Diebstahl von Kreditkarteninformationen 7. Abfluss sensitiver Daten II (Quellcode) 8. Erpressung eines KKW-Betreibers 9. Blockierte Alarmnummern 10. Manipulation bei Abstimmung 11. Ausfall von wichtigen Infrastrukturkomponenten 12. Grossflächiger Ausfall der Telefonie
Seltene Szenarien mit grossem Schadensausmass (Gruppe 3):	<p><i>Bei diesen Szenarien ist die Vertraulichkeit, Integrität und Verfügbarkeit von Daten/Informationen von Systemen von grossem öffentlichen Interesse massiv und länger dauernd eingeschränkt. Vorfälle treten vernetzt auf und führen zu Folgeproblemen.</i></p>

13. Begrenzte Aktionen im Rahmen von Information Warfare
14. Befall mit sehr aggressivem Virus
15. Unsichere Verschlüsselung beim e-Commerce entdeckt

Abbildung 1:
Szenarien zur Gefährdung der
Informationsinfrastruktur



1.3.2 Information Assurance-Landschaft und Krisenstäbe in der Schweiz

Information Assurance-Landschaft in der Schweiz

Organisationen und
Verwaltungseinheiten in der
Schweiz

In der Schweiz beschäftigen sich verschiedene Organisationen und Verwaltungseinheiten mit Aspekten der Informationssicherheit. Die folgende Zusammenstellung zeigt eine Auswahl davon:

CERT SWITCH

Das CERT der SWITCH (Swiss Academic & Research Network) bietet ihren Kunden (Universitäten, Fachhochschulen etc.) Unterstützung, falls Vorfälle im Bereich der Informationssicherheit entdeckt werden. Die Kunden können sich beim CERT-Team melden, das ihre Bedürfnisse dann gegenüber den Internet Service Providern (ISP) vertritt. Dies umfasst beispielsweise die Rückverfolgung von Angriffen auf verschiedenen Netzwerken. Zudem werden Advisories zusammengestellt und öffentlich zugänglich gemacht. Selber erstellt werden diese jedoch nicht. Ebenso wenig ist mit den rund 150 Stellenprozent eine vertiefte Forschungstätigkeit möglich.

Grossunternehmen

In grossen, vor allem internationalen Unternehmungen, bestehen oftmals eigene Notfallorganisationen auch im IT-Bereich. Diese können teilweise auch im Bereich von Gefährdungen der Informationstechnologie eingesetzt

Milizamt „Informations- und Kommunikationsinfrastruktur“	werden. Sie können für eine Organisation wie SONIA sowohl als Frühwarnung (Sensoren) dienen, aber auch als Partner bei der Krisenbewältigung (Einbezug der Privatwirtschaft in SONIA).
	Die wirtschaftliche Landesversorgung hat die Aufgabe, für die Schweiz im Krisenfall die Versorgung mit lebenswichtigen Gütern und Dienstleistungen sicherzustellen. Seit dem 1. Januar 2001 nimmt sich das Milizamt „Informations- und Kommunikationsinfrastruktur“ diesen Aufgaben im Bereich der Informationsinfrastruktur an, um die Handlungsfähigkeit von Verwaltung und Wirtschaft sicherzustellen. ⁶⁾
Stiftung InfoSurance	Die Stiftung InfoSurance schafft seit 2000 in enger Partnerschaft mit privater und öffentlicher Hand die Voraussetzungen, damit moderne Technologien sicher genutzt werden können. Es geht darum, Gefährdungen zu erkennen, Massnahmen zur Prävention zu treffen und ein Forum für die Vertrauensbildung für den Wirtschaftsstandort Schweiz bereitzustellen und ein entsprechendes Kontaktnetz zu fördern. ⁷⁾
Informationssicherheit in der Bundesverwaltung	Innerhalb der Bundesverwaltung beschäftigen sich neben dem Informatikstrategieorgan Bund (ISB) verschiedene Stellen mit Fragen der Informationssicherheit (BIT, KIG, VBS/AIOS u.a.). Diese Organe sind in der Regel nicht alle für den operativen Einsatz im Krisenfall vorgesehen und werden in diesem Bericht nicht weiter diskutiert.
Politische Entscheidungsgremien im Einsatzfall	Der SONIA wirkt im Einsatzfall in beratender Funktion für die politische Führung. Er benötigt daher eine Anbindung an die entsprechenden politischen Entscheidungsgremien. Im Vordergrund stehen dabei der Sicherheitsausschuss des Bundesrates, die Lenkungsgruppe Sicherheit und der Stab Bundesrat.
Sicherheitsausschuss Bundesrat	Der Sicherheitsausschuss des Bundesrates stärkt die sicherheitspolitische Führungstätigkeit des Bundesrates. Er setzt sich aus den Vorstehern des Eidgenössischen Departementes für auswärtige Angelegenheiten, des Eidgenössischen Justiz- und Polizeidepartementes und des Eidgenössischen Departementes für Verteidigung, Bevölkerungsschutz und Sport zusammen.
Stab Bundesrat	Werden in Krisensituationen Entscheide des Gesamtbundesrats notwendig, ermöglicht der Stab Bundesrat der Bundeskanzlei (BK) ein stark gestrafftes Mitberichtsverfahren. In wenigen Stunden kann damit ein Bundesratsbeschluss vorbereitet und zum Entscheid gebracht werden.
Lenkungsgruppe Sicherheit	Die Lenkungsgruppe Sicherheit schafft die Voraussetzungen für eine optimale strategische Führung durch den Bundesrat und befasst sich mit Be-

6) <http://www.bwl.admin.ch>

7) <http://www.infosurance.org>

drohungen der inneren und äusseren Sicherheit. Sie ist als vorbereitendes Stabsorgan des Bundesrates dessen Sicherheitsausschuss unterstellt. Ihre ständigen und nichtständigen Mitglieder vertreten die bedeutenden Aufgabengebiete des Bundes.

Nachrichtendienstliche
Koordinationsstelle

Die nachrichtendienstliche Koordinationsstelle des Bundes koordiniert die Zusammenarbeit der Nachrichtendienste des Bundes und unterstützt den Bundesrat in seiner Führungsarbeit im Sicherheitsbereich. Sie besteht aus dem Nachrichtenkoordinator, dem Lage- und Früherkennungsbüro und einem Sekretariat.

Krisenstäbe in der Schweiz

Vergleich existierender
Krisenstäbe in der Schweiz

Zur Bewältigung von Krisen bestehen in der Schweiz verschiedene Einsatzorganisationen. Drei Beispiele zeigen Einsatzspektren, Organisation und Kompetenzen dieser Stäbe. Der Sonderstab Geiselnahme (SOGE) und die Einsatzorganisation erhöhte Radioaktivität (EOR) sind auf Bundesebene angesiedelt, während Gemeinde- und kantonale Führungsstäbe auf ihrer Stufe führen (vgl. Tabelle 1)

Tabelle 1:
Krisenstäbe in der Schweiz
(Auswahl)

Stab	SOGE	EOR	Gemeindeführungsstab
Charakteristika			
Auftrag und Einsatzspektrum im Alarmfall	Bewältigung erpresserischer Krisensituationen	Schutz der schweiz. Bevölkerung und Lebensgrundlagen bei erhöhter Radioaktivität	Schutz der Gemeindebevölkerung und Lebensgrundlagen in ausserordentlichen Lagen
Gesetzliche Grundlagen	Verordnung über den Sonderstab Geiselnahme und Erpressung (SR 172.213.80)	Verordnung über die Einsatzorganisation bei erhöhter Radioaktivität (VEOR SR 732.32)	Kantonale Grundlagen
Kompetenzen	Lösungsvorschläge an Bundesrat. Sofortmassnahmen ergreifen	NAZ: Sofortmassnahmen und Vorschläge an LAR LAR: Vorschläge BR	Alle Kompetenzen der Gemeindeexekutive für den Krisenfall
Organisation und Aufbau	Ständige Einheit bei der Bundespolizei. Erweitert durch Kernstab	ARMA, NAZ, Stab BR NAZ, LAR	Klassischer Stabsaufbau mit Führung, Unterstützung und Ressorts
Mittel (personell)	Modular (5-20 Personen)	Insgesamt > 200 plus weitere Mittel	Verschieden
Mittel (finanziell)	Budget EJPD	VBS	Gemeindebudget
Mittel (technisch), Infrastruktur	Spezielle Räume	Besondere Anlage	Bestimmte Räume
Aufgebot und Alarmierung	Pikettorganisation BAP (Mittel: Telefon)	Pager, priorisierte Verbindungen, Telefonnetz	Normale Mittel

Zusammenarbeit innerhalb der Schweiz und mit dem Ausland	Verpflichtung zur Zusammenarbeit mit allen Stäben der Kantone resp. des Auslandes	Int. Atomenergiebehörde, kantonale Stäbe und Polizeiorgane	Nachbargemeinden, Kanton
Schulung, Ausbildung, Übungen	Verantwortung bei EJPD	Ausbildung NAZ und drei Ausbildungen pro Jahr für Milizpers. Stab BR NAZ	Training in Führung und Kommunikation. Training der Führungsunterstützung

1.3.3 Ausgewählte ausländische Modelle

Ausgewählte ausländische Melde- und Analysestellen

Lehren aus ausländischen Modellen für die Schweiz

Die Untersuchung von ausgewählten ausländischen Melde- und Analysestellen⁸⁾ haben Elemente aufgezeigt, die für eine schweizerische MELANI übernommen werden können. Die Einbindung dieser Elemente ist jedoch in Zusammenarbeit mit anderen Stellen und primär nach Anforderungen potentieller Kunden noch weiter zu verfeinern. Eine weitergehende systematische Zusammenstellung aller nationalen und internationalen Bemühungen könnte den gegenseitigen Erfahrungsaustausch erleichtern und bei der Umsetzung helfen. Entsprechende Arbeiten wurden bereits angegangen.⁹⁾

Aufgaben

Die wesentlichen Aufgaben der untersuchten Melde- und Analysestellen sind ähnlich und umfassen häufig:

- Prozesskette von der Meldung bis zur Alarmierung:
 - Monitoring von Systemen und Netzen
 - Sammeln, Analysieren und Beurteilen von Meldungen
 - Benachrichten von Kunden und allgemeine Warnungen
- Eine weitere wichtige Aufgabe der Melde- und Analysestellen ist der Informationsaustausch zwischen Regierung und Privatwirtschaft einerseits und zwischen den in- und ausländischen Stellen andererseits.

8) Bericht Melde- und Analysestelle Informationssicherheit, Grobübersicht über ausländische Modelle, Stand: 12.10.2001, Ernst Basler + Partner AG und Anhang A4. Untersucht wurden die folgenden Modelle: Auswerte- und Meldeverbund zum Schutz kritischer Infrastrukturen (Deutschland), NIPC (USA), ISAC (USA), UNIRAS (England), CERT-IST (Frankreich), CanCERT (Kanada), Australian CERT (Australien)

9) ICT In Bits and Pieces on the vulnerability of information-infrastructures, H.A.M. Luijff, M.H.A. Klaver, November 2001, TNO Physics and Electronics Laboratory, P.O. Box 96864, 2509 JG The Hague, The Netherlands. Siehe dort insbesondere Tabelle 3: Overview of relevant (inter)national ICT-security and CIP-activities

- Wichtig ist die Sensibilisierung und Beratung von Firmen und/oder staatlichen Stellen in Bezug auf Sicherheitsvorkehrungen.
- Weitere Aufgaben wie beispielsweise Produkteevaluations, Ausbildung, Sicherheitsprüfungen einzelner Betriebe und Grundlagenforschung sind nur bei gewissen Stellen Teil des Pflichtenhefts.

Produkte Um diese Aufgaben wahrnehmen zu können, werden die folgenden Produkte erarbeitet:

- Netzwerke mit technischen Sensoren und Kontakte zu IT-Betreibern, um Ereignisse frühzeitig festzustellen und den Informationsaustausch sicherzustellen.
- Lagedarstellungen und Statusmeldungen für wichtige Systeme und Netzwerke als Basis für die Lagebeurteilung.
- Warnung, Alarmierung und Empfehlungen bei allfälligen Angriffen oder Angriffsversuchen. Diese gelangen via E-Mail und andere Medien an die Kunden und werden teilweise öffentlich über das Web zugänglich gemacht.
- Publikationen, meist Newsletters, in denen über neue Entwicklungen informiert und über Ereignisse berichtet wird. Als Variante dazu werden teilweise Datenbanken betrieben, über welche die Kunden Informationen beschaffen können. Diese dienen zudem zur statistischen Ereignisauswertung.

Informationsbeschaffung und
-verteilung

Stellen, die ähnliche Aufgabenspektren wie die geplante schweizerische Melde- und Analysestelle haben, weisen die folgenden Modelle der Informationsbeschaffung und -verteilung auf:

- Vorfälle werden entweder über Monitoring von Systemen und Netzwerken, die Auswertung offener Quellen oder über die freiwillige Meldung betroffener Firmen und Regierungsstellen entdeckt. Wichtig ist dabei die Gewährleistung der Vertraulichkeit. Dies betrifft insbesondere die Bereiche, in denen Informationen aus verschiedenen privaten Sektoren zusammenfließen (Anonymisierung). Gewisse Organisationen stellen ihre Produkte auch nur den vertraglich gebundenen Mitgliedern zur Verfügung.
- Die Informationsbeschaffung einiger Melde- und Analysestellen erfolgt in vielen Fällen über die Netzwerke von TF-CSIRT, FIRST und/oder deren regionaler Ableger. Die nationale und internationale Anbindung wird durchwegs als zentrales Element erwähnt. Gute Kontakte müssen auf formeller und informeller Ebene etabliert sein. Vor allem für aktuelle Zwischenfälle und Ereignisse wird oft auf persönliche Kontakte zurückgegriffen.
- Die Zusammenarbeit mit Nachrichtendiensten und Polizeistellen wird gesucht. Probleme tauchen hier bei der Anonymisierung und bei der

Strafverfolgung auf. Solange Vorfälle als Officialdelikte verfolgt werden, scheint eine grosse Zurückhaltung bei Unternehmen vorhanden zu sein, Informationen über Ereignisse herauszugeben.

- Die Zusammenarbeit zwischen staatlichen Stellen und Privatwirtschaft erfolgt meist nicht nur ereignisbezogen, sondern in einem sich etablierenden Prozess, in welchem kritische Infrastrukturen definiert, Gefahren analysiert und Massnahmen diskutiert werden.

Struktur und Organisation

Die Organisationen sind im Kontext der jeweiligen nationalen Bemühungen zur Sicherung der kritischen Infrastrukturen zu betrachten. Oftmals erfolgte eine Anlehnung an Regierungsstellen. Aufgrund der Abhängigkeiten wird unterschiedlich intensiv mit privaten Sektoren zusammengearbeitet, was von einer eher losen Koordination bis zu formalen Absprachen führen kann. Historisch sind die CERTs oftmals an den Hochschulen entstanden, um die dortigen Rechenzentren und Netzwerke zu schützen.

Viele Organisationen verfügen über eine permanente Erreichbarkeit. Zum Teil wird rund um die Uhr gearbeitet, zum Teil stehen Personen ausserhalb der Arbeitszeit auf Abruf zur Verfügung.

In der Regel wird in kleinen Teams (3 bis 5 Personen) gearbeitet. Diese können im Ereignisfall mit weiteren Fachleuten verstärkt werden. Detaillierte Angaben zu Ressourcen in personeller oder finanzieller Hinsicht bestehen kaum.

Drei Beispiele von Einsatzorganisationen Informationssicherheit

Stäbe Informationssicherheit

Verschiedene Organisationen im Ausland beschäftigen sich mit Fragen der Informationssicherheit. Im Vordergrund stehen dabei die sogenannten CERTs (Computer Emergency Response Teams). Die folgende Auswahl beschränkt sich auf solche Stäbe, die während einer Krise eingesetzt werden.

Drei-Säulenmodell in
Deutschland

In Deutschland baut die CERT-Organisation auf einem Verbund von CERTs auf:

- Das CERT des Bundesamts für die Sicherheit der Informationstechnik (BSI) ist primär für die Unterstützung der Behörden zuständig. Im Alarmfall arbeiten rund 7 - 10 Spezialisten aus verschiedenen Behörden an Lösungsvorschlägen.
- Das CERT des Deutschen Forschungsnetzes (DFN) ist für den Bereich Wissenschaft, Forschung und Bildung verantwortlich.
- Das CERT der Wirtschaft resp. Finanz entsteht zur Zeit. Über den Grad der Eigenfinanzierung durch die Wirtschaft resp. staatlicher Beiträge herrscht Uneinigkeit.

Wie sich die notwendige Zusammenarbeit der Gremien einspielen wird, ist noch offen. Eine Kommunikation mit weiteren Lagezentren ist geplant.

National Plan for Information Systems Protection in den USA	Die USA fassten im Jahre 2000 ihre Bemühungen zu „Defending America's Cyberspace“ in einem „National Plan for Information Systems Protection“ zusammen. Die Situationsanalyse weist vor allem auf die Verletzlichkeit der Informationsinfrastruktur und die notwendige Kooperation zwischen Privatwirtschaft und Staat hin.
Dichtes Netz von Zuständigkeiten	Bei der Krisenorganisation ergibt sich ein dichtes Netz von Zuständigkeiten zwischen verschiedensten Behörden aus dem militärischen und zivilen Bereich. Diese haben teilweise einen Schwerpunkt in der Aufklärung und Entdeckung von Ereignissen (FedCIRC, JTF-CNO, NIPC), während Massnahmen von anderen Organen umgesetzt werden (z.B. NSIRC), wobei nicht immer eine scharfe Abgrenzung möglich ist. Für diese meist stehenden Organisationen stehen beachtliche Mittel bereit.
CERT/CC als gemeinsame Melde- und Alarmstelle	Aus Forschung und Wirtschaft ist das CERT/CC entstanden, das als gemeinsame Melde- und Alarmstelle dient und somit Unterstützung auch bei kleineren Vorfällen bietet. Die Zusammenarbeit zwischen Staat und Wirtschaft gestaltet sich schwierig, da erhebliche Unterschiede in der Organisationskultur bestehen.
Sektorübergreifende Koordinationsstelle in Schweden	Im Rahmen der staatlichen Aktivitäten zum Schutz der kritischen Informationsinfrastrukturen setzte die schwedische Regierung im Jahr 2001 eine sektorübergreifende Koordinationsstelle ein, welche die folgenden Aufgaben zu erfüllen hat: Koordination und Sicherstellen der Kooperation im Falle von schwerwiegenden nationalen Informationssicherheitsereignissen. Die Stelle ist in der Verwaltung angesiedelt, setzt sich jedoch aus Vertretern aller Ministerien, Agencies und der Privatwirtschaft zusammen. ¹⁰⁾

1.4 Konsequenzen

Folgerungen für das Konzept	Aus dem Umgang mit Krisen in der Informationsinfrastruktur im Ausland, der Tätigkeit von Krisenstäben im Inland, der Gefährdungsanalyse sowie des politischen Auftrages lassen sich verschiedene Folgerungen ziehen. Insbesondere erweisen sich die folgenden Punkte als zentral:
Privatwirtschaft und öffentliche Hand gemeinsam betroffen	Erste Erfahrungen in den USA sowie aktuelle Diskussionen in Deutschland und der Schweiz zeigen, dass Krisensituationen im Umfeld der Informationssicherheit sowohl die öffentliche Hand als auch die Privatwirtschaft als Ganzes betreffen. Mit der zunehmenden Vernetzung sind die meisten Or-

10) The Swedish Commission on Vulnerability and Security, Vulnerability and Security in a New Era – A Summary, 5S04 2001:41, Stockholm 2001.

ganisationen potentiell Betroffene. Eine Krise lässt sich daher nur im Verbund erfolgreich bewältigen.

- MELANI unabdingbar Die Früherkennung von Verletzungen der Sicherheit in Informationsinfrastrukturen ist prinzipiell schwierig. Einerseits sind die Vorwarnzeiten kurz bis sehr kurz, andererseits lassen sich kaum Schwellenwerte festlegen, wann eine Krisensituation erreicht ist. Zudem kann zur Zeit kaum auf Erfahrungen mit typischen Mustern zurückgegriffen werden. In Deutschland konnten einzig für den Fall von Viren feststehende Kriterien für deren Beurteilung definiert werden. Daraus folgt, dass eine permanente, gut ausgerüstete und stark vernetzte MELANI als Voraussetzung für die laufende Lagebeurteilung unabdingbar ist.
- SONIA: koordinativ und im Verbund Zur Krisenbewältigung und Koordination ist eine rasch verfügbare, kompetente Organisation nötig. Diese muss über entsprechendes Know-how und Kontakte zu den wichtigsten Wirtschaftssektoren verfügen, modular aufgebaut sein und weitere Experten beiziehen können. Solche Organisationsformen haben sich in der Schweiz für vergleichbare Krisenfälle (z.B. SOGE) bewährt. Erfahrungen aus der Einsatzorganisation für erhöhte Radioaktivität zeigen, dass der Vernetzung mit in- und ausländischen Stellen sowohl in der Früherkennung als auch im Einsatzfall eine grosse Bedeutung zukommt.
- Übungen notwendig Eine unbestrittene Tatsache aus Erfahrungen in vielen Bereichen des Krisenmanagements ist, dass für Einsatzorganisationen regelmässige und möglichst realitätsnahe Übungen notwendig sind. Insbesondere Schnittstellen und die Zusammenarbeit mit verschiedensten Partnern können sich als Knackpunkte erweisen.
- Präventionsarbeit unabdingbar Informationssicherheit setzt ein entsprechendes Problembewusstsein und eine politische Verankerung des Themas voraus. Die entsprechenden präventiven Tätigkeiten sind begleitend zu Bemühungen um SONIA fortzusetzen. Darauf zielen sowohl die ausländischen Anstrengungen als auch die Bemühungen der Privatwirtschaft in der Schweiz ab.

2 Melde- und Analysestelle Informationssicherheit

Krisenerkennung schwierig	Das Erkennen möglicher Krisen im Informationsinfrastrukturbereich erweist sich als grosse Herausforderung. Einerseits sind die Vorwarnzeiten kurz bis sehr kurz, andererseits lassen sich schwerlich Grenzwerte festlegen, wann eine Krisensituation erreicht ist. Zudem kann zur Zeit kaum auf Erfahrungen mit typischen Bedrohungslagen zurückgegriffen werden.
Nachrichtendienstliche Informationen	Im Bereich der Informations- und Kommunikationsinfrastruktur geht es weniger um die staatshoheitliche Nachrichtenbeschaffung, als vielmehr um das auf gegenseitigem Vertrauen zwischen Verwaltung und Wirtschaft basierende freiwillige Melden von Vorfällen an eine zentrale Stelle, welche die eingehenden Daten analysiert und zu beidseitigem Nutzen aufarbeitet. Solche Partnerschaften bewährten sich auch im internationalen Kontext bei der Bewältigung eines gemeinsamen Problems im Technologiesektor, nämlich beim Jahr-2000-Wechsel.
MELANI als Voraussetzung für SONIA	Sinn und Zweck von MELANI ist die Früherkennung von Problemen in der Informations- und Kommunikationsinfrastruktur. SONIA ist als nicht permanente Organisation in besonderem Masse auf eine entsprechende Stelle angewiesen. ¹¹⁾

2.1 Kundenbedürfnisse

Umfrage im Herbst 2001	Um die Bedürfnisse und Wünsche von möglichen Kunden und Partnern an eine MELANI zu ermitteln, wurden in der Zeitspanne von Mitte September bis Mitte Oktober 2001 insgesamt 48 Adressaten aus Verwaltung und Privatwirtschaft angeschrieben. Sämtliche relevanten Sektoren waren an der Umfrage beteiligt (Akademie/Forschung, Energie-/Wasserversorgung, Financial Services, Gesundheit, Hochschule, Industrie, Telekommunikation, IT-Security/Consulting, Logistik, Verwaltung, Sonderstab, Vertreter Kantone). Der Rücklauf von 29 Antworten gibt ein differenziertes Bild der Bedürfnisse an die zukünftige MELANI, insbesondere auch deshalb, weil die
------------------------	---

11) Dies war auch eine unbestrittene Forderung aus der Übung INFORMO 2001 (siehe dazu: Auswertungsbericht INFORMO 2001)

Befragten ihre Antworten mehrheitlich mit Kommentaren und Anregungen versehen.¹²⁾

Frage 1: Braucht es nach Ihrer Meinung eine MELANI?

Notwendigkeit bestätigt

Ein überwiegende Mehrheit der Befragten ist der Meinung, dass es eine MELANI braucht. MELANI soll sie mit sicherheitsrelevanten Informationen versorgen und zwar als Ergänzung zu Informationen aus anderen Quellen. Einige Befragte sind der Meinung, dass es MELANI brauche, weil sie noch nicht über diese Informationen verfügen.

	Anz. Nennungen				
	5	10	15	20	25
1 Braucht es MELANI?					
Ja, als Ergänzung zu Infos aus anderen Quellen	█	█	█	█	
Ja, unbedingt	█	█	█		
Ja, da wir noch nicht über solche Infos verfügen	█	█			
Nein, wir sind auf derartige Infos nicht angewiesen					
Nein, wir betreiben selber intern eine analoge Stelle					
Nein, wir beziehen unsere Infos aus anderen Quellen					
weiss nicht					

Frage 2: Welche Produkte/Angebote erwarten Sie von MELANI und in welcher Form?

Produkte und Angebotsformen

Deutlich im Vordergrund des Interesses für die Befragten stehen Warnungen, Lagebeurteilungen und Handlungsempfehlungen, Statusmeldungen sowie Empfehlungen für Sofortmassnahmen zur Schadensverminderung, die MELANI liefern soll. Für die Kommunikation mit MELANI steht für die Befragten die elektronische Form alleine oder in Kombination mit telefonischer und/oder schriftlicher Form im Vordergrund. MELANI soll für die Befragten sowohl «Push-» als auch «Pull-» Kanäle bieten. Für die Befragten ist wichtig, dass sie im Ereignisfall bzw. sofort informiert werden. Eine periodische Information, sei es monatlich, wöchentlich, oder täglich, wird als eher weniger wichtig erachtet. Mehrheitlich werden ausführlichere Meldungen mit Hintergrundinformationen bzw. mit detaillierten Problemlösungen erwartet. Einem Teil der Befragten reicht ein kurze Meldung ohne umfangreiche Erläuterungen.

12) Die ausführliche Auswertung ist nachzulesen in: Melde- und Analysestelle Informationssicherheit, Erhebung von Kundenbedürfnissen, TM 200161-2, 15.10.2001, Informatikstrategieorgan Bund und Ernst Basler + Partner AG.

	5	10	15	20	25
2 Welche Produkte soll MELANI liefern?					
2.1 Welcher Inhalt?					
Warnungen					
Lagebeurteilungen + Handlungsempfehlungen					
Statusmeldungen					
Empf. von Sofortmassn. zur Schadensverhütung					
Empf. von Massn. zur Vorsorge + Schadensverhütung					
Publikationen					
Produkte-Evaluation + Empfehlungen					
Individuelle Beratung bei Vorfällen					
andere					
Hilfestellungen technischer Art					
weiss nicht					
2.2 In welcher Form?					
elektronisch					
Kombination					
telefonisch					
schriftlich (Papierform)					
2.3 «Push» oder «Pull»?					
MELANI soll beide Möglichkeiten bieten					
Ich will die Informationen direkt von MELANI erhalten					
Ich will die Informationen bei MELANI abholen können					
2.4 Wie häufig?					
nur im Ereignisfall					
sofort					
monatlich					
wöchentlich					
täglich					
anders					
weiss nicht					
2.5 Mit welchem Umfang?					
Meldung mit weiteren Hintergrundinformationen					
kurze Meldung umfangreiche Erläuterungen					
Meldung mit Beschr. zur Problembeh. + Hinweisen					
mehr					
weiss nicht					

Frage 3: Welche Informationen würden Sie MELANI liefern?

Bereitschaft zur Meldung von Ereignissen

Im Vordergrund stehen Meldungen zu Hackingattacken und zu Virenbefall. Teilweise würden auch Software-/Hardwarefehler und -ausfälle sowie Netzüberlastungen gemeldet. Kaum mitgeteilt würden Fehlhandlungen durch Mitarbeitende. Als wichtigste Bedingung für das Liefern von Informationen wurde die Anonymisierung genannt. Ein Rolle spielt der mögliche Wettbewerbsnachteil. Ob gelieferte Informationen durch MELANI bezahlt werden sollen, ist hingegen weniger wichtig.

2.3 Produkte

Produkte je nach Situation und Kunden

Durch die Prozesse und Aufgaben lassen sich die Produkte definieren, die durch MELANI erstellt werden. Die folgende Tabelle erläutert die für die einzelnen Kunden notwendigen Produkte. Dabei wird grundsätzlich unterschieden, ob die Produkte im Rahmen der Routineüberwachung oder nur im Ereignisfall erstellt werden. Nur bei kritischen Ereignissen werden Produkte zu Gunsten von SONIA erstellt.

Tabelle 2:
Produkte von MELANI

Produkt		Routineüberwachung	Ereignisfall ohne SONIA	Ereignisfall mit SONIA	Kunden	Kadenz
Warnungen	Sofortige Warnung und Alarmierung bei bedeutenden Vorfällen		X	X	Chef SONIA, Delegierte der kritischen Sektoren	Bei Bedarf
	Informationen bei zeitkritischen und bedeutenden Vorfällen		X	X	Bevölkerung, Wirtschaft, IT-Betreiber in Verwaltung	Bei Bedarf
Statusmeldungen	Statusmeldung zur aktuellen Situation (Netzwerkbelastung, Virenaufkommen, Portscans)	X	X	X	Wirtschaft, SONIA, weitere Interessierte	Fortlaufend (pull)
Lagebeurteilungen	Mittelfristige Trendanalysen	X			Bevölkerung, Wirtschaft, SONIA, Interessierte	Alle 2-3 Monate
	Rückblick, Analyse und Lehren nach Ereignissen		X		Bevölkerung, Wirtschaft, SONIA, Interessierte	Nach Ereignisbewältigung
Varia	Sicherheitshinweise, die nicht zeitkritisch sind		X		Bevölkerung, Wirtschaft, IT-Betreiber in Verwaltung	Bei Bedarf innert Stunden bis Tage
	Individuelle Beratung (Hotline, telefonisch, E-Mail)	X	X	X	Nur innerhalb des Partnernetzwerks	Bei verfügbarer Kapazität und nur für Partner

2.4 Informationsfluss MELANI

Erfolg vom Meldefluss abhängig

Der Erfolg von MELANI wird entscheidend von der Menge und vor allem von der Qualität der eingehenden Meldungen abhängen. Die Bundesverwaltung mit ihrer umfangreichen zivilen und militärischen Informations- und Kommunikationsinfrastruktur gepaart mit der Tatsache, dass staatlich betriebene Infrastrukturen seit jeher eine besondere Anziehung auf Angreifer ausüben, bietet sich in fast idealer Weise als Informationslieferant an. Zu diesem Zweck ist sowohl im zivilen als auch im militärischen Teil der Bundesverwaltung der Aufbau von Intrusion Detection Systemen (IDS) zu prüfen. Die daraus gewonnenen Erkenntnisse, z.B. über versuchte oder erfolgreiche Einbrüche ins Netzwerk, wären an MELANI weiterzuleiten. Ebenfalls zu melden sind Vorfälle mit Computerviren, Würmern, Trojanern ,aber auch Fälle von menschlichem und technischen Versagen, welche die Informationssicherheit der Bundesverwaltung betreffen.¹³⁾

Partnerschaftliches Netzwerk

Wenn man davon ausgeht, dass nicht nur die Informationssicherheit der Verwaltung zur Diskussion steht und man unter Information Assurance in der Schweiz ein Gemeinschaftswerk von Verwaltung und Wirtschaft versteht, dann müsste auch die Privatwirtschaft bereit sein, ihre Beobachtungen an MELANI weiterzuleiten. Neben dem Vertrauen auf die Verschwiegenheit dieser Stelle wird die Bereitschaft der Privaten bei MELANI mitzuarbeiten ganz entscheidend davon abhängen, ob diese auch von den Produkten von MELANI profitieren kann. Gute „Verkaufsargumente“ bilden dabei die Breite des zur Verfügung gestellten Datenmaterials (In- und Ausland).

Breites Sensorennetz notwendig

MELANI benötigt ein breit gefächertes Sensorennetz, um möglichst viele relevante Informationen in möglichst kurzer Zeit sammeln zu können. Dies bedingt, dass Meldungen von verschiedenen Quellen an MELANI gelangen oder von ihr bezogen werden können:

- Meldung aus dem operativen IT-Betrieb von Unternehmungen zu Vorfällen in der Informationsinfrastruktur.
- Meldung aus dem operativen IT-Betrieb der Verwaltung zu Vorfällen in der Informationsinfrastruktur.
- Meldungen und Informationen von wichtigen CERTs resp. Dachorganisationen (FIRST).
- Nachrichtendienstliche Informationen, um gegebenenfalls einen präventiven Einsatz von SONIA auszulösen.

13) Einen vergleichbaren Weg beschreitet übrigens auch die US-amerikanische Verwaltung, die den zivilen Teil ihres „Intrusion Detection Systems“ mit FIDNet (Federal Intrusion Detection Network) und dem entsprechenden militärischen Zweig mit JTF-CND (Joint Task Force-Computer Network Defense) bezeichnet. Die weitere Verarbeitung der Ergebnisse aus FIDNet und JTF-CND ist allerdings ziemlich umständlich und dürfte sich in der Praxis wohl nicht bewähren.


- Meldungen durch Einzelpersonen oder Einzelfirmen in standardisierter und strukturierter Form (z.B. elektronisches Formular)

Sensorenmodell Eine detaillierte Übersicht über die verschiedenen Sensoren gibt das folgende Sensorenmodell. Neben einer Auswahl von Sensoren zeigt das Modell auch die Bedeutung der Sensoren für die einzelnen Produkte. Schliesslich enthält es Hinweise auf den Rhythmus der Informationsbeschaffung und auf den Informationsfluss.

Abbildung 2:
Sensorenmodell MELANI

Sensorenmodell MELANI

Sensor/Quelle	Beispiel	Produkte von MELANI				Info-Beschaffung	Infofluss Richtung
		Warnungen <small>Viren; Attacken; SW-Lücken</small>	Status-meldungen <small>Netzwerk-Monitoring</small>	Lage-beurteilung <small>politische und technische Trends; Risikoanalysen; Forensics</small>	Varia <small>Hotline; Sicherheitshinweise; Beratung (in zweiter Priorität)</small>		
Überregionale CERTs	FIRST, CERT-CC, EWS					laufend	→
Nationale CERTs	CanCert, AusCERT, UNIRAS					laufend	→
Schweiz. CERTs	SwitCh, BERN					laufend	→
Antwiren-SW Hersteller	McAfee, Symantec, ...					laufend	→
OS-, SW-Hersteller	MS, Sun, CA, ...					laufend	→
IT-Betriebe der Sektoren	UBS, CS, ATEL, ...					laufend	→
IT-Betrieb Bünd	ISB, BIT, AIOS, ...					laufend	→
IT-Betrieb Kantone						laufend	→
ISP-Verbände	CIRCA (Ostereich)					laufend	→
ISP International	Worldcom, Tiscali, ...					laufend/tägl.	→
ISP Schweiz	bluewin, green, ...					laufend/tägl.	→
Telekom-Anbieter Internat.	ntl, ...					laufend/tägl.	→
Telekom-Anbieter Schweiz	Swisscom, ...					laufend/tägl.	→
Vernichtungsstellen CH	EDA, EDJ, BK, ...					tägl./wöch.	→
Nachrichtendienste CH	vbs, BAP, ...					tägl./wöch.	→
Verwaltungsstellen Intl.	NIPC, ...					tägl./wöch.	→
Forschung/Universitäten	Infosurance, JAAC, ...					wöch./monatl.	→
«NGOs» CH	CSI, EPIC, ...					wöch./monatl.	→
«NGOs» Intl.						wöch./monatl.	→
IT Sec Unternehmen	SICTA, Swiss ICT, FG Sec, ...					wöch./monatl.	→
Verbände	Heise, ZDNet, AP, CNN					tägl./wöch.	→
Medien						tägl./wöch.	→

- Legende
-  = Sensor ist sehr wichtig für Aufgabe
 -  = Sensor ist mässig wichtig für Aufgabe
 -  = Information von Sensor an MELANI
 -  = Information von MELANI an Sensor
 -  = Beidseitiger Informationsfluss

Vertrauen und Anonymisierung

Es ist von grosser Bedeutung, dass den einzelnen Firmen, die direkte Konkurrenten sein können, durch solche Meldungen keinerlei Wettbewerbsnachteile entstehen dürfen. Zum Schutz ihrer Identität sind daher die Meldungen durch MELANI zu anonymisieren. MELANI muss neutral sein und sowohl in der Verwaltung als auch in der Wirtschaft als verlässlicher Partner anerkannt sein. Ganz allgemein wird es nötig sein, sich über die Klassifizierung von Daten Gedanken zu machen. MELANI muss in dieser Beziehung eine von allen beteiligten Parteien akzeptierbare Politik verfolgen. Dies wird insbesondere für Daten aus den nachrichtendienstlichen Quellen relevant werden.

2.5 Funktionen und Verantwortlichkeiten

Fünf Funktionen

Aufgrund des vorgeschlagenen Aufgaben- und Produktespektrums lassen sich im wesentlichen fünf Funktionen umschreiben. Sie werden im Folgenden diskutiert. In Klammern wird jeweils die Anzahl Arbeitsplätze angegeben, die mindestens erforderlich sind.

Funktion 1: Analyse und Monitoring (3 permanente Arbeitsplätze, 2 Reserveplätze für erhöhte Belegung im Ereignisfall)

Kernaufgabe Analyse und Informationsbeschaffung

Die eigentliche Kerntätigkeit von MELANI verlangt, dass Spezialisten eine permanente Analyse der Ereignismeldungen und des Zustands von Systemen und Netzwerken durchführen. Informationen müssen nach ihrer Bedeutung und im Kontext beurteilt und weiterverarbeitet werden. Je nach verfügbarer Kapazität können beratende Dienstleistungen zur Verfügung gestellt werden. Im Ereignisfall müssen diese Personen eine zeitgerechte Warnung und Alarmierung und eine kontinuierliche Information von SONIA sicherstellen können.

Technische und strategische Beurteilungen

Diese Funktion, die rund um die Uhr zu besetzen ist, kann schwergewichtig der technischen Analyse von Ereignissen und des Netzwerkstatus oder aber der strategischen Analyse zugeordnet werden. Das entsprechende Wissen und die Ausbildung muss bei der Besetzung berücksichtigt werden. Um die Attraktivität der Arbeitsplätze hoch zu halten, sind Rotationen vorzusehen, so dass sich Routineüberwachungsaufgaben, Weiterbildung, aktive Recherchen und Aussenkontakte mit Beratung abwechseln.

Funktion 2: Datenbank/Lagedarstellung (3 Arbeitsplätze)

Arbeitshilfsmittel bereitstellen MELANI wird mit grossen Informationsmengen umgehen müssen. Dementsprechend sind ihr die notwendigen Arbeitsinstrumente zur Verfügung zu stellen. Eine Ereignisdatenbank, ein Wissensmanagement-System und eine graphische Lagedarstellung dienen nicht nur der eigenen Tätigkeit, sondern unterstützen die Aufarbeitung der Grundlagen für die Öffentlichkeitsarbeit und SONIA in der Arbeit.

Keine permanente Präsenz gefordert Für die Konzeption und den Unterhalt dieser Instrumente sind Stellen bereitzustellen, die keine permanente Präsenz erfordern. Die Arbeitszeit beschränkt sich auf gewöhnliche Bürozeiten mit der Vorgabe, im Ereignisfall unterstützend mitzuwirken.

Funktion 3: Kontakte/Informationsplattform (4 Arbeitsplätze)

Anspruchsvolle Kontaktpflege Der Erfolg von MELANI hängt von einem erfolgreichen Informationsfluss ab. Dem Aufbau und der kontinuierlichen Pflege von formellen und informellen Kontakten zu den Sensoren, Partnern und Kunden stellt hohe Anforderungen an die betreffenden Mitarbeiter.

In- und Ausland Eine mögliche Aufteilung ergibt sich aus den Zuständigkeiten für inländische Kontakte und der internationalen Zusammenarbeit. Diese Stellen erfordern keine permanente Präsenz und Erreichbarkeit.

Funktion 4: Öffentlichkeitsarbeit (4 Arbeitsplätze)

Breite Produktpalette, verschiedene Kanäle Die definierten Produkte, das Marketing für die eigene Stelle und für den Gesamtprozess Information Assurance verlangt kontinuierliche Öffentlichkeitsarbeit. Von der Bereitstellung von Informationen und Rückblick auf Ereignisse bis zum Jahresbericht sind verschiedene Produkte zu erstellen. Dabei sind alle heute gängigen Informationskanäle zu berücksichtigen.

Keine Pikettfunktion Diese Funktion kann im Rahmen einer normalen Anstellung ohne Pikettfunktion abgedeckt werden.

Funktion 5: Führung/Administration (4 Arbeitsplätze)

Anspruchsvolle Führung rund um die Uhr Die Führung von MELANI im Routine- wie auch im Ereignisbetrieb stellt hohe Anforderungen. Sie umfasst alle klassischen Führungsaufgaben bis hin zum Ereignismanagement. Die Führungsperson resp. ihre Stellvertretung muss das ganze Jahr über rund um die Uhr erreichbar sein und hat sehr eng mit der Führung von SONIA zusammenzuarbeiten. Denkbar ist auch eine gegenseitige Stellverteter-Regelung zwischen MELANI und SONIA.

Administration SONIA und
MELANI

Administrative Arbeiten für MELANI, aber auch für SONIA, werden ebenfalls im Rahmen dieser Funktion erledigt.

2.6 Organisationsmodell

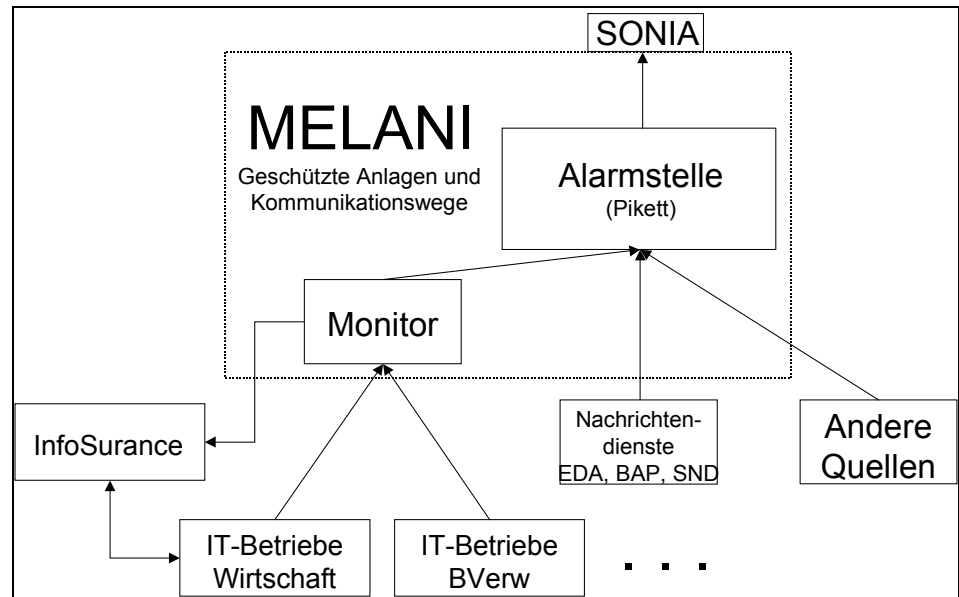
Rahmenbedingungen Die Anforderungen an die Organisation von MELANI ergibt sich aus den definierten Prozessen, Aufgaben und Produkten. Um die geforderte Leistung zu erbringen, müssen die folgenden Rahmenbedingungen berücksichtigt werden:

Geschützte Anlage Die Forderung nach geschützten Anlagen und Kommunikationswegen mag im ersten Moment erstaunen, wenn man bedenkt, dass man es selbst bei dem von US-amerikanischen Experten an die Wand gemalten Schreckgespenst des „Electronic Pearl Harbor“ oder dem vom früheren CIA-Chef John Deutch prognostizierten „Cyber War“ nicht mit Angriffen zu tun hat, bei welchen die physische Zerstörung von Einrichtungen im Vordergrund steht. Bedenkt man jedoch die zentrale Rolle, die MELANI für die Informationssicherheit in der Schweiz und speziell auch für SONIA spielt – sie ist sowohl das Instrument zur Erkennung der Krise als auch der zentrale Informationslieferant während seines Einsatzes – und stellt man diese den verhältnismässig einfachen Mitteln gegenüber, die es erlauben, die ICT-Infrastruktur in einem ungeschützten Gebäude zu zerstören, so wird der Schutzbedarf rasch klar.

Zentrale Anlage Hinzu kommt, dass der Wert von MELANI ganz entscheidend von der Anzahl (und Qualität) der Quellen abhängt. Die Koordination der Bemühungen mit verschiedenen Partnern muss ein starkes zentrales Element aufweisen. Je mehr Informationen zur Verfügung stehen, desto einfacher lässt sich die Situation überblicken und in einen grösseren Zusammenhang stellen. Unter anderem deshalb, aber auch aus rein ökonomischen Gründen, sollte in der Schweiz der Aufbau einer einzigen solchen Anlage ins Auge gefasst werden, die auch den andern Organisationen im Rahmen des Konzepts „Information Assurance“ (z.B. den IO/IW) sowie der Wirtschaft zur Verfügung steht.

Die Abbildung 3 zeigt einen möglichen organisatorischen Aufbau von MELANI:

Abbildung 3:
Organisationsmodell MELANI



Informationsfluss

Auf der untersten Ebene stehen die IT-Betriebe der Wirtschaft respektive der Bundesverwaltung, welche Informationen (z.B. erfolgreiche oder versuchte Einbruchversuche ins Netzwerk, Datendiebstähle, Virenvorfälle u.a.) an den Monitor melden. Die Punkte rechts vom Kasten „IT-Betriebe Bundesverwaltung“ deuten an, dass sich die Liste der Informationslieferanten beliebig erweitern lässt. Der Monitor bewertet die eingehenden Meldungen, triagiert diese und meldet diejenigen von besonderer Brisanz an die Alarmstelle, an die ebenfalls Informationen aus verschiedenen nachrichtendienstlichen und anderen Quellen zusammenlaufen. Je nach der Beschaffenheit der Daten und der noch notwendigen Aufarbeitung respektive Verifizierung lassen sich weitere Quellen entweder am Monitor oder direkt an der Alarmstelle aufhängen.

Pikettfunktion zur Warnung und Alarmierung von SONIA

Schliesslich entscheidet ein Pikett, das neben einem guten ICT-Sachverständnis vor allem ein „Gefühl“ für das Eskalationspotential einer Lage sowie für die Abhängigkeiten der verschiedenen kritischen Sektoren hat, über die Aufbietung des Stabschefs, der dann (allenfalls nach Rücksprache mit verschiedenen Stabsmitgliedern) über die Einberufung von SONIA entscheidet.

Kontakt mit bestehenden Organisationen

Der Monitor lässt seine Erkenntnisse entweder direkt oder über eine Organisation wie InfoSurance der Wirtschaft zukommen. Während die verschiedenen Nachrichtendienste (EDA, BAP, SND) bereits existieren, müsste der Monitor neu aufgebaut werden. Die dazu einzusetzenden personellen Mittel hängen neben seinen Aufgaben stark von der Art und Menge des zu sichtenden Datenmaterials ab. Eine gute Koordination und Absprache mit den Nachrichtendiensten ist daher zu prüfen.

2.7 Kostenschätzung

Geschätzte Mittel für MELANI	Um die geforderten Leistungen zu erbringen, sind die notwendigen personellen, betrieblichen und finanziellen Mittel bereitzustellen.
Zeitliche Lastverteilung	Erfahrungen über die zeitliche Verteilung von Routineüberwachung und Ereignismanagement fehlen weitgehend. Es ist davon auszugehen, dass die überwiegende Anzahl von Fällen Kleinereignisse sind, die weder zum Aufgebot von SONIA noch zu speziellen Aktionen von MELANI führen. In einer ersten Näherung wird angenommen, dass 90% der Zeit der Routineüberwachung, 8% speziellen Aktionen von MELANI und nur 2% den Situationen mit Einsatz SONIA zugerechnet werden.
Annahmen und Rahmenbedingungen	<p>Die Abschätzungen beruhen auf den im Folgenden formulierten Annahmen. Sämtliche Angaben sind jährliche Kosten in Schweizerfranken (CHF).</p> <ul style="list-style-type: none"> • Grundsätzlich wird davon ausgegangen, dass die Stellen von Profis im Vollamt besetzt werden. Bei Stellen, die eine Präsenz rund um die Uhr erfordern, ist die Anzahl Arbeitsplätze mit dem Faktor 4.5 multipliziert, um die Anzahl Stellen zu ermitteln. Dies deckt den Dienst in drei Schichten rund um die Uhr, an den Wochenenden und während Ferien, Krankheit und Militärdienst ab. Bei den Arbeitsplätzen für die Analyse (Funktion 1) wurden zwei Reserveplätze eingerechnet. • Für eine volle Stelle (100%) wird von CHF 200'000.- pro Jahr ausgegangen. • Für MELANI werden bereits bestehende geschützte Anlagen genutzt. Es werden keine neuen baulichen Infrastrukturen und Verbindungen erstellt. Für die Bereitstellung der geschützten Infrastruktur wird ein Betrag von CHF 10'000.- pro Arbeitsplatz eingesetzt. • Für den Normalfall werden zusätzlich normale Büroräumlichkeiten gemietet. Die Kosten werden mit CHF 400.- pro m² angesetzt. Pro Arbeitsplatz wird mit 10 m² gerechnet. • Für die zentrale Informatik wird von neuartigen Softwareprodukten und hochverfügbarer sicherer Infrastruktur ausgegangen, welche auf rund 4 Jahre abgeschrieben wird. Pro Jahr ergibt dies CHF 1'000'000.- Franken. • Für die Informatik-Infrastruktur pro Arbeitsplatz wird zusätzlich von rund CHF 10'000.- pro Jahr ausgegangen. • Um Kosten für Verbrauchsmaterial, Unterhalt und Reparaturen zu decken, werden weitere CHF 10'000.- pro Jahr reserviert. • In der Zusammenstellung sind lediglich ausgabenwirksame Kosten aufgeführt.

Abbildung 4:
Kostenschätzung MELANI

Funktion	Analyse/ Monitoring	Datenbank/ Lagedarstell.	Kontakte/ Infoplattform	Öffentlichkeits- arbeit	Führung/ Administration
Anzahl Arbeitsplätze	5	3	4	2	4
Anzahl Planstellen	13.5	3	4	2	4
Kosten					
Personal	2'700'000	600'000	800'000	400'000	800'000
Geschützte Arbeitsplätze	50'000	30'000	40'000	20'000	40'000
Ungeschützte Arbeitsplätze	20'000	12'000	16'000	8'000	16'000
IT-Mittel zentral	1'000'000				
IT-Mittel Arbeitsplatz	50'000	30'000	40'000	20'000	40'000
Material, Unterhalt, Reparaturen	50'000	30'000	40'000	20'000	40'000
Kosten pro Jahr	3'870'000	702'000	936'000	468'000	936'000
Gesamtkosten pro Jahr	6'912'000				

Jährliche Gesamtkosten von rund
CHF 7 Mio

Aufgrund der oben ausgeführten Annahmen ist von jährlichen Gesamtkosten von rund CHF 7 Mio auszugehen.

3 Sonderstab Information Assurance

Auftrag des Sonderstabs
Informationssicherheit

Der Sonderstab Information Assurance (SONIA) soll zur Beratung bei der Bewältigung von Krisen ausgelöst durch Störungen in der Informationsinfrastruktur (KASII) eingesetzt werden. Eine KASII liegt dann vor, wenn die ordentlichen Strukturen und Verfahren in einzelnen Verwaltungseinheiten oder in Unternehmungen insbesondere im Bereich der lebenswichtigen Sektoren, wie beispielsweise die Energie- oder Wasserversorgung, die Telekommunikation, der öffentliche Verkehr oder das Gesundheitswesen, überfordert sind. Die KASII kann sowohl durch menschliche Fehler, technische Defekte als auch durch vorsätzliche Handlungen ausgelöst werden.

Partnerschaft zwischen
Privatwirtschaft und öffentlicher
Hand

Für SONIA ist einer engen Partnerschaft zwischen privatem und öffentlichem Sektor Rechnung zu tragen. Dazu sind organisatorische und infrastrukturseitige Voraussetzungen zu schaffen, damit die mit der zunehmenden Abhängigkeit von Informationstechnologien verbundenen Gefahren und Risiken für die Schweiz erkannt und geeignete Massnahmen zur Prävention respektive Schadensminderung getroffen werden können. Grundsätzlich ist eine gegenseitige Information bei Vorfällen von grosser Bedeutung. Die Bestrebungen des Bundes sollten Vorbildcharakter haben, von denen Unternehmen profitieren können.

3.1 Aufgaben vor und nach der Krise

SONIA ist nicht permanent
operativ

SONIA ist keine stehende Organisation und somit nur nach einem Aufgebot operativ. Verschiedene Aufgaben müssen im Umfeld von SONIA vor und nach einer Krise wahrgenommen werden. Im Einzelnen sind dies:

Vor der Krise: Vorbereitende
Massnahmen

1. Im Bereich der vorsorglichen Massnahmen zur Führung in der Krise gilt es vor allem die Infrastruktur und Führungsunterstützung zu benennen und bereitzustellen. Zudem können für mögliche Einsatzfälle Einsatzdokumentationen erstellt werden. Die Alarmierung und Kommunikation muss in enger Zusammenarbeit mit MELANI vorbereitet werden.
2. Um die Einsatzbereitschaft sicherzustellen, muss der SONIA beübt werden. Neben Alarmübungen sollen auch reale Übungen durchgeführt werden. Dabei gemachte Erfahrungen sollen als Basis für fortlaufende Anpassungen dienen.¹⁴⁾

14) Erfahrungen mit einem Ausbildungsverbund konnten an INFORMO 2001 gemacht werden (SFA, Stiftung InfoSurance, BAKOM, WL, VBS).

Nach der Krise: Rück- und
Ausblick

3. Ein aktiver Entscheid zum Abschluss der Phase „in der Krise“ soll getroffen und kommuniziert werden. Damit kann die Rückführung in den Normalzustand beginnen.
4. SONIA soll sowohl die Krise wie auch die Führung in der Krise rückblickend kritisch betrachten und evaluieren. Die entsprechenden Erkenntnisse sind in Auswertungsberichten festzuhalten und als „lessons learned“ im Sinne der Weiterentwicklung der Stabsarbeit und des Wissensmanagements zu berücksichtigen.

Allgemeine Prävention nicht
Aufgabe von SONIA

Allgemeine vorsorgliche Massnahmen zur Krisenprävention (Sensibilisieren, Information in der normalen Lage etc.) fallen nicht in den Aufgabenbereich von SONIA. Diese sind von entsprechend qualifizierten Stellen durchzuführen.

3.2 Aufgaben in der Krise

Grundlage

Der Auftrag an SONIA stützt sich auf die Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung vom 23. Februar 2000 (BinfV) und auf den Bundesratsbeschluss zum Konzept „Information Assurance“ vom 22. Juni 2000. Nach geltendem Organisationsrecht des RVOG, auf welchem sich auch die BinfV abstützt, haben Stabsorganisationen vorbereitende Funktionen. Dazu gehören Lagebeurteilungen, die Erarbeitung von Lösungsvorschlägen zu Handen des Bundesrats sowie die interne Koordination. Unter zusätzlicher Berücksichtigung des Leitgedankens eines partnerschaftlichen Verbundes zwischen Verwaltung und Wirtschaft, lassen sich die folgenden Aufgaben für SONIA formulieren.

Vier Aufgaben

1. Er berät den Bundesrat im Falle schwerwiegender Ereignisse im Bereich der Informationssicherheit und stellt diesem sowohl Entscheidungsgrundlagen als auch Lösungsvorschläge zur Verfügung.
2. Er beurteilt laufend die Lage zum Krisenverlauf und kommuniziert diese situationsgerecht an interessierte Stellen. Er stellt der Bundeskanzlei die Grundlagen für die Information der Bevölkerung zur Verfügung.
3. Er kann im Sinne der operativen Krisenbewältigung für die Bundesverwaltung Massnahmen in Absprache mit den für die Informationssicherheit zuständigen Stellen anordnen.
4. Er koordiniert die Anstrengungen der Wirtschaft (kritische Sektoren), der Bundesverwaltung sowie der Kantone und Gemeinden zur Überwindung der Krise durch Bereitstellen einer gemeinsamen Plattform.

Die einzelnen Aufgaben werden im Folgenden weiter ausgeführt:

3.2.1 Beratendes Organ für den Bundesrat

Beratungsbedarf des Bundesrats	Die Erfahrung aus verschiedenen Krisensituationen zeigt, dass relativ rasch der Ruf nach politischer Führung oder zumindest nach Stellungnahmen durch die Regierung ertönt. SONIA soll somit die Rolle des Beratungsorgans des Bundesrats für Krisen ausgelöst durch Störungen in der Informationsinfrastruktur übernehmen.
Aufgabe gemäss Art. 55 RVOG und Konzept Information Assurance	Diese Aufgaben entsprechen auch Sinn und Zweck von Stabsorganen wie sie in Artikel 55 des RVOG festgesetzt sind. Zudem wurden diese Aufgaben bereits im Konzept „Information Assurance“ der KIG vorgeschlagen und durch eine Mehrheit der Teilnehmer an der Übung INFORMO 2001 gefordert.

3.2.2 Information

Vertrauensverlust vermeiden	Krisen können bei unsachgemässer und ungeschickter Informationspolitik rasch zu einem erheblichen und irreparablen Vertrauensverlust in die betroffenen kritischen Sektoren oder Verwaltungseinheit führen. SONIA muss diesem Thema grösste Bedeutung beimessen, da Glaubwürdigkeit der Verwaltung und letztlich auch das Vertrauen in die Zuverlässigkeit der schweizerischen Informationsinfrastruktur auf dem Spiel steht. Daher sind die Mitteilungen von SONIA durch die Kommunikations- und IT-Fachspezialisten gemeinsam zu verfassen und auf die Bedürfnisse des Zielpublikums abzustimmen.
Wege der Information	Für die Information von Bevölkerung, Wirtschaft und Medien in Lagen, in denen SONIA oder noch weitere Mittel eingesetzt werden, ist auf Bundesstufe die Informationszentrale der Bundeskanzlei zuständig. SONIA stellt dabei als Partner die fachlichen Grundlagen zur aktuellen Situation zur Verfügung.
Art der Information	Die Informationen dürfen sich nicht auf Einzelereignisse fokussieren, sondern müssen die gesamte Lage vermitteln. Es ist zu prüfen, wieweit Einzelereignisse (Systemzusammenbrüche, Hackerangriffe etc.) in anonymisierter Form zu kommunizieren sind.
Rhythmus und Kanäle	Im Falle einer Krise ist von einem hohen Erwartungsdruck der Öffentlichkeit und Medien auszugehen. Dementsprechend ist eine häufige, verständliche und korrekte Information von grosser Wichtigkeit. Dabei ist auch neueren Trends im Medienkonsum Rechnung zu tragen. Als Rückfallebene sind immer auch gesicherte Kanäle bereitzustellen, da nicht mehr vom Funkzionieren aller Medien ausgegangen werden kann. Die Medien können selbst als Sektor von Ausfällen der Informationsinfrastrukturen betroffen sein.

Schwergewicht der
Informationen

Bei den Informationen für die Bevölkerung ist das Schwergewicht auf mögliche Massnahmen des Einzelnen oder eines Betriebs zu legen (Einspielen von Patches) und solche, die zur nötigen Klärung der Situation beitragen (Information, unter welchen Konstellationen ein Virus zuschlagen kann und wie die Systeme geschützt werden können). Damit sollen auch falsche Reaktionen verhindert werden. Für die Wirtschaft und deren Verbände werden zudem die Hintergründe von Bedeutung sein, um daraus Lehren zu ziehen und die eigene Strategie festlegen zu können.

3.2.3 Massnahmen in der Bundesverwaltung

Krisenbewältigung in der
Bundesverwaltung

Die Bundesverwaltung kann bei Störungen in der Informations- und Kommunikationsinfrastruktur ebenfalls betroffen sein. Von SONIA wird erwartet, dass er nicht nur gegen aussen kommuniziert und koordiniert, sondern auch die interne Krisenbewältigung unterstützt. Krisenbewältigung ist jedoch typischerweise eine operative Aufgabe, die von den Entscheidungsträgern operativer Einheiten auf Direktionsstufe wahrgenommen werden muss.

Operative Krisenbewältigung
„Kraft ihres Amtes“

Bei der Besetzung von SONIA mit Mitgliedern aus der Bundesverwaltung ist deshalb darauf zu achten, dass diese die Umsetzung der beschlossenen Massnahmen „Kraft ihres Amtes“ verfügen können. Dies erhöht nicht nur die Akzeptanz der getroffenen Entscheide, sondern macht auch den Erlass einer weiteren Verordnung zur Festlegung der Kompetenzen der Stabsmitglieder unnötig. Im Sinne der Doktrin konzentrierter Arbeitsstrukturen und Straffung der Abläufe, sind diesen Entscheidungsträgern Fachspezialisten aus der Bundesverwaltung beizuordnen. Diese können aus dem Informatikstrategieorgan sowie aus den entsprechenden Verwaltungseinheiten, z.B. dem BIT, rekrutiert werden. In einzelnen Departementen könnte es vorteilhaft sein, die entsprechenden ISBDs ebenfalls aufzubieten oder fallweise beizuziehen. Sicherergestellt werden muss zudem die Abstimmung der Massnahmen mit dem Ausschuss Informationssicherheit der Bundesverwaltung.¹⁵⁾

3.2.4 Koordination von Privatwirtschaft und Verwaltung

Mitwirken aller Partner
notwendig

Das Mitwirken der Privatwirtschaft bei SONIA beruht auf der Einsicht, dass wegen der Vernetzung der verschiedenen kritischen Sektoren untereinander und dieser mit der Bundesverwaltung ein staatlicher Alleingang weder zweckmässig noch möglich ist. Auf die Möglichkeit des Bezugs „geeigneter Stellen ausserhalb der Bundesverwaltung“ wird denn auch explizit in der rechtlichen Grundlage für SONIA (BinfV, Art. 7 Abs. 3) hingewiesen. Durch diese Zusammensetzung soll eine rasche Koordination aller Betroffenen möglich sein. Die Zusammensetzung drängt sich ebenfalls auf, dass die

15) Bezüglich Aufgaben und Tätigkeiten: siehe auch BinfV und BinfW

Entscheidungsfindung sowie deren Umsetzung operativer Massnahmen zu den einzelnen IT-Betreibern gehört, wo das spezifische (Fach)wissen vorhanden ist. Ebenso ist der Bund in IT-Fragen nicht alleine sachverständig.

SONIA als Informationsdrehscheibe

SONIA beschränkt sich in seiner Arbeit primär auf die Lagebeurteilung, auf Grund welcher die einzelnen Wirtschaftssektoren selbstständig Massnahmen veranlassen können. Informationen über bevorstehende und bereits erfolgte Massnahmen sowie über deren Erfolg respektive Misserfolg werden zwischen den Sektoren via SONIA ausgetauscht, worauf die Massnahmen angepasst und verfeinert werden können. SONIA versteht sich somit als Lagezentrum und Informationsdrehscheibe in der Krise. Hier könnte die Organisation MILLENNIUM TRANSIT als Beispiel genannt werden.

Lösung nur im Verbund möglich

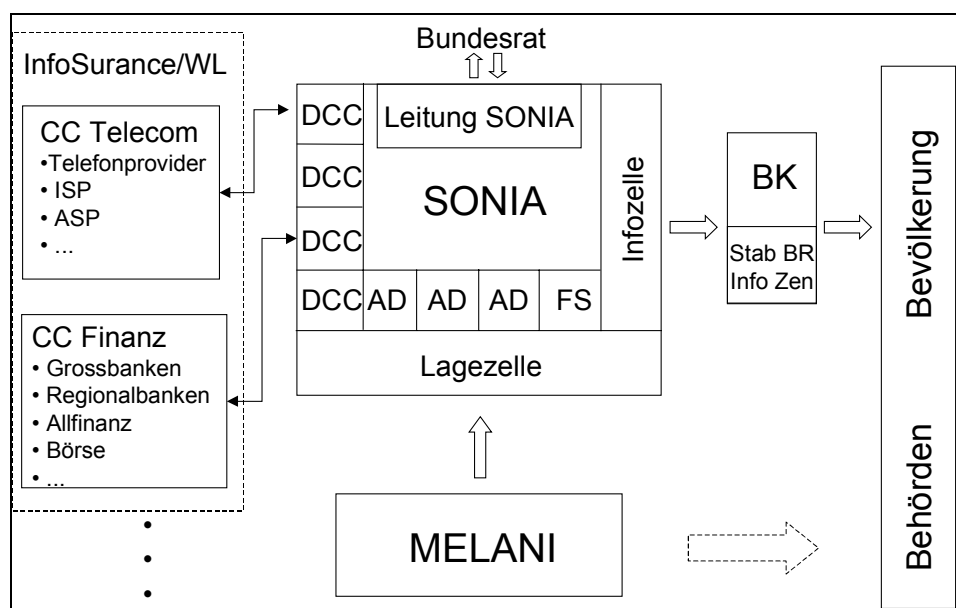
Das dazu notwendige Wissen zur Krisenbewältigung bei Störungen in der Informations- und Kommunikationsinfrastruktur kann kaum an einer einzigen Stelle wie SONIA vereinigt werden; ganz zu schweigen von der immensen Vielfalt an operativen Aufgaben, die sich in so einem Umfeld ergeben. Die Lösung dieser Probleme muss in der Vernetzung von kleineren, wohl definierten Einheiten mit eigenen Befugnissen und Kompetenzen bestehen.

3.3 Organisationsmodell

3.3.1 Grundsätze

Die Organisation von SONIA richtet sich nach seinen Aufgaben. Es wird das folgende Modell vorgeschlagen:

Abbildung 5: Organisationsmodell SONIA



MELANI mit unveränderten Aufgaben im Ereignisfall	MELANI soll ihre Aufgaben – vor allem im Bereich der Nachrichtenbeschaffung und Auswertung – auch in der Krise weiterführen, was der Doktrin der unveränderten Arbeitsabläufe beim Übergang von der Normal- zur Krisensituation entspricht. Im Einsatzfall von SONIA ist eine Erhöhung der Kadenz der Lagebeurteilungen denkbar. Dies sollte durch geeignete personelle Massnahmen (z.B. Ausschöpfung von Überkapazitäten, längeren Dienstzeiten, Streichung von Ferientagen) relativ kurzfristig sichergestellt werden können.
Schnittstelle MELANI und SONIA	Die Schnittstelle zwischen MELANI und SONIA ist seine Lagezelle („Lageoffizier“), welche die Informationen entgegennimmt und in eine auf die Bedürfnisse von SONIA zugeschnittene Form bringt. Die Lageinformation wird durch Nachrichten aus den Sektoren, die über die Delegierten der Coordination Centers (DCC) und die Amtsdirektoren (AD) eintreffen, kontinuierlich ergänzt. Erfahrungen aus der Operation MILLENNIUM TRANSIT sowie aus INFORMO 2001 haben gezeigt, dass eine einzelne Person mit diesen Aufgaben rasch überfordert ist, so dass die Lagezelle mit einer angemessenen Anzahl von Leuten (drei oder mehr) zu besetzen sein wird.
Infozelle in Zusammenarbeit mit der Bundeskanzlei	Die Infozelle arbeitet eng mit der Lagezelle zusammen und erstellt situationgerechte an den jeweiligen Verteiler (Bundesrat, Behörden, Bundeskanzlei) angepasste Mitteilungen. Durch Absprache mit den Stabsmitgliedern stellt die Infozelle sicher, dass keine widersprüchlichen Signale ausgesendet werden. Dies ist besonders wichtig, wenn die Nachrichten für die Bevölkerung bestimmt sind, damit keine unnötigen Ängste geschürt werden. Als weitere vertrauensfördernde Massnahme wird die Information der Bevölkerung durch die Bundeskanzlei vorgenommen. Die Kommunikation mit dem Bundesrat (z.B. das Stellen der Anträge sowie die Entgegennahme von Aufträgen) soll durch den Delegierten für die Informatikstrategie des Bundes (in seiner Funktion als Chef SONIA) wahrgenommen werden.
Stabsmitglieder aus der Bundesverwaltung	Die mit AD (Amtsdirektoren) und FS (Fachspezialisten) bezeichneten Kästchen bilden den Block der Stabsmitglieder aus der Bundesverwaltung, die für die Krisenbewältigung innerhalb der Bundesverwaltung zuständig sind. Ebenfalls vorzusehen ist eine Verbindungsperson zum Milizamt ICT-I sowie zu den Information Operations der Armee.
Koordination mit der Wirtschaft	Die mit DCC bezeichneten Kästchen stehen für die Delegierten der Coordination Centers. Sie stellen die passive Koordination der Massnahmen der Wirtschaft und der Bundesverwaltung sicher. Die entsprechenden Coordination Centers (CCs) sind jeweils für jeden der kritischen Sektoren unter Mitarbeit von InfoSurance und der Wirtschaftlichen Landesversorgung separat aufzubauen. In ihnen sollen die „Key Players“ der Sektoren – also z.B. Swisscom, Sunrise und Orange und Internet Service Provider im Bereich Telekommunikation – aber auch andere interessierte Unternehmungen

Einsatz nehmen. Pro CC sind zwei Delegierte zu bestimmen, die in SONIA als Verbindungspersonen („Verbindungsoffiziere“) zwischen CC und SONIA mitarbeiten. Sie sollen sowohl über vertiefte Kenntnisse ihres Sektors als auch der jeweiligen IT-Infrastruktur verfügen. Auf die gleiche Art wie die CCs mit ihren DCCs in SONIA in Kontakt stehen, sollen diese auch mit ihren IT-Spezialisten und dem Management ihrer Unternehmungen Informationen über die Geschehnisse austauschen. Dadurch wird sichergestellt, dass sich auch die eigentlichen Entscheidungsträger in der Wirtschaft rasch und effizient ein Bild von der Situation machen können.

Die Coordination Centers (CC) Die CCs bilden die Informationsdreh scheiben zwischen SONIA und den einzelnen Firmen. Sie können sich so konstituieren wie es für den jeweiligen Sektor angemessen scheint; dabei ist es sinnvoll, bereits vorhandene Strukturen (z.B. firmeneigene IT-Sicherheitsabteilungen, ehemalige Y2K-Organisationen usw.) miteinzubeziehen und untereinander zu vernetzen. Somit können die CCs mit relativ einfachen Mitteln aufgebaut werden und je nach Bedürfnis wachsen oder allenfalls weitere Aufgaben im Umfeld der Information Assurance wahrnehmen.

Aufbau der CC Ein möglicher Startpunkt für den Aufbau der CC wäre eine Datenbank, durch welche die Mitglieder auf sichere (vertrauliche und authentifizierte) Art Informationen und Erfahrungen miteinander austauschen können. Denn im Fall einer Krise ist es wichtig, dass ein Konsens herrscht, wie Lagen zu beschreiben und Ereignisse zu melden sind (Incident Reporting). Nur so wird kohärentes und rasches Handeln überhaupt erst möglich. Deshalb sollte diese „unité de pensée“ bis hinauf zu SONIA durchgängig vorhanden sein.¹⁶⁾

3.3.2 Funktionen und Verantwortlichkeiten

Die Grundsätze der Zusammensetzung von SONIA wurden bereits im Kapitel 3.3.1 beschrieben. Für die einzelnen Funktionen ergeben sich die folgenden Charakterisierungen:

Leitung SONIA Der Leiter von SONIA entscheidet über die Einberufung von SONIA. Er übernimmt die operative Leitung von SONIA. Die Leitung wird durch den Delegierten des ISB resp. Stellvertreter wahrgenommen. Es gelten zudem die folgenden organisatorischen Anforderungen an die Leitung SONIA:

- Die permanente Erreichbarkeit muss sichergestellt sein.
- Die Stellvertreter (pool) müssen mit voller Entscheidungskompetenz ausgestattet werden.

16) Die entsprechenden Aufgaben wurden aufgenommen. Konkrete Erkenntnisse über Aufgaben und Strukturen der CC liegen noch nicht vor. Entsprechend sind sie auch nicht Bestandteil des Berichts.

Mitglieder SONIA	SONIA ist bewusst klein, um flexibel und schnell agieren zu können. Es ist eine Stellvertreter-Regelung zu bestimmen. Die Personen müssen kurzfristig verfügbar sein. SONIA besteht neben der Leitung, der Info- und Lagezellen aus Amtsdirektoren, Fachspezialisten und den Delegierten der Coordination Centers.
Zusätzliche Experten	SONIA kann bei Bedarf auf weitere Experten zurückgreifen. Wünschbar ist der Einbezug von Fachleuten aus den folgenden Bereichen: <ul style="list-style-type: none"> • Verwaltung (Datenschutz, Rechtsfragen, Cybercrime) • IT-Fachspezialisten, insbesondere Informationssicherheit • Information und Kommunikation
Geschäftsstelle	Zur Unterstützung von SONIA ist eine Geschäftsstelle notwendig. Sie ist im Organisationsschema nicht aufgezeichnet, da die entsprechenden Arbeiten durch die Administration von MELANI übernommen werden. Es sind dies: <ul style="list-style-type: none"> • Administrativen Aufgaben SONIA (z.B. Rufnummern, Erreichbarkeit, Stellvertreter etc.). • Ansprechpartner für alle Fragen im Zusammenhang mit SONIA. • Ausbildung <p>Die Geschäftsstelle selber besitzt im Ereignisfall keine Aufgaben und ist somit kein zeitkritisches Element.</p>

3.3.3 Führung und Einsatz

Elemente des Führungssystems	Für die Organisation von SONIA sind bisherige Erfahrungen aus der Führungslehre zu beachten. Dabei erweisen sich drei Elemente für ein erfolgreiches Führungssystem als zentral: <ul style="list-style-type: none"> • Die innere Organisation des Führungselementes muss klar bestimmt sein (Führungsorganisation). • Die Führungstätigkeit basiert auf dem systematischen Prozess der Entscheidungsfindung. Sie wird unterteilt in Einsatzplanung und Einsatzführung (Führungsprozesse). • Die Infrastruktur des Stabes, seine Führungsunterstützungs- und Kommunikationselemente sind notwendige Arbeitsgrundlagen des Stabes (Führungseinrichtungen).
Bedingungen für einen erfolgreichen Einsatz	Für den erfolgreichen Einsatz von SONIA sind folgende Punkte zu berücksichtigen: <ul style="list-style-type: none"> • Die permanente Erreichbarkeit muss sichergestellt sein. • Ein schnelles Zusammenkommen resp. schnelle Entscheidungsfindung ist sicherzustellen.

- Ein Minimalbestand von SONIA muss gewährleistet sein (Ferienabwesenheiten etc.).

Umsetzungsphase ermöglicht
Einsatzbereitschaft

Das vorliegende ergänzte Konzept legt die Grundsteine SONIA. Zur Erreichung der operativen Einsatzbereitschaft werden in der Umsetzungsphase im Bereich Führungsprozesse und für die konkrete Gestaltung der Führungseinrichtungen weitere Arbeiten notwendig sein.

3.4 Ausbildung und Training

3.4.1 Grundsätze

Ausbildung und Training
notwendig und
ressourcenintensiv

Um ein Krisenorgan für den Einsatzfall vorzubereiten, sind sowohl eine Grundausbildung als auch ein regelmässiges Training notwendig. Nur eingeübte Abläufe, erprobtes Zusammenspiel und in Übungen getestete Schnittstellen können im Ernstfall wirkungsvoll eingesetzt werden. Dies bedingt jedoch einen beachtlichen Aufwand zur Vorbereitung und Durchführung seitens aller Beteiligten.

Vom Einfachen zum
Komplizierten

Für SONIA stehen in einer ersten Phase das Einspielen von grundlegenden Tätigkeiten (Lagebeurteilung, Formulierung von Massnahmen, Kommunikation gegen aussen, Führungsrhythmus) im Vordergrund. Nach und nach können weitere Partner und Elemente in die Ausbildung und umfassendere Übungen einbezogen werden und so die Funktion im Verbund getestet werden.

3.4.2 Rhythmus

Ein bis zwei regelmässige und
ein bis zwei Alarmübungen pro
Jahr

Damit die Mitglieder von SONIA eine gewisse Vertrautheit und Sicherheit in ihren Funktionen erlangen, sind im Minimum ein bis zwei reguläre Übungen pro Jahr in Vollbesetzung einzuplanen. Um das Verhalten im Alarmfall beurteilen zu können und auch Faktoren wie „unsichere Erreichbarkeit“, „unvollständige Besetzung von SONIA“ und „unvorbereitetes Handeln“ aufgreifen zu können, sind zusätzlich ein bis zwei Alarmübungen einzuplanen. Dabei ist jeweils auch MELANI einzubeziehen. Mit dieser Kadenz kann den Entwicklungen im Bereich der Informationsinfrastruktur gefolgt werden.

3.4.3 Inhalte

Es lassen sich zwei Varianten für die Ausbildung und Trainings unterscheiden:

Lernen durch Auswertung -
Crisis Management

Vorfälle aus dem In- und Ausland eignen sich hervorragend, um Lehren im Bereich Früherkennung, aber auch Krisenbewältigung zu gewinnen. Neben technischen und organisatorischen Aspekten, die zu verbessern sind, sollten die ganz kritischen Punkte im Ablauf einer Krise analysiert werden: Wer fällt wann und unter welchen Umständen wesentliche Entscheide, die für den weiteren Verlauf prägend waren? Gibt es Schlüsselfaktoren, die in einer zukünftigen Krise erkannt werden müssten? Und wie lassen sich die Erkenntnisse umsetzen? Diese Fragen können innerhalb von SONIA diskutiert resp. als Grundlage für Übungsszenarien verwendet werden. Möglicherweise sollten die Analysearbeiten jedoch vorgängig erfolgen, damit eine fundierte Diskussionsbasis bereitsteht.

Spezifische Stabstätigkeit

Die eigentliche Stabstätigkeit und die Kernaufgaben von SONIA müssen soweit eingeübt sein, dass sie routinemässig ablaufen können. Es sind dies insbesondere:

- Führungsrhythmus und Stabsorganisation inkl. Kommunikation und Schnittstellen mit Partnern.
- Informationsbeschaffung und Lagebeurteilung.
- Erarbeiten von Massnahmenvorschlägen zu Handen Bundesrat.
- Erarbeiten von Massnahmen und Umsetzung in Weisungen für die Bundesverwaltung.
- Koordination mit Privatwirtschaft und weiteren Behörden.
- Information (inhaltlich, aber auch in Bezug auf Mittel und Umsetzung) der Bevölkerung, Wirtschaft und Medien.

3.4.4 Organisation

Interne Übungen

SONIA ist selbst verantwortlich für die Ausbildung seiner Mitglieder. Solange der Schwerpunkt der Übungen auf der eigenen Stabstätigkeit liegt, soll die Ausbildung durch die Leitung SONIA erfolgen. Dieser kennt die Abläufe und Zielsetzungen resp. SOLL-Vorgaben am besten und kann gezielt auf Schwachpunkte eingehen.

Externe Übungsleitung

Um den Einsatz im Verbund mit allen Partnern und an wirklichkeitsnahen Szenarien zu üben, ist eine externe Übungsleitung vorteilhaft.

3.5 Kostenschätzung

Mittel folgen den definierten
Aufgaben

Zur Aufgabenerfüllung sind für SONIA die notwendigen finanziellen Mittel zur Verfügung zu stellen.

Annahmen und
Rahmenbedingungen

Die Abschätzungen beruhen auf den im Folgenden formulierten Annahmen. Sämtliche Angaben sind jährliche Kosten in Schweizerfranken (CHF).

- Für SONIA werden bereits bestehende geschützte Anlagen genutzt. Es werden keine neuen baulichen Infrastrukturen und Verbindungen erstellt. Für die Bereitstellung der geschützten Infrastruktur wird ein Betrag von CHF 10'000.- pro Arbeitsplatz eingesetzt.
- SONIA basiert weitgehend auf den von MELANI genutzten Informatikmitteln zur Erstellung seiner Produkte. Es werden lediglich weitere Arbeitsplätze zur Verfügung gestellt. Die dazu notwendigen Investitionen werden in jährliche Kosten umgelegt. Pro Arbeitsplatz werden dafür CHF 10'000.- berechnet.
- Es wird von 20 Stabsmitgliedern ausgegangen. Die Entschädigung erfolgt gemäss Organisationsverordnung Landesversorgung.
- Die Aufgaben der Geschäftsstelle von SONIA werden bei MELANI integriert. Die entsprechenden Kosten werden im Kapitel 2.7 ausgewiesen.
- Unterstützungspersonal für SONIA (Betrieb der Anlage, Betrieb der Kommunikationsinfrastruktur, Führungsunterstützung, Logistik, Verpflegung) wird in der Kostenrechnung nicht berücksichtigt.
- Für die Berechnung werden 2 Einsatz- und 2 Übungstage angenommen.
- In der Zusammenstellung sind lediglich ausgabenwirksame Kosten aufgeführt.
- Für die Alarmierung und das Aufgebot der Stabsmitglieder sowie die Kommunikation zwischen SONIA und MELANI wird auf eine bestehende Kommunikationsinfrastruktur zurückgegriffen.

Damit ergeben sich die folgenden jährlichen Kosten für SONIA:

Tabelle 3:
Kostenschätzung SONIA

Position	Annahme	jährliche Kosten [Fr.]
Bereitstellen von 20 geschützten Arbeitsplätzen	„Miete“ von geschützten, permanent verfügbaren Einsatzräumlichkeiten	200'000.-
Betreiben der 20 zusätzlich benötigten Arbeitsplätze	IT-Infrastruktur, Unterhalt des Alarmierungssystems	200'000.-
Kontaktpflege zu ähnlichen Stäben im In- und Ausland sowie zu MELANI	Reisen, Besichtigung, Informationen	50'000.-
Zweitägige Ausbildungssequenz	inkl. Vorbereitung und Auswertung	100'000.-
Zusätzliche Kosten für einen zweitägigen Einsatz	Unterkunft, Verpflegung, Verbrauchmaterial	50'000.-
Total pro Jahr		600'000.-

Genauere Schätzung nach Festlegung der Organisation

Die vorangehenden Kostenschätzungen basieren auf den dargestellten Annahmen. Bei einer veränderten Organisationsstruktur in der Umsetzungsphase kann sich dieser Finanzbedarf noch ändern.

4 Verbundsystem

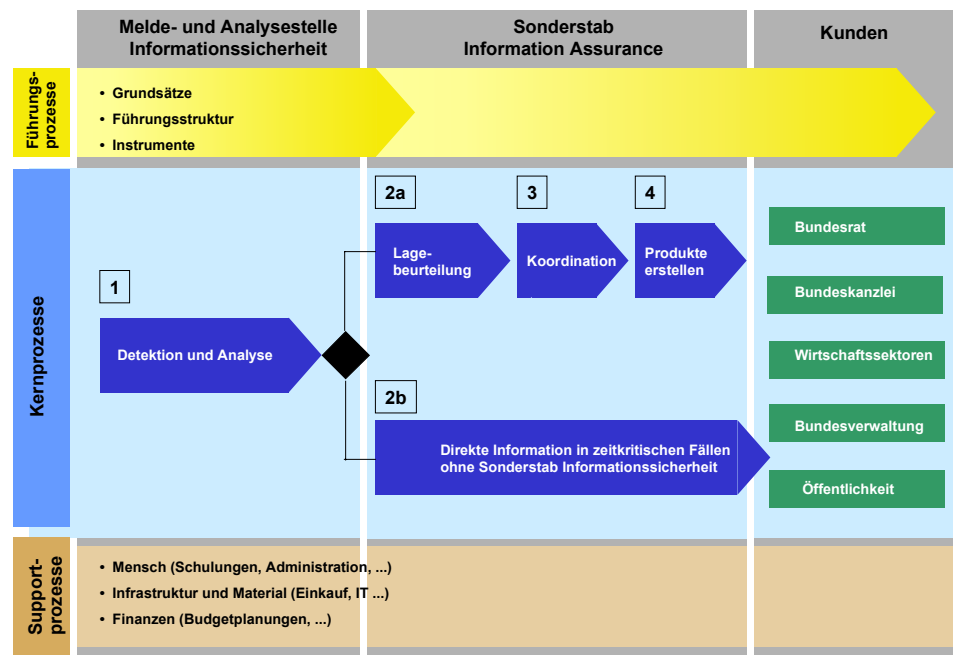
4.1 Zusammenarbeit

Vier Kernelemente Das folgende Kapitel zeigt ein mögliches Modell der Zusammenarbeit im Verbund auf. Das dargestellte Prozessmodell geht von vier Kernelementen aus:

- Informations- und Koordinationsstellen in den kritischen Infrastrukturen (Coordination Centers). Dieses Element wird zur Zeit durch die Stiftung InfoSurance, die wirtschaftliche Landesversorgung, das Informatikstrategieorgan Bund zusammen mit Wirtschaftsvertretern entwickelt und ist nicht Teil des vorliegenden Berichts.
- Die permanente Melde- und Analysestelle Informationssicherheit (MELANI).
- Der Sonderstab Information Assurance (SONIA), der bei umfassenden Ereignissen zum Einsatz kommt.
- Die Kunden von MELANI und SONIA.

Das Zusammenspiel dieser Partner wird im folgenden Prozessmodell Informationssicherheit in einer Übersicht skizziert. Neben den dargestellten Kernprozessen sind weitere Prozesse bei der konkreten Umsetzung zu definieren. Die Coordination Centers sind nicht eingezeichnet.

Abbildung 6:
Prozessmodell
Informationssicherheit



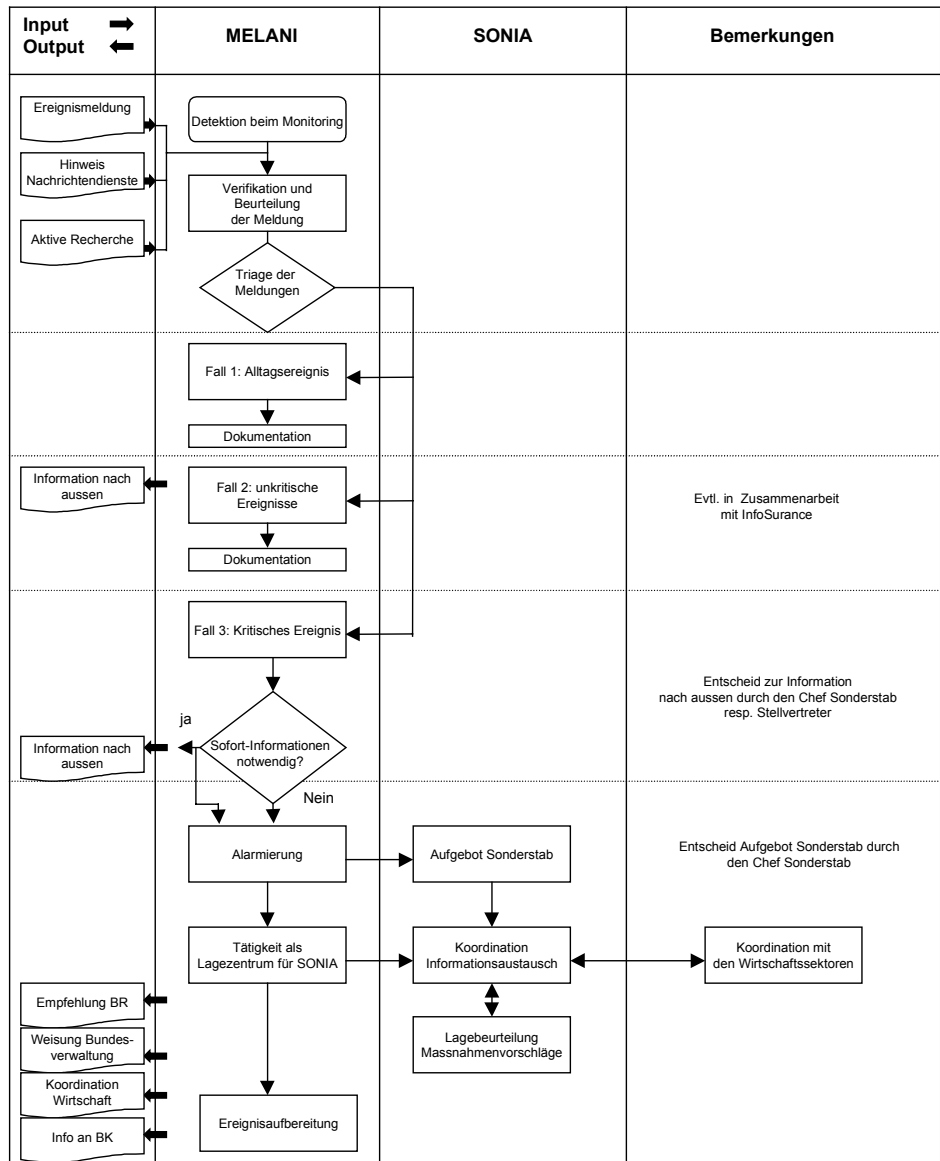
-
- Kernprozesse Grundsätzlich können vier Kernprozesse des Gesamtsystems unterschieden werden. Die aufgeführten Nummern verweisen auf das Prozessmodell in Abbildung 6:
1. Die Detektion und Analyse von Ereignissen erfolgt durch MELANI, die in ein Netz von Sensoren eingebunden sein muss. Die Informationen von IT-Betreibern und nachrichtendienstliche Informationen müssen verifiziert, zu einer Lagedarstellung aufbereitet und beurteilt werden [1].
 2. Ergibt die Lagebeurteilung eine für das Gesamtsystem kritische Situation, ist SONIA anzubieten und in den Prozess einzubinden [2a]. Ansonsten werden die Informationen lediglich systematisch aufbereitet, publiziert und fliessen in die allgemeine Lageanalyse ein [2b].
 3. Der Absprache und Zusammenarbeit mit den Wirtschaftssektoren durch Coordination Centers, aber auch mit den Kantonen und dem Ausland fällt eine grosse Bedeutung zu. Die Problemlösung erfolgt durch SONIA im Verbund von Wirtschaft und Staat [3].
 4. Als letzter Prozessschritt erfolgt das Erstellen der Produkte für die verschiedenen Kunden: Beratungsleistungen für die strategische Führung, Erteilen von Weisungen für die Bundesverwaltung, Grundlagen für die Information der Öffentlichkeit [4].
- Führungsprozesse Neben den Kernprozessen helfen die Führungsprozesse mit, die entsprechenden Rollen wahrzunehmen und Entscheide zu kommunizieren. Der Führungsprozess umfasst die folgenden Elemente:
- Führungsgrundsätze
 - Führungsstruktur
 - Führungsinstrumente
- Supportprozesse Um die Funktion des Gesamtsystems aufrechtzuerhalten sind die folgenden Aspekte für den Supportprozess beachten:
- Menschen (Schulung, Administration, ...)
 - Infrastruktur und Material (Einkauf, Unterhalt, ..)
 - Finanzen (Ressourcenbereitstellung, ...)

Ein detailliertes Bild eines möglichen Prozessablaufs gibt die Abbildung 7. Die Triage unterscheidet dabei drei Fälle, die sich an der Darstellung aus Kapitel 1.3 orientieren.

- Fall 1 „Alltagsereignis“ : Ereignisse dieser Kategorie führen zu keiner Gefährdung der Informations- und Kommunikationsinfrastrukturen. Sie lösen deshalb keine Massnahmen von MELANI nach aussen auf und werden zu Dokumentationszwecken abgelegt. SONIA wird nicht aufgegeben.
- Fall 2 „Unkritische Ereignisse“ : Diese Ereignisse können Beeinträchtigungen bei einzelnen Systemen oder Netzen auslösen. Ganze Sektoren sind in ihrer Funktion jedoch nicht gefährdet. Die Information wird allen wichtigen Partnern von MELANI zur Verfügung gestellt. SONIA wird nicht aufgegeben.
- Fall 3 „Kritische Ereignisse“ : Unter diese Kategorie fallen Ereignisse mit grossem Schadenpotential und Gefährdung der kritischen Infrastrukturen. Sie können zu einem Aufgebot von SONIA führen. Bei Bedarf kann MELANI nach Absprache mit dem Chef SONIA als Sofortmassnahme Informationen nach aussen bereitstellen.

Abbildung 7:
Prozessbeschreibung bei
Ereignissen Information
Assurance

Prozessbeschreibung bei Ereignissen Information Assurance



Die Zuweisung der einzelnen Prozesse, der resultierenden Produkte und Aufgaben erfolgt in den entsprechenden Kapiteln zu SONIA und MELANI.

4.2 Kunden und Partner

Kunden des Gesamtprozesses
Information Assurance

Der Gesamtprozess Information Assurance betrifft verschiedene Kunden mit unterschiedlichem Bedarf an Produkten:

Unkritische Situation

In unkritischen Situationen kann MELANI ohne Aufgebot von SONIA und in Zusammenarbeit mit weiteren Organisationen der Informationssicherheit

ein breites Publikum von Wirtschaft, Verwaltung und Öffentlichkeit informieren.

Kritische Situation Bedingt die Situation sofortige Massnahmen, kann MELANI die Kunden in einer ersten Phase direkt informieren. Beim Aufgebot von SONIA sind die entsprechenden Produkte durch SONIA bereitzustellen und via Bundeskanzlei zu kommunizieren.

Die folgende Liste charakterisiert die einzelnen Kunden des Gesamtsystems Information Assurance:

Tabelle 4:
Kunden und Produkte des
Gesamtsystems Information
Assurance

Kunde	Produkt	Bemerkung
Bundesrat	Strategische Beratung	
Wirtschaftssektoren, kantonale Verwaltungen	Lageinformation, Absprachen, Informationsaustausch	Sind gleichzeitig auch Sensoren
IT-Betreiber in der Bundesverwaltung	Weisungen	Sind gleichzeitig auch Sensoren
Bundeskanzlei	Grundlagen für die Information der Öffentlichkeit	
Öffentlichkeit	Informationen	In Zusammenarbeit mit InfoSurance

Zusammenarbeit mit anderen
Organisationen notwendig

Neben den Partnern im dargestellten Verbundsystem arbeitet sowohl MELANI als auch SONIA eng mit anderen Organen zusammen. Stellen, die als Sensoren dienen, sind entsprechend gekennzeichnet. Die wichtigsten Partner und die Beschreibung der Zusammenarbeit sind in der folgenden Tabelle aufgeführt:

Tabelle 5:
Weitere Organe

Organ	Beschreibung der Zusammenarbeit
Milizamt BWL (Bereich INI)	<ul style="list-style-type: none"> Aufbau der Coordination Centers und damit möglicher Partner im Bereich der Früherkennung und Alarmierung Gegenseitige Information
Stiftung InfoSurance	<ul style="list-style-type: none"> Präventionstätigkeit der Stiftung Gegenseitige Information Informationskanal bei unkritischen Ereignissen
Nationale Alarmzentrale NAZ	<ul style="list-style-type: none"> Möglicher Partner im Bereich der Alarmierung
Nachrichtendienste	<ul style="list-style-type: none"> Möglicher Partner im Bereich der Früherkennung und Analyse
Universitäten und Fachhochschulen	<ul style="list-style-type: none"> Möglicher Partner im Bereich der Früherkennung und Analyse
Informatikstrategieorgan Bund (ISB)	<ul style="list-style-type: none"> Ist auch in der Leitung SONIA vertreten

Organ	Beschreibung der Zusammenarbeit
Informatiksicherheitsbeauftragte der Departemente (ISBD)	<ul style="list-style-type: none"> Gegenseitige Information
Bundesamt für Kommunikation (BAKOM)	<ul style="list-style-type: none"> Gegenseitige Information
Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS)	<ul style="list-style-type: none"> Gegenseitige Information Sind in SONIA (Verwaltung; Koordination VBS) vertreten Enger Kontakt zu AIOS
Bundesamt für Polizeiwesen (BAP)	<ul style="list-style-type: none"> Gegenseitige Information Enge Zusammenarbeit, falls die KASII in den Bereich der BAP fällt (vorsätzliche Handlung, kriminelle Aktivität, etc.)
Botschaften im Ausland	<ul style="list-style-type: none"> Dienen als Sensoren für die Situation im Ausland
Grossfirmen aus der Wirtschaft	<ul style="list-style-type: none"> Dienen als ständige Sensoren Bilden die Coordination Centers der kritischen Sektoren Gegenseitige Information
Kantone	<ul style="list-style-type: none"> Koordination der Massnahmen Austausch von Informationen
Internationale und nationale ausländische CERTs und Melde- und Analysestellen	<ul style="list-style-type: none"> Informationsaustausch Institutionalisierte und informelle Zusammenarbeit
Fachverbände Informatiksicherheit in der Schweiz	<ul style="list-style-type: none"> Gegenseitige Information

4.3 Einsatzkriterien für SONIA

4.3.1 Einleitung

Grundsätzliche Kriterien

Die Frage, in welchen Situationen SONIA eingesetzt werden soll, lässt sich zur Zeit nicht abschliessend klären. Die folgenden Punkte fassen das vorgeschlagene Einsatzspektrum von SONIA im Falle einer Krise in der Informationsinfrastruktur auf einer allgemeinen Ebene zusammen:

- Die Verfügbarkeit von Systemen der öffentlichen Hand ist in mehreren Bundesämtern/Departementen im grösseren Masse durch Vorfälle eingeschränkt und die Vertraulichkeit von Daten nicht mehr gewährleistet.
- Kritische Sektoren sind elektronisch nicht erreichbar und Leistungen nicht mehr verfügbar, wobei die Probleme nicht auf ein einzelnes technisch bekanntes und definiertes Vorkommnis zurückzuführen sind (unklare Ursachen und unbekannte Täter).
- Die Integrität von kritischen Informationen kann gefährdet sein.
- Eine gemeinsame Lösung muss effektiver und effizienter sein als die Einzellösung.

- In verschiedenen Organisationen treten gleichzeitig ähnliche Ereignisse auf. Dies gilt auch für Vorfälle im Ausland, die ein Potential für Auswirkungen in der Schweiz haben (Aussenpolitik).
- Es besteht ein bedeutendes öffentliches und/oder mediales Interesse.
- Die aktuelle Lage deutet darauf hin, dass sehr rasch (in Stunden) ein oder mehrere der obigen Punkte erfüllt sein werden.

Präventiver Einsatz möglich

Im Weiteren sind präventive Einsätze denkbar, schon bevor es zu Aktivitäten resp. Vorfällen kommt. Ist aufgrund „nachrichtendienstlicher“ Tätigkeiten und beim Bekanntwerden von massiven Sicherheitslöchern mit aktiven Angriffen oder Zwischenfällen zu rechnen, kann SONIA vorsorgliche verwaltungsinterne Massnahmen veranlassen oder Abklärungen vornehmen.

Entscheidungshilfe für MELANI

In der Praxis wird eine konkrete Entscheidungshilfe für MELANI notwendig sein. Die folgenden Ausführungen sollen eine erste Orientierung ermöglichen.¹⁷⁾

4.3.2 Aspekte zur Beurteilung eines Einsatzes von SONIA

Instrument für MELANI

Die simultane Beurteilung der Ereignisse wird im Normalfall durch MELANI sichergestellt. Daher soll MELANI über ein Instrument verfügen, mit welchem auf die Ereignisse bezogen eine strukturierte Entscheidung über die Einberufung von SONIA herbeigeführt werden kann.

Drei Aspekte

Es werden drei Aspekte zum Entscheid über den Einsatz von MELANI berücksichtigt:

- Ursache- / Themenabgrenzung
- Wirkung
- Eskalationspotential

a) Ursachen- / Themenabgrenzung

Folgende Kriterien, bezogen auf die Ursachen der Ereignisse, sollen als Voraussetzung gelten, damit SONIA aktiv wird:

Themen von Ursachen

SONIA kann aktiv werden, wenn die Ursache der Ereignisse in der Informationsinfrastruktur liegt.

Informationsinhalte

Krisen, die durch Informationsinhalte ausgelöst werden und die über die einwandfrei funktionierende Informationsinfrastruktur übertragen werden, befinden sich ausserhalb des Einsatzspektrums von SONIA. Die Situation

17) Die folgenden Ausführungen entstammen dem Bericht „Szenarien für MELANI und SONIA, Informatikstrategieorgan Bund und HTA Luzern, Bern und Horw, 28.11.2001“.

kann dann in den Zuständigkeitsbereich von SONIA fallen, wenn eine Kettenreaktion eines derartigen Ereignisses die Informationsinfrastruktur beeinträchtigt. Je nach Aufgaben- und Kompetenzdefinition kann MELANI die richtigen Stellen zeitgerecht avisieren.

b) Wirkung

Die Analyse der Wirkung eines Ereignisses hinsichtlich verschiedener Kriterien soll ebenfalls helfen, die Problemstellung in kurzer Zeit zu strukturieren und den Entscheid über die Einberufung von SONIA herbeizuführen. Dabei unterscheiden wir die Wirkung in folgende Kriterien:

Abbildung 8:
Wirkung von Ereignissen in
verschiedenen Dimensionen



Anzahl der Betroffenen	Die Ausdehnung eines Ereignisses in der Informationsinfrastruktur kann über die Anzahl der direkt und indirekt betroffenen Personen gemessen werden.
Intensität der Betroffenheit	Die Art der Betroffenheit und deren Intensität in Hinblick auf die Grundbedürfnisse (Maslov'sche Pyramide) der Menschen oder die Grundfunktionen von Sektoren und Branchen können Hinweise auf das mögliche Eskalationspotential des Ereignisses geben. Die Intensität der Betroffenheit wird in dieser Betrachtung auf die Fakten reduziert und nicht auf die individuelle Wahrnehmung.
Wahrnehmungsintensität	Ereignisse im Umfeld von Informationssicherheit werden aus subjektiver Sicht meist indirekt wahrgenommen: Business Prozesse (Funktionen) werden blockiert oder Bedürfnisse können nicht mehr abgedeckt werden. Eine individuelle Analyse der Ereignisse durch die Betroffenen lässt in gewissen Fällen erste Rückschlüsse auf Probleme in der Informationsinfrastruktur zu (z.B. Bankomat).

Die Wahrnehmungsintensität ist sehr oft das Resultat aus der Anzahl der Betroffenen und der Intensität der Betroffenheit. Über diese Faktoren definiert sich das Medieninteresse. Die Medien leisten in der Aufklärungsphase einen grossen Beitrag zur allgemeinen Information, sofern ein lokales, wenn nicht sogar nationales Interesse besteht.

Derartige Informationen verbreiten sich durch die hohe Medienpräsenz im Alltag blitzartig. Je nach Dimension der Berichterstattung wird auch der politische Druck zunehmend grösser.

Eine Falschinformation über ein KKW-Unglück kann in der Bevölkerung grosse Verunsicherung und damit Betroffenheit durch Information auslösen. Menschen werden durch die Medien bewusst oder unbewusst beeinflusst. Die Intensität der Betroffenheit und das Interesse für das Ereignis kann durch eine entsprechende Information verändert werden.

c) Eskalationspotential

Ereignisse können auf folgende zwei Arten eskalieren:

Weitere Fehlfunktionen	Ein Ereignis kann weitere Fehlfunktionen im gleichen oder in anderen Systemen zur Folge haben, welche weitere Betroffene mit einer gewissen Intensität der Betroffenheit provoziert. In einem solchen Fall verlängern sich durch die Fehlfunktionen die Einzelvektoren in Abbildung 8 und die Gesamtwirkung vergrössert sich entsprechend.
Verstärkte Wahrnehmung	Die Wahrnehmung einzelner oder summierter Ereignisse wird durch die Medien intensiviert, so dass weitere indirekt Betroffene provoziert werden. Bei genügend breitflächiger Informationsverteilung und Wahrnehmungsintensivierung wird ein derartiges Thema auf politischer Ebene aufgegriffen, was den Einsatz von SONIA zur Folge haben kann.

4.3.3 Entscheidungshilfen

Entscheidungshilfen im praktischen Einsatz prüfen

Folgende Tabellen bieten eine Entscheidungshilfe, die für die Beurteilung eines Einsatzes von SONIA herangezogen werden können. Diese Tabellen sind für den praktischen Einsatz von MELANI zu ergänzen und zu prüfen.

Ausgehend von der Primär- und Sekundärwirkung¹⁸⁾ wird versucht, Rückschlüsse auf die Ursache zu ziehen. Allerdings müssen sich die Analysten bewusst sein, dass zwischen Wirkung und Finden der Ursache einige Zeit verstreichen kann. Dies hat zur Folge, dass bereits aufgrund der Wirkung über ein Engagement von SONIA zeitgerecht entschieden werden muss.

18) Unter Primärwirkung verstehen die Autoren die Summe der Wirkungen, die durch Einzelereignisse im gleichen Bereich auftreten. Betrifft die Wirkung durch weitere Fehlfunktionen einen anderen Bereich, wird diese zur Sekundärwirkung. Die Grenze zwischen Primär- und Sekundärwirkung ist unscharf.

Tabelle 6:
Thematische Bestimmung des
Einsatzspektrums von SONIA

Nr	Ursache	Primärwirkung	Sekundärwirkung	Aufgebot SONIA
1	Informations-sicherheit /-infrastruktur	Informationsinfra- struktur	Informationsinfra- struktur oder andere Bereiche	Ja
	<i>z.B. logischer Betriebssy- stemfehler</i>	<i>z.B. Ausfall von IT- Infrastrukturkompo- nenten</i>	<i>z.B. Business Prozesse fallen aus</i>	
2	Informations-sicherheit /-infrastruktur	Andere Bereiche	Andere Bereiche	Ursachenabhängig – relevant ist der Stö- rungsgrad der In- formationsinfrastruk- tur
	<i>z.B. Fehler in Bahnleitsy- stemsoftware</i>	<i>z.B. Zugsunglück</i>	%	
3	Informations-sicherheit /-infrastruktur	Andere Bereiche	Informationsinfra- struktur	Ursachen- und Wir- kungsabhängig – relevant ist der Stö- rungsgrad der In- formationsinfrastruk- tur
	<i>z.B. Energie- versorgungs- Steuerungs- software</i>	<i>z.B. Stromversorgung</i>	<i>z.B. Ausfall von Infor- mations- Infrastrukturkompo- nenten</i>	
4	In anderen Bereichen	Informationsinfra- struktur oder an- dere Bereiche	Informationsinfra- struktur oder andere Bereiche	Nein
	<i>z.B. Energie- versorgung</i>	<i>z.B. Ausfall von Informations- Infrastrukturkompo- nenten</i>	%	

Entscheid zum Einsatz von
SONIA

Falls die simultane Beurteilung der Ereignisse gemäss obiger Tabelle grund-
sätzlich auf eine Aktivierung von SONIA hinweist, soll durch die Abschät-
zung der Wirkung und des Eskalationspotentials eine Entscheidung über
den Einsatz von SONIA herbeigeführt werden können.

Tabelle 7:
Komponentenbasierte Analyse
der Wirkung

Nr	Anzahl Betroffene			Intensität der Betroffenheit		Wahrnehmung	Eskalationspotential	Aufgebot SONIA
	Sektorübergreifend	Unternehmensübergreifend	Viele Einzelpersonen	Grundfunktionen	Grundbedürfnisse	Intensität		
5	X	X	X	Nein	Nein	1	Nein	Nein
6	X	X	X	Nein	Nein	2	Ja	Eventuell im Sinne der Prävention
7	X	X	Ja	X	Ja	1-4	X	Ja
8	Ja	X	X	Ja	X	1-4	X	Ja
9	Nein	Ja	Nein	Ja	Nein	1-2	Nein	Nein
10	Nein	Ja	Nein	Ja	Nein	2	Ja	Ja, im Sinne der Prävention

Erläuterungen:

Generell:

X: Ja oder Nein: In der gegebenen Konstellation nicht mehr relevant, Entscheid über den Einsatz von SONIA wird bereits gefällt.

Wahrnehmungsintensität:

- 1: Nur direkt Betroffene nehmen das Ereignis wahr
- 2: Lokale Medien (Druck, Lokalradio) interessieren sich für das Ereignis.
- 3: Nationale Medien (Druck, nationale Radiosender und Fernsehen) interessieren sich für das Ereignis.
- 4: Globale Medienpräsenz, Stellungnahmen werden erwartet, Pressekonferenzen.

Eskalationspotential:

Ja: Wahrnehmungsintensivierung durch die Medien oder weitere logische Fehlfunktionen.

Nein: Es werden keine weiteren logischen Fehlfunktionen erwartet und das Medieninteresse bleibt gleich oder nimmt ab.

Interpretation von Informationen Wichtig beim Analyseprozess ist die Fähigkeit, die Informationen über Ereignisse richtig zu interpretieren und das Eskalationspotential richtig abzuschätzen. Fehlalarme werden unumgänglich sein, um erste Erfahrungen aufzubauen.

4.3.4 Überprüfung der Entscheidungshilfe anhand von drei Szenarien

Beurteilung Einsatz SONIA
anhand von Szenarien

In diesem Abschnitt versuchen die Autoren die Szenarien anhand der aufgeführten Kriterien zu untersuchen und einen Einsatz von SONIA zu beurteilen. Die detaillierten Szenarien sind im Anhang A6 aufgeführt. Da sich SONIA ausschliesslich Ereignissen im Informationsinfrastrukturbereich annimmt, müssen die Ereignisse speziell auf deren Relevanz für MELANI und SONIA untersucht werden.

4.3.5 Szenario 1: Inhaltliche Bedrohung über E-Mails

Fall a) In diesem Szenario handelt es sich um eine Einschüchterungskampagne, welche das Internet als Medium verwendet.

Die Aktivierung von SONIA ist nicht notwendig, da nur Inhalte über eine einwandfrei funktionierende Informationsinfrastruktur übertragen werden. In dieser Phase könnte MELANI als Triagestelle dienen und z.B. die Bundespolizei informieren, damit diese vom Ausmass der Massensendungen informiert ist und dadurch Massnahmen einleiten kann.

Fall b) Aus der allgemeinen Verunsicherung in der Bevölkerung entsteht auch in der Informationsinfrastruktur ein Problem. Die Internetbenutzer verschicken unzählige E-Mails mit grossen Attachments, die in dieser Ansammlung das Internet zu überlasten beginnen (Szenario 1, Abschnitt 12). Damit nimmt auch die Performance des Internets langsam ab. Für diesen Fall wäre ein Einsatz von SONIA thematisch grundsätzlich denkbar.

Tabelle 8:
Themenrelevanz Szenario 1

<i>Nr</i>	<i>Ursache</i>	<i>Primärwirkung</i>	<i>Sekundärwirkung</i>	<i>Aufgebot SONIA</i>
1	Informationssicherheit /infrastruktur	Informationsinfrastruktur	Informationsinfrastruktur oder andere Bereiche	Ja
4	In anderen Bereichen	Informationsinfrastruktur oder andere Bereiche	Informationsinfrastruktur oder andere Bereiche	Nein

In der Analyse der Wirkung zeigt der Fall a (Zeile Nr. 5), dass eine grosse psychologische Wirkung in der Bevölkerung erzielt wird, dass aber auf die Informationsinfrastruktur bezogen keine Wirkung spürbar ist. SONIA muss deshalb nicht aufgegeben werden. Dieses Szenario hat ein kleines Eskalationspotential (Zeile Nr. 6). Das Aufgebot von SONIA ist aber auch in diesem Fall nicht zwingend, da die Ursache der Internet-Überlastung in den Userinteraktionen (E-Mails) liegt.

Tabelle 9:
Wirkungsrelevanz Szenario 1

<i>Nr</i>	<i>Anzahl Betroffene</i>			<i>Intensität der Betroffenheit</i>		<i>Wahrnehmung</i>	<i>Eskalationspotential</i>	<i>Aufgebot SONIA</i>
	Sektorübergreifend	Unternehmensübergreifend	Viele Einzelpersonen	Grundfunktionen	Grundbedürfnisse			
5	X	X	X	Nein	Nein	Intensität	Nein	Nein
6	X	X	X	Nein	Nein	2	Ja	Eventuell im Sinne der Prävention

4.3.6 Szenario 2: Illegale Banktransaktionen

Im Szenario 2 nutzen Mafia-ähnliche Gruppierungen bekannte Schwächen in der „Sandbox“ der Java Virtual Machine, um Login-Versuche von Bankkunden abzufangen und selber Transaktionen auf fremde Konten durchzuführen.

MELANI als zentrale Sammelstelle hat den Überblick über alle Meldungen, die bezüglich Hacking der Banken auftauchen. Die Anhäufung von Hacking Attacken (Szenario 2, Abschnitte 1, 4, 6) lässt bereits vermuten, dass es sich um gezielte Angriffe handelt. Falls nicht schon initiiert, müsste MELANI durch einen Informationsaustausch die betroffenen Firmen zusammenbringen und/oder koordinieren. Zu diesem Zeitpunkt hat MELANI jedoch noch keine Kenntnis über die Wirkung des Ereignisses.

Tabelle 10:
Themenrelevanz Szenario 2

<i>Nr</i>	<i>Ursache</i>	<i>Primärwirkung</i>	<i>Sekundärwirkung</i>	<i>Aufgebot SONIA</i>
1	Informationssicherheit /- infrastruktur	Informationsinfrastruktur	Informationsinfrastruktur oder andere Bereiche	Ja

Kurz nach den Hacking Attacken ist die Primärwirkung noch nicht bekannt. Spätestens nach der Fernsehsendung über die aufgebrachtten Bürger zeigt sich erstmals die Wirkung. Sie kann jedoch noch nicht unbedingt in Zusammenhang mit den Hacking-Attacken gebracht werden. Die Wahrnehmungsintensität in der Bevölkerung nimmt mit den auftretenden Medienmeldungen stetig zu, so dass der Einsatz von SONIA in Erwägung gezogen werden muss (Szenario 2, Abschnitt 8-10). Es scheinen viele Einzelpersonen in Kombination mit einem spezifischen Sektor betroffen zu sein. Zudem sind Einzelpersonen in ihren Grundbedürfnissen unbefriedigt, wenn sie an den Bankomaten falsche Kontomutationen feststellen und kein Geld beziehen können.

Spätestens zu dem Zeitpunkt, wo das modifizierte Applet auftaucht, kann davon ausgegangen werden, dass die Hacking Attacken mit den jüngsten Medienmeldungen in Zusammenhang stehen. Die Softwareanalyse des Applets bestätigt, dass das Applet auf die Ressourcen zugreifen kann (Ursache). Die Tragweite dieser Feststellung provoziert ein Aufgebot von SONIA (Szenario 2, Abschnitt 14), da nun auch weitere Sektoren betroffen sein könnten und e-Commerce und e-Government Anwendungen überprüft werden müssen.

Tabelle 11:
Wirkungsrelevanz Szenario 2

Nr	Anzahl Betroffene			Intensität der Betroffenheit		Wahrnehmung	Eskalationspotential	Aufgebot SONIA
	Sektorübergreifend	Unternehmensübergreifend	Viele Einzelpersonen	Grundfunktionen	Grundbedürfnisse	Intensität		
7	X	X	Ja	X	Ja	1-4	X	Ja
8	Ja	X	X	Ja	X	1-4	X	Ja

4.3.7 Szenario 3: Krise aufgrund von Indizien

Das Szenario 3 versucht, aufgrund von Indizien eine Reaktion zu provozieren. Die hohen Übertragungsgeschwindigkeiten haben in Fällen von Fehlerübertragungen sehr kurze Reaktionszeiten zur Folge. In diesem Szenario ist die Ursache zunächst nicht bekannt. Sichtbar sind allerdings die Auswirkungen im Informationsinfrastrukturbereich, dessen Funktionen beeinträchtigt sind.

Tabelle 12:
Themenrelevanz Szenario 3

Nr	Ursache	Primärwirkung	Sekundärwirkung	Aufgebot SONIA
1	Informationssicherheit /-infrastruktur	Informationsinfrastruktur	Informationsinfrastruktur oder andere Bereiche	Ja

Die Wirkung zeigt sich sehr schnell, indem innerhalb von rund 30 Minuten der Netzwerkverkehr auf gegen Null geht. Sobald der Netzwerkverkehr abnimmt, kann davon ausgegangen werden dass mehrere Sektoren betroffen sind und daher auch Grundfunktionen (über Internet) nicht mehr funktionieren. Die Wahrnehmungsintensität wird in naher Zukunft stark zunehmen und es ist noch nicht abzuschätzen, welches Eskalationspotential diese Ereignisse haben. Ein Aufgebot von SONIA ist unumgänglich (Szenario, Abschnitt 8).

Tabelle 13:
Wirkungsrelevanz Szenario 3

Nr	Anzahl Betroffene			Intensität der Betroffenheit		Wahrnehmung	Eskalationspotential	Aufgebot SONIA
	Sektorübergreifend	Unternehmensübergreifend	Viele Einzelpersonen	Grundfunktionen	Grundbedürfnisse	Intensität		
8	Ja	X	X	Ja	X	1-4	X	Ja

Nach der Feststellung der technischen Ursachen muss SONIA als Koordinator auftreten, um die Netzwerkinfrastruktur auf definierte Weise wieder hochzufahren. Es werden mit grosser Wahrscheinlichkeit Stellungnahmen verlangt.

Die Autoren gehen davon aus, dass die Reaktionszeit von 30 Min. zu kurz ist, um präventive Entscheide treffen zu können, zumal die Entwicklung der Netzbelastung nicht voraussehbar ist.

5 Ausblick und Empfehlungen

- Grosses Interesse und weitere Vorschläge
- Dieser Bericht wurde zwischen November 2000 und November 2001 zu Händen des Informatikstrategieorgans Bund (ISB) erarbeitet. Während der Projektarbeit zeigten verschiedene Stellen und Betroffene grosses Interesse an den Bemühungen des ISB. Ziel dieses Berichts war es, ein umsetzbares Konzept für MELANI und SONIA zu formulieren. In der Konzeption wurde darauf geachtet, dass weitere Lösungsansätze und Ideen von externen Partnern in einer späteren Phase integriert werden können. Insbesondere sei für die Umsetzung auf die folgenden Punkte im Sinne von Empfehlungen hingewiesen:
1. Einsatzkonzepte den Erfahrungen anpassen

SONIA und MELANI werden eine gewisse Zeit brauchen, bis optimale Einsatzformen und -konzepte vorliegen. Anpassungen aufgrund von Erkenntnissen aus Übungen und Einsätzen sollen bewusst vorgenommen werden können.

 2. Personelle Besetzung SONIA sicherstellen

Bei der Umsetzung ist zu beachten, dass der Sonderstab personell genügend stark besetzt wird. Erfahrungsgemäss ist im Einsatzfall nur mit einem stark reduzierten Bestand zu rechnen (Abwesenheit, Personen nicht erreichbar etc.). Grosse Sorgfalt ist einer funktionierenden Stellvertreterregelung zu schenken. Zudem ist der Einsatz von Unterstützungspersonal zu prüfen, um im Einsatzfall die gewünschten Produkte zeitgerecht erstellen zu können.

 3. Schrittweiser Aufbau MELANI

Mit MELANI wird in vielerlei Hinsicht Neuland betreten. Der Aufbau wird Zeit brauchen und aus ersten Erfahrungen sind die Lehren für die weiteren Arbeiten zu ziehen. Es wird kaum möglich und sinnvoll sein, die gesamte Organisation und die entsprechenden Informatikmittel auf einen einzelnen Zeitpunkt hin abschliessend bereitzustellen.

 4. Synergien in Bund und Wirtschaft nutzen

Synergien mit bestehenden Analyse- und Alarmstellen sowie Einsatzorganisationen des Bundes, aber auch der Privatwirtschaft sind zu nutzen.

 5. Kontakt ins Ausland aufbauen

MELANI kann nur mit einem funktionsfähigen Sensorennetz funktionieren. Die Kontakte ins Ausland sind dabei von grosser Wichtigkeit und sollen rasch organisiert werden (CERTs, EWIS etc.). Damit kann auch vom Austausch während des Aufbaus analoger Strukturen im Ausland profitiert werden.

 6. Die Kantone als Partner in die Übungen einbauen

Die Kantone sind wichtige Partner auf dem Weg zu sicheren kritischen Informationsinfrastrukturen. Sie sind frühzeitig in die Kontaktnetze von MELANI zu integrieren. Sobald die wesentlichen Elemente der Organisationen bereitstehen, können gemeinsame Übungen aufgenommen werden.

7. Vertrauen durch Information Die Aufgaben und Strukturen von MELANI und SONIA sind frühzeitig zu kommunizieren, um den entsprechenden Bekanntheitsgrad und das notwendige Vertrauen zu gewinnen. Dies erleichtert im Ereignisfall die Kommunikation.
8. Kritische Infrastrukturen Dem Internet kommt bei den Betrachtungen von MELANI und SONIA eine grosse Bedeutung zu. Aus weiteren Überlegungen im Themenbereich Critical Infrastructure Protection (CIP) folgt, dass auch andere elektrische und elektronische Netzwerke inkl. der Telefonie eine grosse strategische Bedeutung haben und entsprechend in die Konzeption einbezogen werden sollten.
9. Gesamtkonzept Information Assurance Das vorliegende Konzept diskutiert die Einsatzorganisation Information Assurance zur Ereignisbewältigung. Im Sinne eines ganzheitlichen Risikoansatzes soll der vollständige Risk Management Zyklus berücksichtigt und auch präventive Arbeiten betrachtet werden. Solche Arbeiten würden zu einer umfassenden Information Assurance Strategie Schweiz beitragen. Für das Erarbeiten einer solchen Strategie wird vorgeschlagen, neben den staatlichen Stellen wichtige Vertreter der Wirtschaft und der Wissenschaften zu begrüessen.

Ausgewählte Literatur

Auswertung INFORMO 2001: Gesamtüberblick über die Hauptprobleme und Kernfragen, Carrel, Laurent F., Bern, September 2001

Grundlagen zum Konzept Melde- und Analysestelle Informationssicherheit (MELANI) sowie für den Sonderstab Information Assurance (SONIA), Rytz, Ruedi, Informatikstrategieorgan Bund, Bern, Version vom 24. September 2001

Konzept „Information Assurance“, Koordinationsgruppe Informationsgesellschaft KIG, Bern, Mai 2000

Konzept für einen Sonderstab Informationssicherheit Version 1.0 (vertraulich) Informatikstrategieorgan Bund ISB und Ernst Basler + Partner AG, Bern und Zollikon, März 2001

Lagezentrum Schweiz – Schlussbericht der Operation MILLENNIUM TRANSIT s.15ff, Generalstab, Bern, Mai 2000

Melde- und Analysestelle Informationssicherheit, Erhebung von Kundenbedürfnissen, TM 200161-2, Informatikstrategieorgan Bund und Ernst Basler + Partner AG, Bern und Zollikon, 15.10.2001,

Melde- und Analysestelle Informationssicherheit, Grobübersicht über ausländische Modelle“, TM 200161-3, Informatikstrategieorgan Bund und Ernst Basler + Partner AG, Bern und Zollikon, 12.10.2001

Prüfung der Verordnung Sonderstab Informationssicherheit Rechtsdienst des Eidgenössischen Finanzdepartements GS-EFD Juli 2001

Sonderstab Informationssicherheit – Auswertung der Übung INFORMO 2001, Ernst Basler + Partner AG, Zollikon, Juni 2001

Szenarien für MELANI und SONIA, Informatikstrategieorgan Bund und HTA Luzern, Bern und Horw, 28.11.2001

Y2K: Starting the Century Right Report of the International Y2K Cooperation Center, Washington, February 2000

A1 Szenarien zur Gefährdung der Informationsinfrastruktur

Methodik

Generelles

Die betrachteten Szenarien beziehen sich auf die Schweiz, d.h. dass entweder die Ursache oder das Ausmass eines bestimmten Ereignisses die Schweiz betreffen.

Wahrscheinlichkeit (w)

häufig Ereignis tritt einmal pro Jahr oder häufiger ein

gelegentlich Ereignis tritt einmal pro 10 Jahre oder häufiger ein

selten Ereignis tritt seltener als einmal pro 10 Jahre ein

Ausmass (A)

Beim Ausmass werden sowohl direkte Schäden (Sachschäden, finanzieller Verlust etc.) als auch indirekte Schäden (Imageverlust u.ä.) erfasst.

klein Ereignis tritt nur in einem Unternehmen/einer Verwaltungseinheit auf; Schaden kann durch eigene Kräfte behoben werden, Bürger ist nicht betroffen.

mittel Ereignis betrifft mehrere Unternehmen/ganze Branche oder ganze Verwaltungen; Schaden kann nicht durch eigene Kräfte behoben werden, Bürger ist betroffen (Verzögerungen von Dienstleistungen); Schaden ist reparabel.

gross Ereignis betrifft mehrere Branchen oder mehrere Verwaltungen; Schaden kann nicht durch eigene Kräfte behoben werden, Bürger ist betroffen (Ausbleiben von Dienstleistungen); Schaden ist irreparabel.

Szenarien

Virenbefall von PCs in der Verwaltung und Privatwirtschaft

Ein Mitarbeiter in der Verwaltung öffnet durch Doppelklick ein E-Mail-Attachment, das mit einem Virus versehen ist. Das Virus manipuliert Dateien auf dem PC und versendet selbständig E-Mails an Adressaten aus dem elektronischen Adressbuch des Benutzers. Nach dem Abschalten kann die Arbeitsstation nicht mehr gestartet werden. Es werden mehrere Arbeitsstationen in der Verwaltung und in der Wirtschaft mit dem Virus befallen.

w = häufig , A = klein

Beispiele dazu sind der „Melissa“ , „I Love You“ und „Anna Kournikova“ Virus.

Abfluss sensibler Daten I (persönliche Daten)

Es wird bekannt, dass Insider aus der Verwaltung sensitive Daten (Informationen aus den Bereichen AHV/IV/Krankenversicherung, Löhne, interne Buchhaltungsdaten, Adressen, Pensionskassengelder) an ausländische Kunden weiterverkaufen.

w = häufig, A = mittel (Image?)

Ein Beispiel: Vertrauliche Informationen aus der UBS werden unabsichtlich an die Webadresse wdr.org gesendet. Diese Adresse gehörte früher der UBS-Tochter Warburg Dillon Read, wurde aber nach der Freigabe vom deutschen Journalisten Wolf-Dieter Roth übernommen. *Quelle: Sonntagszeitung, 16. Juli 2000*

Fehlerhaftes Software-Update in kritischem Sektor (z.B. Energie)

Ein Software-Update löst einen kurzen Stromausfall (wenige Stunden) in einem Elektrizitätswerk aus.

w = gelegentlich, A = klein

Ein Beispiel: Mitte September 1991 führte ein Fehler in der Software zur Steuerung der Strahlenschutz-Türen im britischen Kernkraftwerk „Sellafield“ dazu, dass die Türen trotz hoher Radioaktivität in den Kammern geöffnet wurden. Obwohl keine Menschen direkt zu Schaden kamen, blieb das Kraftwerk seither abgeschaltet. Der Fehler steckte in einer neueren Softwareversion, welche die alte fehlerfreie Software ersetzte.

Propagandamissbrauch des Webservers der Bundesverwaltung

Einige Web-Server der Verwaltung (teilweise auch www.admin.ch resp. Portal-Seite des Bundes) werden während zweier Tage für ausländische Propaganda missbraucht.

w = gelegentlich, A = klein (Imageschaden?)

Über einige namhafte Schweizer Grossunternehmen werden wiederholt im Internet negative Meldungen und Gerüchte verbreitet. Gefälschte E-Mails und Pressecommuniquées werden Finanzanalysten zugespielt. Die Grossunternehmen verzeichnen kurzfristig Kurseinbussen an der Börse und verlieren einige ihrer Kunden (Umsatzeinbussen).

w = gelegentlich, A = mittel (Imageschaden?)

Überlastung mehrerer Webserver der Privatwirtschaft

Durch einen konzentrierten Angriff werden Web-Server von privaten Unternehmen überlastet. Die Denial-of-Service-Attacke hat zur Folge, dass die Unternehmen während einiger Tage im Internet nicht erreichbar sind, was eine beträchtliche Umsatzeinbusse und einen Imageverlust nach sich zieht.

w = gelegentlich, A = mittel (Imageschaden?)

Beispiel: Die distributed Denial-of-Service Attacke in der ersten Februarwoche 2000 auf verschiedene amerikanische Unternehmen (Amazon, yahoo, eBay, buy.com). *Quelle: Tages-Anzeiger 14. Februar 2000*

Organisierter und koordinierter Diebstahl von Kreditkarteninformationen

Virtueller Kreditkartendiebstahl mit realen Auswirkungen

w = gelegentlich, A = mittel

Ein Beispiel: Nach amerikanischen Agenturberichten ist es einem Cracker gelungen, bis zu 55'000 Kreditkartennummern von den Webseiten der Firma CreditCards.com zu stehlen. CreditCards.com habe die Anzahl dementiert, den Einbruch aber bestätigt. Das Unternehmen ist spezialisiert auf die Transaktionsabwicklung für Unternehmen, die Zahlungen per Kreditkarte von ihren Kunden akzeptieren wollen. Das Sicherheitsproblem sei offensichtlich schon vor vier Monaten aufgetaucht, und der Cracker habe seitdem versucht, CreditCards.com zu erpressen. Nun seien die Nummern im Internet veröffentlicht worden, mit der Anmerkung des Crackers, er werde die Firma „in den Ruin treiben“. Die Geschichte sei erst aufgefliegen, als Kunden nicht

von ihnen autorisierte Umsätze auf ihren Kreditkartenrechnungen vorfanden. CreditCards.com habe sich bei den betroffenen Kunden nicht gemeldet und dies auch nicht vorgehabt. Die Firma beharrt weiter auf ihrer Position, dass nur sehr wenige Kundendaten erbeutet wurden; zum grössten Teil habe es sich um „Testdaten“ gehandelt.

Quelle: <http://www.heise.de/newsticker/data/pmo-13.12.00-000/>

Abfluss sensibler Daten II (Quellcode)

Es wird bekannt, dass Hacker Softwareentwicklungsunternehmen angreifen und an Quellcode von Applikationen gelangen. Dieser Code kann an die ausländische Konkurrenz verkauft werden. Die betroffenen Unternehmen verlieren ihren Entwicklungsvorsprung bzw. ihre Marktposition.

w = gelegentlich, A = gross

Ein Beispiel: Unbekannte Cracker sind in das Computernetz von Microsoft eingedrungen und haben Sourcecode von neuesten Windows-Versionen und Office-Software entwendet, berichtet das Wall Street Journal unter Berufung auf informierte Quellen. Die Cracker hatten drei Monate lang Zugriff auf das Netzwerk – ob sie auch Code verändert haben, wird zur Zeit noch untersucht. Ein Microsoft-Sprecher bestätigte inzwischen den Einbruch in das firmeneigene Netz, wollte aber keinen weiteren Kommentar abgeben. Der Software-Riese wollte den Einbruch ursprünglich auf eigene Faust untersuchen, schaltete dann aber am gestrigen Donnerstag das FBI ein. Der Einbruch wurde am Mittwoch entdeckt. Log-Files belegen, dass an diesem Tag Quellcode an einen E-Mail-Empfänger in St. Petersburg (Russland) geschickt wurde. Eine anonyme Quelle bei Microsoft erklärte der US-Zeitung, dass der Einbruch wahrscheinlich ursprünglich mit Hilfe des QAZ-Trojaners bewerkstelligt wurde: Ein unbekannter Angestellter hat demnach den so genannten „Notepad-Wurm“ in einem E-Mail Attachment bekommen. Die unbekannteren Cracker haben dann Programme installiert, die heimlich Passwörter von Microsoft-Mitarbeitern protokollierten. Das Motiv ist noch unklar. Sicherheitsexperten spekulieren allerdings, dass es sich um eine „Daten-Entführung“ handeln könnte, bei der die unbekannteren Cracker Lösegeld mit der Drohung erpressen, die Daten ansonsten zu veröffentlichen. *Quelle: www.heise.de/newsticker/ vom 27.10.00*

Erpressung eines KKW-Betreibers

Um ihre Ziele durchzusetzen, droht eine Gruppe militanter Separatisten, die Steuerung eines KKW zu manipulieren. Als Beweis ihres angeblichen Zugriffs auf die Steuerungssoftware spielen sie den Medien Teile von log-Dateien zu, welche die Steuerungssoftware erstellt hat. Da nicht absolut ausgeschlossen werden kann, dass die Gruppe tatsächlich Zugriff hat, treten die Behör-

den auf Verhandlungen ein. Durch das Medienecho und die zurückhaltende Informationspolitik der Behörden entsteht in der Bevölkerung eine grosse Verunsicherung. Teilweise kommt es zu Panikreaktionen und Demonstrationen.

w = selten, A = mittel

Blockierte Alarmnummern

Es gelingt Hackern, in das Telefonsystem einer Stadtverwaltung einzudringen und die Notfallnummern auf eine nicht existierende Nummer umzuleiten. Während Stunden sind die Notfalldienste nicht erreichbar. Bei einigen Unfällen kommen die Notfalldienste deshalb zu spät, um Hilfe leisten zu können. Über das Radio wird die Bevölkerung aufgefordert, im Ereignisfall die Notfalldienste direkt aufzusuchen.

w = selten, A = mittel

Beispiel: Am 15. April 1996 gelang es Hackern, in das Telefonsystem des New Yorker Polizei Departements einzudringen und die Notfallnummer 911 während 12 Stunden komplett zu blockieren. *Quelle: unbekannt*

Manipulation bei Abstimmung

Es wird bekannt, dass in den Rechensystemen zur Speicherung der Abstimmungsergebnisse Unregelmässigkeiten aufgetaucht sind. Manipulationsgerüchte machen die Runde; Tageszeitungen nehmen die Meldung auf. Auch nach intensiven Nachforschungen kann nicht eruiert werden, ob und wo Manipulationen aufgetreten sind. Die Abstimmung muss neu ausgezählt werden.

w = selten, A = mittel (Imageschaden?)

Logische Bombe in Chip

Eine logische Bombe im neuesten Pentiumchip führt zu einem flächendeckenden Ausfall wichtiger Server der Verwaltung und Wirtschaft. Wichtige Applikationen liefern Fehlermeldungen und falsche Ausgabe-Daten.

w = selten, A = gross

Beispiel: Eine frühe Generation der Pentium-Prozessoren führte unter bestimmten Randbedingungen Divisionen inkorrekt aus.

Ausfall von wichtigen Infrastrukturkomponenten

Ausfall Stromversorgung

Es gelingt politisch motivierten Aktivisten in ein Elektrizitätswerk einzudringen und die Produktionsanlagen abzuschalten. Die Produktionsanlagen können nicht innert nützlicher Frist wieder ans Netz geschaltet werden. Verschiedene direkt abhängige Unternehmen müssen ihre Produktion während Tagen einstellen.

w = selten, A = gross

Ausfall der Stromversorgung in Neuseeland

Ein Beispiel: Der Zusammenbruch der Stromversorgung im neuseeländischen Auckland im Jahr 1997 während mehr als einer Woche führte zu wirtschaftlichen Schäden in der Höhe von mehreren hundert Millionen Dollar.

Ausfall der Wasserversorgung in USA

Beispiel: Wegen eines Ausfalls eines Rechners funktionierte die Wasserversorgung in Lewston (USA) bis zu 30 Stunden nicht korrekt. 40'000 Bewohner waren betroffen. Es passierte nachts und wurde bei der Routinekontrolle 14 Stunden später nicht bemerkt. Die Konsumenten wurden umgehend dazu angehalten, das Wasser zuerst abzukochen. Die Stadt hat nun ein „automatic system to notify an on-call supervisor in case this recurs“ installiert. *Quelle: Risks-Forum Digest; 18.08.1998*

Ausfall im Transportwesen bei den SBB

Beispiel: Als 1995 plötzlich zur gleichen Zeit am gleichen Tag 18 Lokomotiven der SBB zum Stillstand kamen und sich nicht mehr bewegen liessen, glaubte vorerst niemand an einen mutwilligen Hackerangriff. Aus sehr glaubhaften Quellen konnte man aber in Erfahrung bringen, dass sich mehrere Hacker einen Spass daraus machten, ihre Macht zu demonstrieren. Von Seiten der SBB war lediglich zu vernehmen, dass es sich bei diesem mysteriösen Massenstillstand um ein technisches Problem handle. *Quelle: Output, Nr. 5, 2. Mai 1996, p.55*

Grossflächiger Ausfall der Telefonie

Ein grosser Festnetzbetreiber rüstet seine Schaltzentralen mit neuer Hard- und Software aus. In der Testphase wurde die neue Konfiguration nur unter den üblichen betrieblichen Randbedingungen getestet. Nach einer Gratisaktion des Betreibers bricht das Netz infolge Überlastung zusammen. Es gelingt vorerst nicht, die Schaltzentralen wieder zu aktivieren. In einer Grossstadt und deren Agglomeration können grosse Teile weder telefonieren noch haben sie Zugang zum

Internet. Auch das Mobilfunknetz ist in der Folge überlastet. Verwaltung und Wirtschaft können nur das Allernötigste erledigen.

w = selten, A = gross

Ein Beispiel: Es begann ganz harmlos. Der Manager einer Telefongesellschaft in Baltimore hörte das Heulen einer elektronischen Alarmglocke, als er den Kontrollraum der Schaltzentrale betrat. Das Warngerät zeigte an, dass eine Platte mit integrierten Schaltkreisen fehlerhaft arbeitete und geprüft werden musste. Im Verlauf der nächsten Stunde wurde ihm klar, dass er sich mitten in einer Katastrophe befand. Die Computerbildschirme füllten sich mit Alarmbotschaften, die Drucker spuckten Unmengen von Fehlermeldungen aus, und die Techniker in den benachbarten Telefonzentralen meldeten, dass sie den Kontakt zum Hauptnetz verloren hatten. Was dann folgte, war einer der grössten Telefonnetz-Zusammenbrüche in der Geschichte der USA. Der Hauptrechner in Baltimore meldete, er sei total überlastet. Jedermann rechnete nun damit, dass die drei Ausweichrechner in der Region seine Aufgaben übernehmen würden. Dem war aber nicht so. Zwar hatte der Baltimore-Rechner die anderen Maschinen automatisch über seinen Zustand informiert. Diese entzifferten aber bloss eine Überlastungsmeldung und stellten daraufhin ihre Aktivitäten ebenfalls ein. Die Folge war ein sechsstündiger totaler Zusammenbruch des Nahverkehrsnetzes in den Bundesstaaten Maryland, Virginia, Westvirginia und in Washington DC. Rund 6,7 Millionen Telefonleitungen waren tot. Die Pizza-Auslieferkette Domino's blieb auf ihren Kuchenbergen sitzen. Sekretärinnen und Makler drehten Daumen. Apotheker verkauften zusätzliche Medikamente, ohne ein Rezept zu verlangen, da der Kontakt zu den Ärzten abgebrochen war. Rechtsgelehrte hatten keine Möglichkeit mehr, mit ihren Klienten zu konferieren. Die Notruf-Nummer der Region war zwar die ganze Zeit über in Betrieb, jedoch vollkommen überlastet, weil viele Leute anriefen, die einfach mal schauen wollten, ob sie im Notfall funktionsstüchtig wäre. Das Chaos war perfekt. Einige Tage nach diesen Ereignissen im Jahr 1991 brach das Telefonnetz im Bundesstaat Pennsylvania zusammen. Die Rechner taten so, als seien sie überlastet. Es wurden Software-Fehler vermutet, da das kürzlich installierte Zusatzprogramm nicht ausgiebig getestet worden war. Die Untersuchungen begannen heiss zu laufen. Gerüchte über Viren und Sabotage häuften sich. Der Satz „wenn das Telefonnetz zusammenbricht, folgt ihm die ganze moderne Gesellschaft auf dem Fuss“ schien sich bewahrheitet zu haben. *Quelle: Computerworld Schweiz, Nr. 29/91, 15. Juli 1991, p. 9, hoc*

Begrenzte Aktionen im Rahmen von Information Warfare

Der israelische Geheimdienst findet heraus, dass sich auf Schweizer Konten hohe Summen von verschiedenen palästinensischen Befreiungsorganisationen befinden. In einer Kombination aus politischem Druck und Einsatz von Information Warfare (Manipulation der Konten, Abhören von Gesprächen, Einspeisen von Falschinformationen, Störung von Regelsystemen) wird versucht zu verhindern, dass diese finanziellen Mittel eingesetzt werden können.

w = selten, A = gross

Befall mit sehr aggressivem Virus

In einer Bilddatei, die angeblich das Cover der noch nicht veröffentlichten neuen CD Michael Jacksons enthält, verbirgt sich ein äusserst aggressives Virus, das sich mittels der gängigen Mailprogramme selber in jeweils veränderter Form weiter verschickt. Dann löscht das Virus Teile aus den Officedateien, auf die der User Zugriff hat. Anschliessend löscht das Virus wichtige Dateien des Betriebssystems, sodass die Arbeitsstationen nicht mehr gestartet werden können. Da sich das Virus sowohl über Outlook als auch über Netscape Mail verbreitet, sind innert Stunden ganze Unternehmen betroffen und blockiert. Es vergeht mehr als eine Woche, bis die betroffenen Unternehmen ihre produktiven Aktivitäten wieder aufnehmen können.

w = selten, A = gross

Unsichere Verschlüsselung beim eCommerce entdeckt

Ein Mathematiker entdeckt, dass wichtige Verschlüsselungstechniken, die für die Systeme mit Public und Private Keys benötigt werden, nicht sicher sind. In kürzester Zeit werden über das Internet Tools verbreitet, mit denen elektronische Kundenbeziehungen missbraucht werden können. Verschiedene grosse Unternehmen reagieren auf diese Bedrohung zu wenig schnell und verlieren grosse Geldbeträge.

w = selten, A = gross

Vergleichbares Beispiel: Entdeckung einer möglichen Sicherheitslücke beim Speichern des Private Keys von PGP-Implementationen.

Quelle: <http://www.heise.de/newsticker/data/ju-22.03.01-001/>

A2 Basisinformationen zu Melde- und Analysestellen weltweit

Auswerte- und Meldeverbund zum Schutz kritischer Infrastrukturen (Deutschland)

Als Teil der deutschen Bemühungen zum Schutz der kritischen Infrastrukturen wird zur Zeit ein Auswerte- und Meldeverbund geplant. Während sich das CERT-Bund mit technischen Hilfestellungen beschäftigt, soll der Auswerte- und Meldeverbund Warnungen und Informationsaustausch betreiben. Er stützt sich dabei auf Meldungen aus Behörden, Bereichen kritischer Infrastrukturen, Grossunternehmen und Einzelpersonen. Im Detail sieht die Struktur und Arbeitsweise des Auswerte- und Meldeverbundes aufgrund des aktuellen Planungsstandes folgendermassen aus:

Auswerte- und Meldeverbund zum Schutz kritischer Infrastrukturen (zukünftig) (persönliche Mitteilung, Sept. 2001)		
Aufgaben und Produkte		
X	Warnungen/Alarmierung	<ul style="list-style-type: none"> Alarmierungen: Abteilungsleiter, Vorstände, Führungspersonal (Zielgruppe)
X	Statusmeldungen	<ul style="list-style-type: none"> Lagedarstellung (Virenaktivität, Hacking-Attacken, Netzbelastungen wichtiger Netze,...) für den eigenen Bereich. Nach aussen nur Meldungen und Handlungsempfehlungen
X	Lagebeurteilungen und Handlungsempfehlungen	<ul style="list-style-type: none"> Lagebeurteilungen nach Fachbereichen Kritische Infrastruktur und Gesamtbild
X	Empfehlung von Sofortmassnahmen zur Schadensverhütung	<ul style="list-style-type: none"> Handlungsempfehlungen: INFOCON, schematisierte Alarmierungsstufen
X	Empfehlung von allgemeinen Massnahmen zur Vorsorge und Schadensverhütung	<ul style="list-style-type: none"> Sensibilisierung als vorrangige Aufgabe einer koordinierten Presse- und Öffentlichkeitsarbeit in Zusammenarbeit mit einem gemeinsamen Meldekopf Auswerten der Metainformationen für den Schutz kritischer Infrastrukturen KRITIS liefert konzeptionelle, strategische Empfehlungen
	Produkte-Evaluation und Empfehlungen für Firewalls, Viren-	

	schutz etc.	
X	Publikationen	<ul style="list-style-type: none"> • Publikationen (wissenschaftl. Berichte, Newsletter, Tagesberichte) in Form von aktuellen Infos auf Homepage, Tagesmeldung (wie Newsgroup) Berichte
X	Individuelle Beratung bei Vorfällen	<ul style="list-style-type: none"> • Einsatzunterstützung: im Bereich des eigenen Hauses (Spezialisten) später amtsübergreifend + evtl. zivile Spezialisten der Branchen • Individuelle Beratung bei Vorfällen/Sorgentelefon <ul style="list-style-type: none"> - Detailberatung / Weitervermittlung an die Spezialisten nur in Ausnahmefällen - Ergebnis wird allen zur Verfügung gestellt (Wissensbank)
	Hilfestellungen technischer Art (Bereitstellen von Patches oder Recovery-Programmen,...)	
X	Weitere Aufgaben	<ul style="list-style-type: none"> • Grundlagenforschung: Auswertungs-Unterstützungsprogramme, Visualisierung komplexer Zusammenhänge, Auswertung über alle Infrastrukturbereiche hinweg
Kunden		<ul style="list-style-type: none"> • Behörden auf Bundesebene • Grossunternehmen im Bereich der kritischen Infrastrukturen • Wirtschaftsverbände • Bevölkerung (eingeschränkt) in Krisensituationen
Struktur und organisatorische Einbettung		<ul style="list-style-type: none"> • Aufteilung in einen Routinebetrieb und Schichtbetrieb im Krisenfall
Anzahl Personen		<ul style="list-style-type: none"> • 1 Person (Routinebetrieb) • 5 Personen (Krisenfall)

NIPC National Infrastructure Protection Center (USA)

Das *National Infrastructure Protection Center* (NIPC) ist für die Gefährdungsanalyse, Aufklärung und Warnung in Zusammenarbeit mit dem *Department of Defense* und der Privatwirtschaft zuständig. Es hat die Aufgabe, Gefährdungsanalysen für die nationale kritische Infrastruktur durchzuführen und Aspekte der Verletzlichkeit und der Strafverfolgung zu untersuchen, um bei Vorfällen reagieren zu können. Das NIPC warnt bei internationalen Gefährdungen.

Das NIPC hat in Zusammenarbeit mit der Privatwirtschaft das Projekt „InfraGard“ (<http://www.infragard.net>) ins Leben gerufen. Damit sollen die Verbindungen mit den privatrechtlichen Besitzern von kritischen Infrastrukturen gestärkt und der Informationsaustausch gefördert werden. Der Informationsaustausch über Gefährdungen, aber auch Vorfälle wird durch lokale „InfraGard chapters“ gefördert. Diese setzen sich aus Vertretern der lokalen FBI-Büros, Personen der Privatwirtschaft und der Verwaltung zusammen. Der Fokus liegt somit auf dem Zusammenfassen der regionalen Ressourcen zum Schutz der kritischen Infrastrukturen, der Bildung eines weitreichenden Sensornetzes über das ganze Land und der Möglichkeit, Warnungen schnell an eine breite Basis streuen zu können. Im Detail sieht die Struktur und Arbeitsweise des NIPC folgendermassen aus:

National Infrastructure Protection Center NIPC (http://www.nipc.gov , Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities, January 2001)		
Aufgaben und Produkte		
X	Warnungen/Alarmierung	<ul style="list-style-type: none"> Management eines „Cyber Emergency Support Teams“, das auf Cyberattacken gegen kritische Infrastrukturen reagieren soll (CIOS)
X	Statusmeldungen	<ul style="list-style-type: none"> Watch Operations Center: Entdeckung von Bedrohung und Verbreitung von Einschätzungen und Warnungen (AWS)
X	Lagebeurteilungen und Handlungsempfehlungen	<ul style="list-style-type: none"> Umfassende Einschätzungen/Analyse von Bedrohung aus dem In- und Ausland, von Verwundbarkeiten, von Ausnutzungstechniken in bezug auf Bedrohung physischer Art oder „aus dem Cyberspace“ gegen kritische Infrastrukturen der USA (AWS)
	Empfehlung von Sofortmassnahmen zur Schadensverhütung	
X	Empfehlung von allgemeinen Massnahmen zur Vorsorge und Schadensverhütung	<ul style="list-style-type: none"> Ausbildung von „Cyberdetektiven“ in den bundesstaatlichen, staatlichen und lokalen Strafverfolgungsbehörden von Personal aus dem privaten Sektor (TOSS)

	Produkte-Evaluation/ Empfehlungen für Firewalls/Virenschutz	
	Publikationen	
X	Individuelle Beratung bei Vorfällen	<ul style="list-style-type: none"> • Analytische Unterstützung bei Nachforschungen (AWS) • Koordination und technologische Unterstützung von Nachforschungen bei „Computer Intrusions“ (CIOS)
	Hilfestellungen technischer Art (Bereitstellen von Patches oder Recovery-Programmen,...)	
X	Weitere Aufgaben	<ul style="list-style-type: none"> • Plattform für Forschung und Analyse (AWS) • Netzwerkfunktion zwischen Regierungsstellen, Industrie und Wissenschaft, um Informationen über Bedrohungen, Verwundbarkeit und technologische Entwicklungen zu teilen
	Struktur und organisatorische Einbettung	<ul style="list-style-type: none"> • Zusammenarbeit mit Nachrichtendiensten (CIA, NSA, etc.) und dem privaten Sektor (Antivirus-Firmen, Industrieverbände, etc.) • 3 Untersektionen: CIOS: Computer Investigations and Operations Section AWS: Analysis and Warning Section TOSS: Training, Outreach, and Strategy Section
	Anzahl Personen	keine Angaben
	Operationsmodus	Die Sektion „Analysis and Warning Section“ (AWS) unterhält ein „Watch Operations Center“, das 24 Stunden an 7 Tagen pro Woche im Einsatz ist und in Verbindung mit Partnern in der Privatwirtschaft und mit Behörden im Bereich der Nachrichtendienste, der Verteidigung und Strafverfolgung steht.

ISACs Information Sharing and Analysis Centers (USA)

Im Bemühen um die Einbindung der privaten Besitzer und Betreiber bedeutender Infrastrukturen in den Schutz kritischer Infrastrukturen forderte die amerikanische Regierung die Schaffung sogenannter „Information Sharing and Analysis Centers“ (ISACs) durch den privaten Sektor. Die ISACs sollen Partnerschaften ermöglichen, das Problembewusstsein fördern und den Zugang zu Informationen erleichtern. Ausserdem sollen substantielle und umfassende Analysen von sektorspezifischen Verwundbarkeiten innerhalb und zwischen den Infrastrukturen durchgeführt und entsprechende Lösungsvorschläge erarbeitet werden. Bislang sind sechs sektorspezifische ISACs aufgebaut worden bzw. sind sektorspezifische Infrastrukturvertreter und –koordinatoren bestimmt worden, und zwar für die folgenden Bereiche:

- Telekommunikation
- Elektrizitätswerke
- Feuerwehrnotdienste
- Finanzdienstleistungssektor
- IT-Bereich
- Strafverfolgungsbehörde

Daneben gibt es weitere ISACs, die teilweise noch im Aufbau sind: Das „Millennium Solution Center ISAC“ (MSC-ISAC) beispielsweise ist ausschliesslich für den US-Regierungssektor vorgesehen und weder US-amerikanische Nichtregierungsorganisation noch Strafverfolgungsbehörden können auf das MSC-ISAC zugreifen. Die Anonymität bleibt auch zwischen den Mitgliedern gewährleistet. Zwei ISAC werden nachfolgend etwas genauer betrachtet:

ISAC des Finanzdienstleistungssektors

Financial Services Informations Sharing and Analysis Center

(<http://www.fsisac.com>, Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities, January 2001)

Das Financial Services Information Sharing and Analysis Center besteht aus einer sicheren Datenbank, Analysetools, und Informationserfassungs und –weiterverbreitungsmöglichkeiten. Diese sollen es autorisierten Einzelpersonen und -firmen ermöglichen, gegebenenfalls auch anonymisierte Berichte über Informationssicherheitsbedrohungen, -verwundbarkeiten, -vorfälle und –lösungen vorzulegen. ISAC-Mitglieder haben Zugang zu Informationen und Analysen, die von anderen Mitgliedern zur Verfügung gestellt werden oder die von anderen Quellen bezogen wurden (z.B. am. Regierung und Strafverfolgungsbehörden, Technologieprovider und Sicherheitsvereinigungen, z.B. CERT). Das „Financial Services ISAC (FS/ISAC)“ wendet sich ausschliesslich an Experten aus der Banken- und Versicherungsindustrie.

Aufgaben / Aufgabenbereiche

- Experten im Bereich Informationssicherheit können in einer industrieweiten Datenbank zu elektronischen Sicherheitsbedrohungen,

	-verwundbarkeiten, -vorkommnissen und -lösungen anonym Informationen teilen.
Produkte oder angebotene Leistungen	<ul style="list-style-type: none">• Datenbank mit anonymen oder nicht-anonymen Berichten• Sicherheitsspezialisten analysieren den Input im Hinblick auf mögliche Lösungen und verteilen – je nach Bedeutung – eine Warnung an ihre Mitglieder.
Struktur und organisatorische Einbettung	<ul style="list-style-type: none">• Das FS/ISAC und die Daten gehören den Mitgliedern via die FS/ISAC-GmbH und es wird von der „Global Integrity Managed Services Practice, Predictive Systems“ -Aktiengesellschaft betrieben.• Die Mitgliedschaft ist vertraulich, d.h. es existiert keine Mitgliedschaftsliste!• Informationen können von Regierungsstellen eingespeist, aber nicht abgefragt werden.• Privat und vertraulich organisiert.
Anzahl Personen	Keine Angaben
Operationsmodus	Keine Angaben

ISAC des IT-Bereichs

Information und Kommunikation: IT-ISAC

(<http://www.ita.org/infosec/itisacfaq.htm>, Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities, January 2001)

Das IT-ISAC ist eine Non-profit-Organisation der Informationstechnologiebranche. Es sammelt und verteilt Meldungen zur Verletzung der Informationssicherheit in seinem Sektor. Daneben werden auch Informationen zur Verletzlichkeit, Gefährdung, Angriffen, Schutz- und Gegenmassnahmen gesammelt und diskutiert. Das IT-ISAC besteht zur Zeit aus den 19 Gründungsmitgliedern mit namhaften Firmen von AT&T über IBM bis VeriSign. Beitreten können alle Betriebe der Branche nach Abschluss eines entsprechenden Vertrags.

Aufgaben / Aufgabenbereiche	<ul style="list-style-type: none"> Erfassung und Austausch von Information bezüglich elektronischen Vorfällen, Bedrohungen, Attacken, Verwundbarkeiten sowie Schutz- und Lösungsmöglichkeiten.
Produkte oder angebotene Leistungen	<ul style="list-style-type: none"> Sammlung und Synthese von Informationen Weitergabe von Informationen Koordination der Reaktion der IT-Industrie auf Bedrohungen
Struktur und organisatorische Einbettung	<ul style="list-style-type: none"> Internet Security Systems (ISS) übernimmt Tätigkeit (in Atlanta, GA) 19 Gründungsmitglieder offen für sämtliche IT-Firmen
Anzahl Personen	keine Angaben
Operationsmodus	24 Stunden, 7 Tage/Woche

UNIRAS UK Government CERT (Grossbritannien)

Das *Unified Incident Reporting and Alert Scheme (UNIRAS)* ist das britische Regierungs-CERT. Es ist ein Hauptpfeiler des britischen *National Infrastructure Security Co-ordination Center (NISCC)*. Mitglieder der UNIRAS Community sind Verwaltungseinheiten und Unternehmen, die mit sensiblen Daten der Regierung arbeiten oder sich mit dem Schutz der kritischen nationalen Infrastrukturen befassen. Im Detail sieht die Struktur und Arbeitsweise von UNIRAS folgendermassen aus:

Unified Incident Reporting and Alert Scheme (http://www.uniras.gov.uk)		
Aufgaben und Produkte		
X	Warnungen/Alarmierung	<ul style="list-style-type: none"> Warnungsfunktion über IT Sicherheitsvorfälle und entsprechende Verwundbarkeiten Alerts and Briefings (Alarm und Instruktionen) für Mitglieder (via e-mail) oder auf der Webseite
X	Statusmeldungen	<ul style="list-style-type: none"> Aufgabe als „Computer Emergency Response Team“ (UK Govt CERT)
X	Lagebeurteilungen und Handlungsempfehlungen	<ul style="list-style-type: none"> Koordination der „Electronic Attack Response Group (EARG)“ der NISCC, die bei schwerwiegenden elektronischen Angriffen gegen kritische Infrastrukturen Massnahmen ergreifen muss
X	Empfehlung von Sofortmassnahmen zur Schadensverhütung	<ul style="list-style-type: none"> Reaktion auf elektronische Attacken und weitere wesentliche IT Vorfälle
X	Empfehlung von allgemeinen Massnahmen zur Vorsorge und Schadensverhütung	<ul style="list-style-type: none"> Zusammenstellen von Informationen zur IT-Sicherheit
	Produkte-Evaluation und Empfehlungen für Firewalls, Virenschutz etc.	
X	Publikationen	<ul style="list-style-type: none"> Publikationen: „UNIRAS Quarterly Report“ (nun: „NISCC Quarterly Review“); Monatliches Bulletin mit Berichten über elektronische Attacken und Virusvorfälle
X	Individuelle Beratung bei Vorfällen	<ul style="list-style-type: none"> Help desk mit Beratung (Virenvorfälle, Hacker-Angriffe, Informationsanfragen)
	Hilfestellungen technischer Art (Bereitstellen von Patches oder	

	Recovery-Programmen,...)	
	Weitere Aufgaben	
Kunden		<ul style="list-style-type: none">• UNIRAS Community-Mitglieder• Weitere Betriebe und Privatpersonen nur sekundär (Publikation von Hinweisen auf der Web-Site)
Struktur und organisatorische Einbettung		<ul style="list-style-type: none">• Integraler Teil des „ National Infrastructure Security Co-ordination Centre“ (NISCC)• Unterstützung durch die technischen Ressourcen der „Communications & Electronics Security Group“ (CESG)
Anzahl Personen		keine Angaben
Operationsmodus		Help Desk, 24 Stunden, 7 Tage pro Woche, (telefonisch oder über e-mail)

CERT-IST Industrie Services et Tertiaire (Frankreich)

In Frankreich existiert ähnlich wie in Deutschland ein CERT für die Verwaltung (CERTA, <http://www.certa.ssi.gouv.fr>) sowie eines für die Forschung und Hochschulen (CERT-RENATER, http://www.renater.fr/Securite/CERT_Renater.htm). Das CERT-IST hingegen übernimmt die Koordination bei Informationssicherheitsproblemen im Bereich der Dienstleistungen und Industrie, um damit Schäden und entsprechende Kosten zu reduzieren. Ziel ist die Reduktion von Netzwerkangriffen.

CERT-IST Industrie Services et Tertiaire, Frankreich (http://www.cert-ist.com)		
Aufgaben und Produkte		
X	Warnungen/Alarmierung	<ul style="list-style-type: none"> Sicherheitsberatung und Benachrichtigung bei Alarm (je nach Interesse und Konfiguration des Kunden)
X	Statusmeldungen	<ul style="list-style-type: none"> innerhalb des grundsätzlichen Auftrags
X	Lagebeurteilungen und Handlungsempfehlungen	<ul style="list-style-type: none"> innerhalb des grundsätzlichen Auftrags
X	Empfehlung von Sofortmassnahmen zur Schadensverhütung	<ul style="list-style-type: none"> innerhalb des grundsätzlichen Auftrags
X	Empfehlung von allgemeinen Massnahmen zur Vorsorge und Schadensverhütung	<ul style="list-style-type: none"> Zugang übers Web zu einer Datenbank über Verwundbarkeiten, die seit 1997 besteht und seither regelmässig nachgeführt wird Sammlung von Logs und Training bei deren Auswertung Bereitstellung von Methodik und Instrumenten
X	Produkte-Evaluation und Empfehlungen für Firewalls, Virenschutz etc.	<ul style="list-style-type: none"> Produkt-Evaluationen hinsichtlich deren Sicherheit
X	Publikationen	<ul style="list-style-type: none"> Monatliches Sicherheitsbulletin (kurze Wiederholung aller Sicherheitsratschläge und –warnungen des vergangenen Monats, Artikel zu aktuellen Themen, nachgeführte und ausführliche Liste der Sicherheitsratschläge und –warnungen)
X	Individuelle Beratung bei Vorfällen	<ul style="list-style-type: none"> Hotline
X	Hilfestellungen technischer Art (Bereitstellen von Patches oder	<ul style="list-style-type: none"> Unterstützung wenn nötig vor Ort für die Behebung von Vorfällen

	Recovery-Programmen,...)	
	Weitere Aufgaben	
Struktur und organisatorische Einbettung	<ul style="list-style-type: none">• Unter der Schirmherrschaft der französischen nationalen Sicherheitsorganisationen (SGDN und DCSSI)• Zwei Partnerorganisationen: CERT-RENATER (Forschungs- und Bildungssektor); CERTA (Regierungs- und Verwaltungssektor)• Mitglied der von der franz. Regierung ins Leben gerufenen Organisation zum Schutz kritischer Infrastrukturen	
Anzahl Personen	keine Angaben	
Operationsmodus	Hotline (unklar, ob 24h-Betrieb)	

CanCERT (Kanada)

Das CanCERT bietet einen öffentlichen non-profit Service für die internationale Koordination mit CERTs und FIRST. Bei Zwischenfällen initiiert das Team einen Beantwortungsservice für Regierung, Wirtschaft und akademische Organisationen, macht Untersuchungen und beantwortet Fragen bezüglich der Informationstechnologie. Es existiert ein Service rund um die Uhr zur Meldung von Zwischenfällen und für Beratungen. Das CanCERT veröffentlicht ein Bulletin mit neuen Nachrichten. Für seine Kunden offeriert das Team Tools, Sicherheitshinweise, Seminare zum Sicherheitsbewusstsein, Scans zur Überprüfung der Verletzlichkeit, Tests zur Durchlässigkeit des Netzwerkes, Monitoring der Netzwerke und Trainings zur Erkennung von Eindringenden.

CanCERT (http://www.cancert.ca)		
Aufgaben und Produkte		
X	Warnungen/Alarmierung	<ul style="list-style-type: none"> • Warnungshinweise über mögliche Attacken • „Incident Response Service“ (24h, 7 Tage/Woche im Einsatz)
	Statusmeldungen	
X	Lagebeurteilungen und Handlungsempfehlungen	<ul style="list-style-type: none"> • Siehe auch Statusmeldungen resp. Empfehlungen für Sofortmassnahmen
X	Empfehlung von Sofortmassnahmen zur Schadensverhütung	<ul style="list-style-type: none"> • Sicherheitsberatung: CanCERT stellt Informationen über Verwundbarkeiten und Schutzzmöglichkeiten und –werkzeuge zur Verfügung.
X	Empfehlung von allgemeinen Massnahmen zur Vorsorge und Schadensverhütung	<ul style="list-style-type: none"> • Sicherheitskoordination: Kunden erhalten Unterstützung beim Aufbau der Kommunikation mit Behörden, weiteren Dienststellen, CanCERT-Kunden oder Experten zur Lösung von IT-Sicherheitsproblemen. • Sammlung, Analyse und Statistikmeldungen von kanadischen IT-Sicherheitsvorkommnissen
	Produkte-Evaluation und Empfehlungen für Firewalls, Virenschutz etc.	
X	Publikationen	<ul style="list-style-type: none"> • Publikation: CanCERT Bulletin (5 Ausgaben/Jahr)

X	Individuelle Beratung bei Vorfällen	<ul style="list-style-type: none"> • Individuelle Dienstleistungen für CanCERT-Kunden: <ul style="list-style-type: none"> - Zugeschnittener Beratungsservice - Auskunftsdienst für Nachfragen bezüglich IT-Sicherheit - Seminare zur Sicherheit in Netzwerken (Bewusstsein) - Überprüfung der Sicherheitseinstellungen und –konfigurationen - „Einbruchversuche“ - Netzwerk-Monitoring • „Intrusion Detection Training“ : Trainingskurse zum Erlernen der Grundkenntnisse und –techniken zum Entdecken von System-Einbrüchen
X	Hilfestellungen technischer Art (Bereitstellen von Patches oder Recovery-Programmen,...)	<ul style="list-style-type: none"> • Beschränkte Einsätze bei Zwischenfällen für kanadische Regierungsstellen, Unternehmen und akademische Organisationen
	Weitere Aufgaben	
Struktur und organisatorische Einbettung		Keine Angaben
Anzahl Personen		Keine Angaben
Operationsmodus		„Incident Response Service“ (24h, 7 Tage/Woche im Einsatz)

Australian Computer Emergency Response Team (Australien)

Das australische CERT bietet eine Anlaufstelle für alle Internetnetbenutzer in Fragen der Informationssicherheit. Ziel ist die Reduktion der Wahrscheinlichkeit eines erfolgreichen Angriffs, die Reduktion der Kosten für die Sicherheitsmassnahmen und die Senkung der Risiken mit bedeutenden Folgeschäden. Das AusCERT ist Mitglied des FIRST.

Das AusCERT hat den Auftrag, das Bewusstsein und die Informationen bezüglich IT-Sicherheit sowohl lokal als auch international zu verbessern, und will sich als führende zuverlässige und unabhängige Informationsquelle zur IT-Sicherheit etablieren.

Australian Computer Emergency Response Team (http://www.auscert.org.au , Thinking about the Unthinkable: Australien Vulnerabilites to High-Tech Risks, 29 Juni 1998)		
Aufgaben und Produkte		
X	Warnungen/Alarmierung	<ul style="list-style-type: none"> AusCERT erleichtert die Kommunikation zwischen betroffenen Kunden, gibt Ratschläge und Informationen weiter Incident Response (24h, 7 Tage / Woche)
	Statusmeldungen	
X	Lagebeurteilungen und Handlungsempfehlungen	<ul style="list-style-type: none"> AusCERT koordiniert weiter Informationsflüsse zwischen betroffenen Kunden und ausländischen „Incident Response Teams“, Verkäufer, Mitgliedern und Strafverfolgungsbehörden.
X	Empfehlung von Sofortmassnahmen zur Schadensverhütung	<ul style="list-style-type: none"> Sicherheitsinformationen können übers Web oder einen FTP-Server abgefragt werden.
X	Empfehlung von allgemeinen Massnahmen zur Vorsorge und Schadensverhütung	<ul style="list-style-type: none"> Forschung auf politische Ebene: Schutz der nationalen Informationsinfrastrukturen, die Auswirkungen des Y2K in bezug auf die Sicherheit, die Auswirkungen von „Melissa“ oder „The Love Bug“ auf die Wirtschaftstätigkeit, Beteiligung an der Debatte zur Copyright-Reform in Australien und ihr Einfluss auf die IT-Sicherheitsindustrie.
X	Produkte-Evaluation und Empfehlungen für Firewalls, Virenschutz etc.	<ul style="list-style-type: none"> Forschung auf technische Ebene: Analyse von Software-Verwundbarkeiten von Betriebssystemen, Applikationen und Netzwerksoftware sowie von Einbruchswerkzeugen; Beratung des Handels und von Kunden.
X	Publikationen	<ul style="list-style-type: none"> Hinweise, Sicherheitswarnungen, Newsletter-Artikel, Berichte und Überblicke. Alle Publikationen werden den Kunden zur Verfügung gestellt und der Öffentlichkeit entweder gegen Zahlung oder zu einem späteren Zeitpunkt zugänglich gemacht, sofern sie nicht als „Community Service“ veröffentlicht werden.

X	Individuelle Beratung bei Vorfällen	<ul style="list-style-type: none"> Community Services: Sämtliche Einzelpersonen und Organisationen können um Unterstützung nachfragen, allerdings haben die Bedürfnisse der Kunden Priorität.
	Hilfestellungen technischer Art (Bereitstellen von Patches oder Recovery-Programmen,...)	
X	Weitere Aufgaben	<ul style="list-style-type: none"> Training und Ausbildung <ul style="list-style-type: none"> Entwicklung und Präsentation von Kursen für IT-Berufstätige, Entscheidungsträger und weitere Berufstätige. Aufbau weiterer „Computer Security Incident Response Teams“ (CSIRTs) weltweit
	Struktur und organisatorische Einbettung	<ul style="list-style-type: none"> Einsatzfähiger Arm der University of Queensland Finanziert v.a. durch Mitgliederbeiträge sowie durch Forschung und Ausbildung.
	Anzahl Personen	Keine Angaben
	Operationsmodus	Incident Response (24h, 7 Tage / Woche):

A3 Fragebogen Sonderstab Informationssicherheit

1. Welches ist nach ihrer Meinung das generelle Einsatzspektrum des Sonderstabes?

Grau hinterlegt sind Ausprägungen von Kriterien, die unserer Meinung nach in das generelle Einsatzspektrum des Sonderstabes fallen. Bitte markieren Sie Ihre Sichtweise, beispielsweise durch Umrandung der entsprechenden Felder. Weitere Kriterien können am unteren Ende der Tabelle ergänzt werden.

Kriterium	Kleines Ausmass	Mittleres Ausmass	Grosses Ausmass
Betroffene Stelle Verwaltung	Einzelnes Bundesamt	Mehrere Bundesämter Ein Departement	Mehrere Departemente
Betroffene Stelle Wirtschaft	Einzelnes Unternehmen	Mehrere Unternehmen Ein Sektor (z.B. Transport)	Flächendeckend viele Unternehmen
Wirkung / Ausmass	Primäre Funktionen ¹⁾ der Schweiz sind nicht betroffen. Sekundäre Funktionen ²⁾ der Schweiz sind betroffen.	Primäre Funktionen der Schweiz sind betroffen, können aber aufrecht erhalten werden.	Primäre Funktionen der Schweiz fallen aus.
Vorwarnzeit	> 3 Tage	> 1/2 Tag	≤ 1/2 Tag
Wahrnehmung bei der Bevölkerung	Insider, Fachspezialisten	Einige	Grossteil der Bevölkerung
Berichterstattung in den Medien	Klein Unwichtige Meldungen	Mittel Wichtige Meldungen	Gross Schlagzeilen
Motiv bei einer vorsätzlichen Handlung I	Persönlich	Wirtschaftlich Politisch	Militärisch
Motiv bei einer vorsätzlichen Handlung II	Vandalismus (pers.)	Industriespionage Propaganda Direkte Schädigung	Information Warfare ³⁾ Information Dominance Nachrichtendienstliche Aktivitäten
Angreifer bei vorsätzlicher Handlung	Einzelner Gruppe	Organisation	Staat
Vorfälle, Ereignisse im Ausland	Lokal isolierte Einzelfälle	Potential für Auswirkungen bis in die Schweiz	Weltweite Betroffenheit
...			

1) Primäre Funktionen sind lebenswichtige Funktionen wie die Energieversorgung, die Wasserversorgung, die Telekommunikation, der öffentlicher Verkehr und das Rettungswesen

2) Sekundäre Funktionen: alle anderen

3) Im Fall von Information Warfare und Information Dominance liegt die Hauptverantwortung beim VBS. Der Sonderstab Informationssicherheit arbeitet eng mit den entsprechenden Stellen zusammen.

2. Welche Kompetenzen hat der Sonderstab in einer Krise?

Diese Frage sollte abhängig vom Ausmass der Krise beantwortet werden. Es wird definiert:

Krisenausmass	Beschreibung
<i>Klein</i>	<i>Primäre Funktionen der Schweiz sind nicht betroffen. Sekundäre Funktionen der Schweiz sind betroffen.</i>
<i>Mittel</i>	<i>Primäre Funktionen der Schweiz sind (teilweise) betroffen, können aber aufrecht erhalten werden.</i>
<i>Gross</i>	<i>Primäre Funktionen der Schweiz fallen aus.</i>
Kompetenzen	Beschreibung
<i>Alarmierung</i>	<i>Der Sonderstab alarmiert und informiert die Verwaltung, die Wirtschaft oder die Bevölkerung.</i>
<i>Empfehlung</i>	<i>Der Sonderstab gibt Empfehlungen an die Verwaltung, die Wirtschaft oder die Bevölkerung ab.</i>
<i>Weisung</i>	<i>Der Sonderstab formuliert verbindliche Weisungen an die Verwaltung, die Wirtschaft oder die Bevölkerung. Voraussetzung für eine Weisung ist eine entsprechende Rechtsgrundlage.</i>

Unser Vorschlag ist jeweils grau hinterlegt. Bitte kreuzen Sie die entsprechenden Felder an. Weitere gewünschte oder notwendige Kompetenzen können ergänzt werden.

Empfänger der Resultate	Ausmass der Krise		
	Klein	Mittel	Gross
Verwaltung oder staatliche Betreiber und Anbieter von primären Funktionen	<input type="checkbox"/> Alarmierung <input type="checkbox"/> Empfehlung <input type="checkbox"/> Weisung <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> Alarmierung <input type="checkbox"/> Empfehlung <input type="checkbox"/> Weisung <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> Alarmierung <input type="checkbox"/> Empfehlung <input type="checkbox"/> Weisung <input type="checkbox"/> <input type="checkbox"/>
Privatrechtliche Betreiber und Anbieter von primären Funktionen ⁴⁾	<input type="checkbox"/> Alarmierung <input type="checkbox"/> Empfehlung <input type="checkbox"/> Weisung <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> Alarmierung <input type="checkbox"/> Empfehlung <input type="checkbox"/> Weisung <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> Alarmierung <input type="checkbox"/> Empfehlung <input type="checkbox"/> Weisung <input type="checkbox"/> <input type="checkbox"/>
Bevölkerung / Wirtschaftsbetriebe	<input type="checkbox"/> Alarmierung <input type="checkbox"/> Empfehlung <input type="checkbox"/> Weisung <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> Alarmierung <input type="checkbox"/> Empfehlung <input type="checkbox"/> Weisung <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> Alarmierung <input type="checkbox"/> Empfehlung <input type="checkbox"/> Weisung <input type="checkbox"/> <input type="checkbox"/>

4) Beispielsweise Telekom-Anbieter, private Energielieferanten, etc.

3. Wo sehen Sie die Aufgabenschwerpunkte des Sonderstabes vor der Krise, in der Krise und nach der Krise?

In der ersten Spalte der Tabelle sind die Krisenphasen aufgeführt. In der zweiten Spalte der Tabelle sind mögliche Aufgaben für den Sonderstab aufgeführt.

Bitte kreuzen Sie an: ja = Schwerpunkt; nein = Kein Schwerpunkt. Formulieren Sie bitte in der Spalte ganz rechts, was der Sonderstab genau zu tun hat oder wer allenfalls diese Aufgabe übernimmt. Schwerpunkte können in der Tabelle ergänzt werden. Grau hinterlegt sind die Vorschläge des Projektteams.

	Aufgabe	ja	nein	Falls ja: was hat der Sonderstab zu tun? Falls nein: wer übernimmt diese Aufgabe?
Vor der Krise	Früherkennung und Warnung	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	Vorsorgliche Massnahmen zur Führung in der Krise	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	Vorsorgliche Massnahmen zur Krisenprävention	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	Ausbildung, Training, Controlling	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	Information und Kommunikation zur aktuellen Situation	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	...	<input type="checkbox"/>	<input type="checkbox"/>	
	...	<input type="checkbox"/>	<input type="checkbox"/>	
In der Krise	Information und Kommunikation (Grundlagen für die Bundeskanzlei)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	Führungsorganisation	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	Nachrichten und Informationsbeschaffung	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

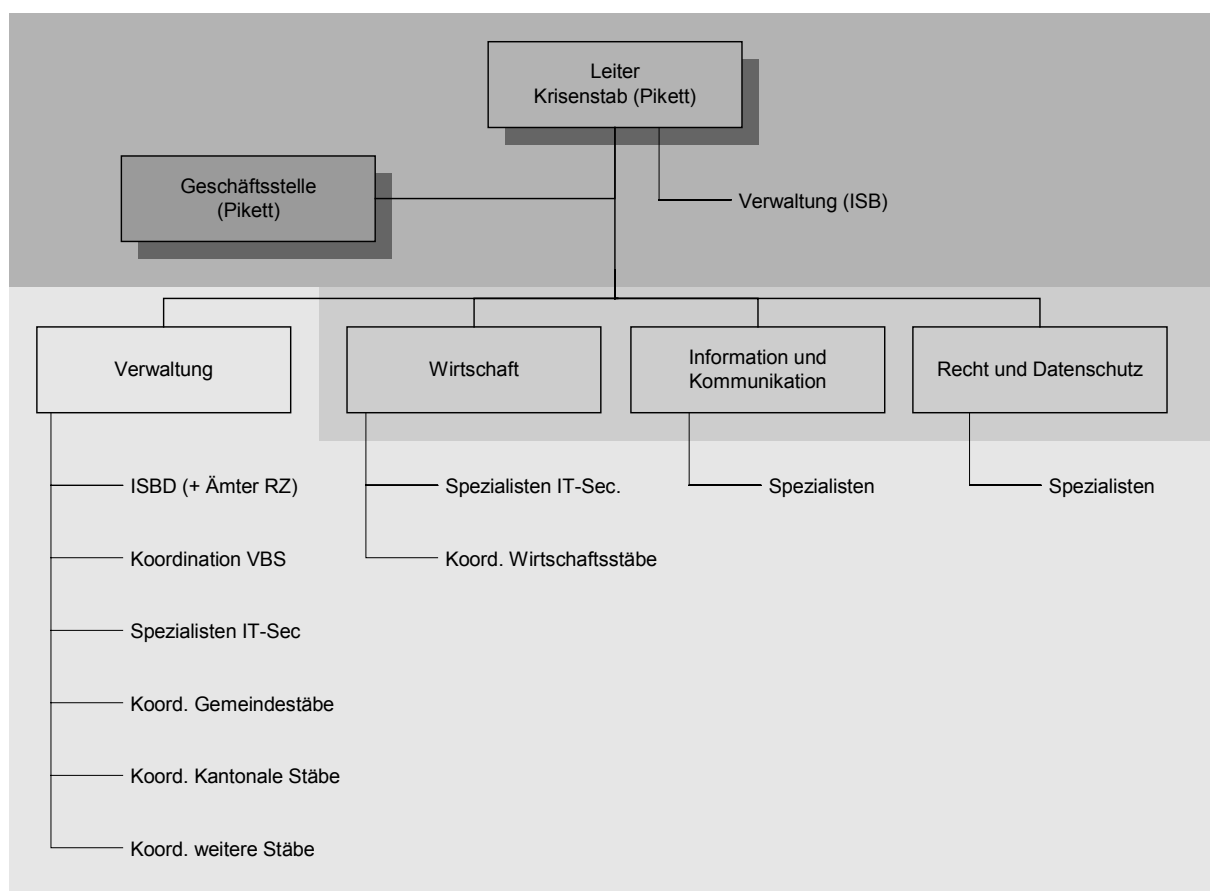
	Aufgabe	ja	nein	Falls ja: was hat der Sonderstab zu tun? Falls nein: wer übernimmt diese Aufgabe?
In der Krise	Krisenproblem erfassen	<input type="checkbox"/>	<input type="checkbox"/>	
	Krisenproblem lösen	<input type="checkbox"/>	<input type="checkbox"/>	
	Entschlussfassung und Entscheid	<input type="checkbox"/>	<input type="checkbox"/>	
	Umsetzung und Vollzug der Entscheidung	<input type="checkbox"/>	<input type="checkbox"/>	
	...	<input type="checkbox"/>	<input type="checkbox"/>	
	...	<input type="checkbox"/>	<input type="checkbox"/>	
Nach der Krise	Krisenaustritt und Genesung	<input type="checkbox"/>	<input type="checkbox"/>	
	Evaluation der Führung in der Krise	<input type="checkbox"/>	<input type="checkbox"/>	
	Umsetzung der Erkenntnisse in Lehren "Lessons learned"	<input type="checkbox"/>	<input type="checkbox"/>	
	...	<input type="checkbox"/>	<input type="checkbox"/>	
	...	<input type="checkbox"/>	<input type="checkbox"/>	

4. Aus welchen Organisationselementen muss sich der Sonderstab zusammensetzen?

Die folgende Abbildung zeigt einen Vorschlag für die Zusammensetzung des Sonderstabes. Die Tabelle auf der nächsten Seite beschreibt die verschiedenen Organisationselemente.

Sonderstab Informationssicherheit

16 November, 2000



In der ersten Spalte sind die vorgeschlagenen Organisationselemente aufgeführt. In der zweiten Spalte finden Sie unseren Vorschlag für deren Beschreibung und Aufgaben. Bitte formulieren Sie Ihre Ergänzungsvorschläge in der dritten Spalte. Am unteren Ende der Tabelle können weitere Organisationselemente ergänzt werden.

Element	Beschreibung / Aufgaben	Änderungsvorschläge
Geschäftsstelle bzw. Pikettorganisation	<p>Die Geschäftsstelle ist eine Einheit (eine bis zwei Personen), die im Sinn einer Pikettorganisation rund um die Uhr erreichbar sind.</p> <p>Ihre Hauptaufgaben:</p> <ul style="list-style-type: none"> • Verantwortlich für alle administrativen Aufgaben des Sonderstabes • Ansprechpartner für alle Fragen im Zusammenhang mit dem Sonderstab • Laufende Analyse der Situation vor der Krise; Zusammenarbeit mit einer Alarmzentrale (z.B. NAZ, CERT, FIRST) und gebietsverwandten Geschäftsstellen • Administrative Koordination im Krisenfall • Ausbildung • Evtl. Einberufung der Leitung Krisenstab im Bedarfsfall 	
Leitung Krisenstab	<p>Die Leitung des Krisenstabes übernimmt nach Einberufung des Kernstabes die operative Leitung.</p> <p>Sie besteht aus:</p> <ul style="list-style-type: none"> • Leiter Krisenstab • Zwei Personen des ISB (Leitung der Geschäftsstelle und 2. Person) <p>Die Leitung Krisenstab entscheidet über die Einberufung des Kernstabes.</p>	
Kernstab	<p>Der Kernstab besteht aus der Leitung Krisenstab und zusätzlich folgenden Bereichen (je nach Bedarf):</p> <ul style="list-style-type: none"> • Wirtschaft <ul style="list-style-type: none"> – Ein Vertreter Energie – Ein Vertreter Telekommunikation – Ein Vertreter Wasserversorgung – Ein Vertreter Transportwesen – Ein Vertreter Banken / Finanzen • Information und Kommunikation (zuhanden der Bundeskanzlei) • Recht und Datenschutz (evtl. Eidg. Datenschutzbeauftragter) <p>Der Kernstab entscheidet über die Einberufung des erweiterten Stabes (ganz oder teilweise).</p>	

Element	Beschreibung / Aufgaben	Änderungsvorschläge
Erweiterter Stab	<p>Der erweiterte Stab besteht aus dem Kernstab und zusätzlich folgenden Bereichen (je nach Bedarf):</p> <ul style="list-style-type: none"> • Verwaltung <ul style="list-style-type: none"> – Die ISBD der betroffenen Departemente + Vertreter Ämter RZ – Koordination VBS – Spezialisten IT-Sec – Koordination Gemeindestäbe – Koordination Kantonale Stäbe – Koordination weitere Stäbe, z.B. Milizamt BWL (Amt I+K) • Wirtschaft <ul style="list-style-type: none"> – Spezialisten IT-Sec – Koordination Wirtschaftsstäbe (kann durch die Vertreter im Kernstab übernommen werden) • Information und Kommunikation <ul style="list-style-type: none"> – Spezialisten • Recht und Datenschutz <ul style="list-style-type: none"> – Spezialisten 	
...		
...		
...		

5. Wie soll der Sonderstab organisiert sein?

In der ersten Spalte ist das jeweilige Ausmass der Krise aufgeführt. In der zweiten Spalte finden Sie unseren Vorschlag für die Organisation des Sonderstabes, bezogen auf das Ausmass der Krise. Bitte formulieren Sie Ihre Ergänzungsvorschläge in der dritten Spalte. Am Ende der Tabelle können weitere Varianten ergänzt werden. Unten auf der Seite finden Sie eine grafische Übersicht.

Ausmass Krise	Organisation (Vorschlag)	Änderungsvorschläge
Keine Krise	Geschäftsstelle, rund um die Uhr erreichbar	
Ab Potential für eine kleine Krise	Leitung Krisenstab <ul style="list-style-type: none"> • Einberufen durch Geschäftsstelle oder durch Externe • Geschäftsstelle rund um die Uhr besetzt 	
Ab Potential für eine mittlere Krise	Kernstab <ul style="list-style-type: none"> • Durch Leitung Krisenstab einberufen • Personelle Zusammensetzung je nach Bedarf 	
Ab Potential für eine grosse Krise	Erweiterter Stab = Vollorganisation <ul style="list-style-type: none"> • Durch Leitung Krisenstab einberufen • Personelle Zusammensetzung je nach Bedarf 	
...		

Grafische Übersicht:

Ausmass	Keine Krise		Kleine Krise		Mittlere Krise		Grosse Krise
Potential		Potential für eine kleine Krise		Potential für eine mittlere Krise		Potential für eine grosse Krise	
Organisation	Geschäftsstelle	Leitung Krisenstab	Kernstab		Erweiterter Stab		

6. Durch wen muss die Leitung Krisenstab einberufen werden?

Während das Aufbieten der einzelnen Stabselemente situationsgerecht durch die Leitung Krisenstab erfolgt, sollten gewisse Grundsätze für das Aufbieten der Leitung Krisenstab festgelegt werden.

Bitte kreuzen Sie an. Am unteren Ende der Tabelle können weitere Varianten ergänzt werden. Mehrfachnennungen sind möglich.

<input type="checkbox"/>	Wenn die laufende Analyse der Lage durch die Geschäftsstelle eine Einberufung als sinnvoll erachtet.
<input type="checkbox"/>	Durch den Leiter Krisenstab selbst
<input type="checkbox"/>	Durch das ISB (Vertreter Sonderstab)
<input type="checkbox"/>	Auf Verlangen der ISBD
<input type="checkbox"/>	Auf Verlangen des Bundesrates
<input type="checkbox"/>	Auf Verlangen der Bundeskanzlei
<input type="checkbox"/>	Auf Verlangen von Direktoren von Bundesämtern
<input type="checkbox"/>	Aufgrund von Anfragen aus der Wirtschaft
<input type="checkbox"/>	Aufgrund von Anfragen aus der Bevölkerung
<input type="checkbox"/>	...
<input type="checkbox"/>	...
<input type="checkbox"/>	...

7. In welcher Form muss der Sonderstab mit anderen Organen zusammenarbeiten?

In der ersten Spalte sind die Organe aufgeführt. In der zweiten Spalte finden Sie unseren Vorschlag für die Zusammenarbeit. Bitte formulieren Sie Ihre Ergänzungsvorschläge in der dritten Spalte. Am unteren Ende der Tabelle können weitere Organe ergänzt werden.

Organ	Beschreibung Zusammenarbeit	Änderungsvorschläge
Milizamt BWL (Amt für I+K)	<ul style="list-style-type: none"> Gegenseitige Information Koordination der Aktivitäten im erweiterten Stab (Verwaltung; Weitere Stäbe) 	
Stiftung InfoSurance	<ul style="list-style-type: none"> Gegenseitige Information Koordination der Aktivitäten im erweiterten Stab (Wirtschaft; Wirtschaftsstäbe) 	
Nationale Alarmzentrale NAZ	Wünschenswert wäre eine Erweiterung der Aufgabenbereiche der NAZ, so dass diese Aktivitäten im Bereich KASII ⁵⁾ überwachen und Meldungen an die Geschäftsstelle weitergeben könnte. Alarmierung der Bevölkerung?	
ISB	Ist in der Leitung Krisenstab vertreten	
ISBD	<ul style="list-style-type: none"> Gegenseitige Information Sind Teil des erweiterten Stabes (Verwaltung; ISBD) 	
BAKOM	Gegenseitige Information	
KIG	Gegenseitige Information	
VBS	<ul style="list-style-type: none"> Gegenseitige Information Sind im erweiterten Stab (Verwaltung; Koordination VBS) vertreten Enger Kontakt zu AIOS 	
BAP	<ul style="list-style-type: none"> Gegenseitige Information Enge Zusammenarbeit, falls die KASII in den Bereich der BAP fällt (vorsätzliche Handlung, kriminelle Aktivität, etc.) 	

5) KASII ist die Abkürzung für *Krisen, ausgelöst durch Störungen in der Informationsinfrastruktur*

Organ	Beschreibung Zusammenarbeit	Änderungsvorschläge
Grossfirmen aus der Wirtschaft	<ul style="list-style-type: none"> • Gegenseitige Information • Dienen als ständige Sensoren • Sind im Kernstab (Wirtschaft) vertreten • Koordination der Aktivitäten über Wirtschaft; Koordination Wirtschaftsstäbe 	
Krisenstäbe der Kantone	<ul style="list-style-type: none"> • Gegenseitige Information • Koordination der Aktivitäten über Verwaltung; Koordination Gemeindestäbe 	
Krisenstäbe der Gemeinden	<ul style="list-style-type: none"> • Gegenseitige Information • Koordination der Aktivitäten über Verwaltung; Koordination kantonale Stäbe 	
Krisenstäbe aus dem Ausland	<ul style="list-style-type: none"> • Gegenseitige Information • Koordination der Aktivitäten über Verwaltung; Koordination weitere Stäbe 	
Verbände in der Schweiz (FGSec, ISACA)	Gegenseitige Information	
CERT/ CC, CERT-BSI, FIRST, FedCIRC, NIPC (USA), etc.	<ul style="list-style-type: none"> • Regelmässige Auswertung der Informationen durch die Geschäftsstelle (evtl. in Zusammenarbeit mit der Stiftung InfoSurance) • Anstreben einer institutionalisierten Zusammenarbeit 	
...		
...		

8. Welche Mittel müssen dem Stab zur Verfügung stehen?

In der ersten Spalte sind die Mittel aufgeführt. In der zweiten Spalte finden Sie unseren Vorschlag für deren Beschreibung. Bitte formulieren Sie Ihre Ergänzungsvorschläge in der dritten Spalte. Am unteren Ende der Tabelle können weitere Mittel ergänzt werden.

Mittel	Beschreibung	Änderungsvorschläge
Personelle Mittel	<ul style="list-style-type: none"> • Ca. 1.5-Stellen für die Geschäftsstelle • 3-5 (inkl. Vertretungen) Personen für die Leitung Krisenstab • Zusätzlich 6 -9 (inkl. Vertretungen) Personen für den Kernstab • Zusätzlich ca. 20-30 Personen (inkl. Vertretungen) für den erweiterten Stab 	
Finanzielle Mittel	Das EFD, ISB stellt die notwendigen Mittel für den Betrieb der Geschäftsstelle.	
Räumlichkeiten	<ul style="list-style-type: none"> • Permanente Räumlichkeiten für die Geschäftsstelle • Weitere Räumlichkeiten im Bedarfsfall • Das EFD ist für den Unterhalt der Räumlichkeiten und Einrichtungen verantwortlich. 	
EDV		
Methoden / Werkzeuge		
...		
...		
...		

9. Müssen Empfehlungen des Sonderstabes mit einem "Legal Disclaimer" versehen werden?

<input type="checkbox"/> Ja	<input type="checkbox"/> Nein	Begründung
-----------------------------	-------------------------------	---------------------------------------

10. Kann der Sonderstab für fehlende oder falsche Warnungen oder Empfehlungen haftbar gemacht werden?

<input type="checkbox"/> Ja	<input type="checkbox"/> Nein	Begründung
-----------------------------	-------------------------------	---------------------------------------

11. Muss der Sonderstab selbst finanzielle Rückstellungen tätigen? Wenn ja, für welchen Zweck?

<input type="checkbox"/> Ja	<input type="checkbox"/> Nein	Falls ja, Zweck
-----------------------------	-------------------------------	--

12. Soll der Sonderstab über Verträge Leistungen aus der Wirtschaft im Krisenfall sicherstellen?

<input type="checkbox"/> Ja	<input type="checkbox"/> Nein	Begründung
-----------------------------	-------------------------------	---------------------------------------

13. Wer könnte substantielle Beiträge zum Aufbau des Sonderstabes leisten? Bitte nennen Sie hier nur Personen mit einschlägiger Erfahrung im Bereich Krisenmanagement, vorzugsweise im IT-Bereich.

Person Name, Vorname, Funktion Organisation)	Fachgebiet Erfahrungen

Verteiler

Der Fragebogen zum Sonderstab Informationssicherheit (November 2000) richtete sich an die folgenden Personen:

- Kurt Häring Stiftung InfoSurance
- Peter Fischer Bundesamt für Kommunikation
- Matthias Ramsauer Bundesamt für Kommunikation
- Hans-Peter Nägeli UBS AG, IT Business Services
- Hanspeter Lingg sunrise communications AG
- Anton Lagger Bundesamt für wirtschaftl. Landesversorgung
- Peter Genkinger Novartis International AG
- Rolf Schatzmann Sicherheitsdienst der Bundesverwaltung
- Thomas Köppel Bundespolizei, Sektion Auswertung
- Urs Freiburghaus Generalstab, Untergruppe Planung AIOS
- Dr. Michel Dufour Gruppe Rüstung
- René Favre Swiss Re
- Tobias Muster Swiss Re
- Dr. Jürg Römer Informatikstrategieorgan Bund
- Marcel Frauenknecht Informatikstrategieorgan Bund
- Dr. Ruedi Rytz Informatikstrategieorgan Bund
- A. Hardmeier Nationale Alarmzentrale
- Frank W. Felzmann CERT Deutschland
- Prof. Dr. B. Hämmerli HTA Luzern
- Pius Ziegler HTA Luzern

A4 Fragebogen für ausländische Melde- und Analysestellen

FRAGEBOGEN ZUR MELDE- und ANALYSESTELLE INFORMATIONSSICHERHEIT SCHWEIZ

Rücksendung

Bitte schicken Sie diesen Fragebogen bis zum **7. September 2001** zurück an:

Ernst Basler + Partner AG
Herr Matthias Holenstein
Zollikerstrasse 65
CH-8702 Zollikon
Schweiz
Telefon ++41 1 395 12 71 oder ++41 1 395 11 11

Angaben zur Person

Name:.....

Funktion:.....

Organisationseinheit / Unternehmen:

Ort, Datum:

Hinweis zur Verwendung der Antworten

Falls gewünscht, werden die Antworten vertraulich behandelt. Bitte machen Sie einen entsprechenden Hinweis. Im Übrigen wird eine offene Informationspolitik verfolgt.

Einleitung

Der Schutz von kritischen Informationsinfrastrukturen für die Wirtschaft und Verwaltung ist weitgehend unbestritten und wurde an den strategischen Führungsübungen 1997 und 2001 sowie im sicherheitspolitischen Bericht 2000 klar bestätigt. Der Schweizerische Bundesrat hat zudem mit der Unterstützung der Stiftung InfoSurance die Bedeutung des Themas Informationssicherheit unterstrichen. Als Massnahme zur Gewährleistung der Aktionsfähigkeit der Schweizerischen Bundesverwaltung in Krisensituationen erarbeitete das Informatikstrategieorgan Bund (ISB) ein Konzept für einen Sonderstab „Informationssicherheit“. Das Konzept beschreibt Auftrag und Einsatz des Sonderstabes sowie die Aufbau- und Ablauforganisation. Der Sonderstab soll die Lagebeurteilung für die strategische Führung in Krisensituationen wahrnehmen.

Als zentrales Element des Konzepts Sonderstab Informationssicherheit wurde in verschiedenen Gesprächen und insbesondere im Rahmen der strategischen Führungsübung INFORMO 2001 die Schaffung einer permanenten Melde- und Analysestelle genannt. Diese Melde- und Analysestelle soll über ein breit gefächertes Sensorennetz verfügen, um möglichst viele relevante Informationen in möglichst kurzer Zeit sammeln und auswerten zu können. Dies bedingt, dass Kontakte zu Betreibern von IT-Systemen in der Wirtschaft und der Verwaltung sowie anderen in- und ausländischen Warnstellen etabliert sind. Die Melde- und Analysestelle soll somit den Zweck erfüllen, die bereits bestehenden Einzelinitiativen zu koordinieren und aus den bestehenden Informationsquellen und –netzwerken die für die Informationssicherheit relevanten Meldungen klar zu identifizieren und nach ihrer Bedeutung einzuteilen. Diese Stelle soll im Ereignisfall im direkten Kontakt zum Sonderstab stehen und diesen mit Meldungen zu den neusten Entwicklungen versorgen.

Im vorliegenden Fragebogen sind wesentliche Punkte für die Konzeption einer Melde- und Analysestelle Informationssicherheit enthalten. Der Fragebogen richtet sich an bestehende Institutionen mit einem vergleichbaren Aufgabenspektrum oder ähnlichen Prozessen (CERTs, Meldestellen, Lagezentren, Koordinationsbüros etc.). Bestehendes Know-how und Erfahrungen der Befragten sollen helfen, die Melde- und Analysestelle Informationssicherheit Schweiz bestmöglich zu konzipieren. Auch Hinweise, welche über die gestellten Fragen hinausgehen, werden gerne berücksichtigt.

Besten Dank für Ihre Unterstützung!

15. Welche Aufgaben hat Ihre Stelle?

Bitte markieren und ergänzen Sie die zutreffenden Stichworte. Bei Bedarf bitte Rückseite oder Beiblatt verwenden.

Stichwort	Bemerkungen
<input type="checkbox"/> Meldungen sammeln	
<input type="checkbox"/> Meldungen bewerten	
<input type="checkbox"/> Lagebeurteilung	
<input type="checkbox"/> Eigene Recherchen durchführen	
<input type="checkbox"/> Alarmierung von IT-Administratoren	
<input type="checkbox"/> Aufbieten weiterer Einsatzorgane oder –mittel (z.B. technische Analysestellen, Strafverfolgungsbehörden,	
<input type="checkbox"/> Kontakte zu anderen Melde- und Analysestellen sicherstellen	
<input type="checkbox"/> Grundlagenforschung	
<input type="checkbox"/> Sensibilisierung	
<input type="checkbox"/> Schulung	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	

16. Welches sind die Produkte und Leistungen Ihrer Stelle?

Unter „Beschreibung“ können zusätzliche Ergänzungen zu den angebotenen Produkte angefügt werden.

Produkte	Beschreibung
<input type="checkbox"/> Lagedarstellung (Virenaktivität, Hacking-Attacken, Netzbelastungen wichtiger Netze,...)	
<input type="checkbox"/> Produkte-Evaluation und Empfehlungen (z.B. Einsatz Firewalls, Virenschutz, ...)	
<input type="checkbox"/> Publikationen (wissenschaftl. Berichte, Newsletter, Tagesberichte,...)	
<input type="checkbox"/> Individuelle Beratung bei Vorfällen/Sorgentelefon (Bitte Art der Beratung angeben)	
<input type="checkbox"/> Hilfestellungen technischer Art (z.B. Bereitstellen von Patches oder Recovery Programmen,...)	
<input type="checkbox"/> ...	
<input type="checkbox"/> ...	
<input type="checkbox"/> ...	

17. Welches sind Ihre Kunden?

Unter „Beschreibung“ können zusätzliche Ergänzungen zur Kundengruppe angefügt werden.

Kunden	Beschreibung
<input type="checkbox"/> Verwaltungsstellen national	
<input type="checkbox"/> Verwaltungsstellen regional	
<input type="checkbox"/> Einzelunternehmen (kleine und mittlere Betriebe)	
<input type="checkbox"/> Einzelunternehmen (Grossbetriebe)	
<input type="checkbox"/> Wirtschaftsverbände	
<input type="checkbox"/> Einzelne Fachexperten	
<input type="checkbox"/> Produktheersteller	
<input type="checkbox"/> Bevölkerung	
<input type="checkbox"/> Öffentliche Diskussionsforen z.B. Newsgroups	
<input type="checkbox"/> Ausländische Stellen	
<input type="checkbox"/> ...	
<input type="checkbox"/> ...	

18. Wie gelangen Sie zu Informationen/Meldungen?

Mit welchen Partnern wird zusammengearbeitet? Bestehen offizielle Netzwerke mit Partnern oder handelt es sich eher um informelle resp. individuelle Kontakte?

Informationslieferanten	Art der Meldungen	Beschreibung
<input type="checkbox"/> Eigene Recherchen (Internet, Journals, Medien, Direktkontakte,...)		
<input type="checkbox"/> Andere Meldestelle (CERTS,...)		
<input type="checkbox"/> Produkthanbieter (Anti-Viren-Programme, SW/HW,...)		
<input type="checkbox"/> Nachrichtendienstliche Stellen		
<input type="checkbox"/> Meldungen von Unternehmen		
<input type="checkbox"/> Meldungen von Privatpersonen		
<input type="checkbox"/> ...		
<input type="checkbox"/> ...		

19. Wie werden eingehende Informationen/Meldungen verifiziert?

Werden den Meldungen/Informationen bestimmte Qualitätsattribute mitgegeben?

Informationen/Meldungen werden verifiziert durch:	Kommentar:
<input type="checkbox"/> Nachrichtendienstliche Stellen	
<input type="checkbox"/> Zusammenarbeit mit Polizeistellen	
<input type="checkbox"/> Zusammenarbeit mit Stellen der militärischen Verteidigung	
<input type="checkbox"/> Medienmitteilungen	
<input type="checkbox"/> Vergleiche mit anderen Meldungen	
<input type="checkbox"/> Andere Meldestelle (CERTS,...)	
<input type="checkbox"/> Produkthanbieter (Anti-Viren-Programme, SW/HW,...)	
<input type="checkbox"/> ...	

20. Wie sind Sie organisiert?

a) Welcher Stelle sind Sie zugeordnet? Gibt es bei Vorfällen weitere Organe, welche Sie unterstützen?

.....
.....
.....
.....
.....

b) Wie sind Sie intern organisiert (Aufgabenzuteilung, Rund-um-die-Uhr-Betrieb?, Schichten,...)

.....
.....
.....
.....
.....

c) Gibt es Schwellenwerte für bestimmte Aktivitäten (z.B. zur Alarmierung)?

.....
.....
.....
.....
.....
.....
.....
.....

d) Welche konkrete Aufgaben haben Sie im Ereignisfall?

.....
.....
.....
.....
.....
.....

e) Wo sehen sie den grössten Anpassungsbedarf für ihre Stelle? (Rechtliche Grundlagen, Partner für Zusammenarbeit, Mittel, Breitenwirkung,...)

.....

.....

.....

.....

.....

.....

.....

21. Welche Mittel stehen Ihnen zur Verfügung?

Mittel	Beschreibung	Anzahl/Betrag	Bemerkungen
Personelle Mittel	<ul style="list-style-type: none">• Leitung/Führung• Funktionen• Ausbildung		
Finanzielle Mittel	<ul style="list-style-type: none">• Budget (Höhe)• Wer trägt die Kosten?		
Räumlichkeiten	<ul style="list-style-type: none">• Einrichtungen• Geschützte Infrastruktur		
EDV und Telekommunikation (Verbindungen)	<ul style="list-style-type: none">• Spezielle Systeme• Lagedarstellungen• Datenbank zur Erfassung von Ereignissen• Geschützte Infrastruktur		
Weitere Mittel			

Verteiler

Der Fragebogen für ausländische Melde- und Analysestellen (20. August 2001) richtete sich an die folgenden Institutionen:

- Abteilung für Rettungswesen, Innenministerium, Helsinki/Finnland
- Bundesamt für Polizeiwesen, Dienst für Analyse und Prävention, Bern/Schweiz
- CanCERT™, Ottawa/Kanada
- Computer Emergency Response Team im Bundesamt für Sicherheit in der Informationstechnik, Bonn/Deutschland
- FIRST, Mountain View/USA
- National Infrastructure Protection Center, USA
- Unified Incident Reporting and Alert Scheme, London/England

A5 Fragebogen Kundenbedürfnisse einer Melde- und Analysestelle

Rücksendung

Bitte schicken Sie diesen Fragebogen bis zum **5. Oktober 2001** zurück an:

Ernst Basler + Partner AG
Christof Egli
Zollikerstrasse 65
CH-8702 Zollikon
Schweiz

E-Mail: christof.egli@ebp.ch
Tel. direkt +41 1 395 12 18
Tel. zentral +41 1 395 11 11
Telefax +41 1 395 12 34

Angaben zur Ihrer Person

Name:

Funktion:

Unternehmen/Organisationseinheit:

Ort, Datum:

Hinweis zur Verwendung der Antworten

Falls Sie es wünschen, werden Ihre Antworten vertraulich behandelt. Bitte machen Sie einen entsprechenden Hinweis. Im Übrigen wird eine offene Informationspolitik verfolgt.
--

Einleitung

Der Schutz von kritischen Informationsinfrastrukturen für die Wirtschaft und Verwaltung ist weitgehend unbestritten und wurde an den strategischen Führungsübungen 1997 und 2001 sowie im sicherheitspolitischen Bericht 2000 klar bestätigt. Der Schweizerische Bundesrat hat zudem mit der Unterstützung der Stiftung InfoSurance die Bedeutung des Themas Informationssicherheit unterstrichen. Als Massnahme zur Gewährleistung der Aktionsfähigkeit der Schweizerischen Bundesverwaltung in Krisensituationen erarbeitete das Informatikstrategieorgan Bund (ISB) ein Konzept für einen Sonderstab «Informationssicherheit». Das Konzept beschreibt Auftrag und Einsatz des Sonderstabes sowie die Aufbau- und Ablauforganisation. Der Sonderstab soll die Lagebeurteilung für die strategische Führung bei Krisensituationen in der Informationssicherheit wahrnehmen.

Als zentrales Element des Konzepts Sonderstab Informationssicherheit wurde in verschiedenen Gesprächen und insbesondere im Rahmen der strategischen Führungsübung INFORMO 2001 die Schaffung einer **permanenten Melde- und Analysestelle Informationssicherheit (MELANI)** genannt. Diese Melde- und Analysestelle soll über ein breit gefächertes Sensorennetz verfügen, um möglichst viele relevante Informationen in möglichst kurzer Zeit sammeln und auswerten zu können.

Die Hauptaufgabe der Melde- und Analysestelle ist die **Beobachtung, Analyse und Beurteilung** der Lage. Dies bedingt, dass Kontakte zu Betreibern von IT-Systemen in der Wirtschaft und der Verwaltung sowie anderen in- und ausländischen Warnstellen etabliert sind. Ein partnerschaftliches Netzwerk soll das **frühzeitige Erkennen von Krisen** und den Austausch von Informationen fördern.

Mit diesem Fragebogen sollen die Bedürfnisse und Wünsche von möglichen Kunden und Partnern der Melde- und Analysestelle ermittelt werden. Ein Kunde ist dabei der Sonderstab Informationssicherheit. Weitere Partner sind die IT-Betreiber und Verantwortlichen. Somit ist es für das ISB von grossem Interesse, auch die entsprechenden Wünsche und Vorstellungen zu kennen. Die Erkenntnisse sollen in die Realisierung der Melde- und Analysestelle Informationssicherheit integriert werden. Mit der Beantwortung dieses Fragebogens leisten Sie damit einen wertvollen Beitrag, um die Melde- und Analysestelle Informationssicherheit Schweiz bestmöglich zu konzipieren.

Im Hinblick auf die zukünftige Arbeit der Melde- und Analysestelle hat der Kontakt mit verschiedensten Partnern eine grosse Bedeutung. In diesem Sinn können bei Bedarf die Ergebnisse des Konzepts und das Pflichtenheft an die Interviewpartner abgegeben werden. Gerne informieren wir Sie auch über den weiteren Projektfortschritt. Auch Hinweise, welche über die gestellten Fragen hinausgehen, werden gerne berücksichtigt.

Besten Dank für Ihre Unterstützung!

23. Braucht es nach Ihrer Meinung eine Melde- und Analysestelle Informationssicherheit Schweiz?

Bitte markieren Sie die zutreffende(n) Antwort(en) und ergänzen Sie bei Bedarf die Spalte Bemerkungen. Bei ausführlichen Ergänzungen verwenden Sie bitte ein Beiblatt.

Antwort	Bemerkungen
<input type="checkbox"/> Ja, braucht es unbedingt	<i>weil...</i>
<input type="checkbox"/> Ja, braucht es, da wir bei Ereignissen noch nicht über solche Informationen verfügen	
<input type="checkbox"/> Ja, braucht es, als Ergänzung zu Informationen aus anderen Quellen	
<input type="checkbox"/> Nein, braucht es nicht, wir sind auf derartige Informationen gar nicht angewiesen	
<input type="checkbox"/> Nein, braucht es nicht, wir beziehen unsere Informationen aus anderen Quellen	
<input type="checkbox"/> Nein, braucht es nicht, wir betreiben selber intern eine analoge Stelle	
<input type="checkbox"/> weiss nicht	
<input type="checkbox"/> ...	

24. Welche Produkte/Angebote erwarten Sie von MELANI und in welcher Form?

Bitte markieren Sie die zutreffende(n) Antwort(en) und ergänzen Sie bei Bedarf die Spalte Bemerkungen. Bei ausführlichen Ergänzungen verwenden Sie bitte ein Beiblatt.

Welcher Inhalt?

Antwort	Bemerkungen
<input type="checkbox"/> Warnungen (Virenaktivität, Hacking-Attacken, Netzbelastungen wichtiger Netze,...)	
<input type="checkbox"/> Statusmeldungen (Virenaktivität, Hacking-Attacken, Netzbelastungen wichtiger Netze,...)	
<input type="checkbox"/> Lagebeurteilungen und Handlungs- empfehlungen (Virenaktivität, Hacking-Attacken, Netzbelastungen wichtiger Netze,...)	
<input type="checkbox"/> Empfehlung von Sofortmassnahmen zur Schadensverhütung	
<input type="checkbox"/> Empfehlung von allgemeinen Massnahmen zur Vorsorge und Schadensverhütung	
<input type="checkbox"/> Produkte-Evaluation und Empfehlun- gen (Firewalls, Virenschutz etc.)	
<input type="checkbox"/> Publikationen (wissenschaftliche Berichte, News- letter, Tagesberichte,...)	
<input type="checkbox"/> Individuelle Beratung bei Vorfällen	<i>falls angekreuzt, bitte Art der Beratung angeben ...</i>
<input type="checkbox"/> Hilfestellungen technischer Art (Bereitstellen von Patches oder Recovery-Programmen,...)	
<input type="checkbox"/> andere	<i>nämlich ...</i>
<input type="checkbox"/> weiss nicht	

In welcher Form?

Antwort	Bemerkungen
<input type="checkbox"/> schriftlich (Papierform)	
<input type="checkbox"/> elektronisch	
<input type="checkbox"/> telefonisch	
<input type="checkbox"/> Kombination	

«Push» oder «Pull»?

Antwort	Bemerkungen
<input type="checkbox"/> Ich will die Informationen direkt von MELANI erhalten	
<input type="checkbox"/> Ich will die Informationen bei MELANI abholen können (z.B. geschützte Website)	
<input type="checkbox"/> MELANI soll beide Möglichkeiten bieten	

Wie häufig?

Antwort	Bemerkungen
<input type="checkbox"/> sofort	
<input type="checkbox"/> nur im Ereignisfall	
<input type="checkbox"/> täglich	
<input type="checkbox"/> wöchentlich	
<input type="checkbox"/> monatlich	
<input type="checkbox"/> anders	<i>nämlich</i>
<input type="checkbox"/> weiss nicht	

Mit welchem Umfang?

Antwort	Bemerkungen
<input type="checkbox"/> eine kurze Meldung über ein Ereignis ohne umfangreiche Erläuterungen	
<input type="checkbox"/> eine Meldung mit weiteren Hintergrundinformationen	
<input type="checkbox"/> eine Meldung mit detaillierter Beschreibung zur Problembeseitigung und weiteren Hinweisen (z.B. technische Analysen, ausführliche Anleitungen)	
<input type="checkbox"/> mehr	<i>nämlich...</i>
<input type="checkbox"/> weiss nicht	

25. Welche Informationen würden Sie MELANI liefern?

Eine Melde- und Analysestelle ist auf ein breites Netzwerk von Informationslieferanten angewiesen. Welche Informationen wären Sie bereit als Beitrag zur Informationssicherheit Schweiz zu liefern? Bitte markieren die zutreffende(n) Antwort(en) und ergänzen Sie bei Bedarf die Spalte Bemerkungen. Bei ausführlichen Ergänzungen verwenden Sie bitte ein Beiblatt.

Inhalt

Antwort	Bemerkungen
<input type="checkbox"/> Virenbefall	
<input type="checkbox"/> Hacking-Attacken	
<input type="checkbox"/> Netzüberlastungen	
<input type="checkbox"/> Software-/Hardwarefehler und -ausfälle	
<input type="checkbox"/> absichtliche/unabsichtliche Fehlhandlungen durch Mitarbeitende	
<input type="checkbox"/> andere	<i>nämlich ...</i>
<input type="checkbox"/> weiss nicht	

Welche Bedingungen müssen dabei erfüllt sein?

Antwort	Bemerkungen
<input type="checkbox"/> keine	
<input type="checkbox"/> Information muss anonymisiert sein	
<input type="checkbox"/> Information muss bezahlt werden	
<input type="checkbox"/> Es darf kein Wettbewerbsnachteil entstehen	
<input type="checkbox"/> andere	<i>nämlich ...</i>
<input type="checkbox"/> weiss nicht	

26. Sind Sie bereit, MELANI mit weiteren Leistungen zu unterstützen?

Bitte markieren Sie die zutreffende(n) Antwort(en) und ergänzen Sie bei Bedarf die Spalte Bemerkungen. Bei ausführlichen Ergänzungen verwenden Sie bitte ein Beiblatt.

Würden Sie MELANI direkt unterstützen?

Anwort	Bemerkungen
<input type="checkbox"/> nein	
<input type="checkbox"/> Wir wollen bei MELANI direkt mitwirken können (personelle Unterstützung)	
<input type="checkbox"/> Wir wollen MELANI finanziell unterstützen	
<input type="checkbox"/> Wir wollen die Öffentlichkeit für MELANI sensibilisieren	
<input type="checkbox"/> Wir wollen MELANI anders unterstützen	<i>nämlich...</i>
<input type="checkbox"/> weiss nicht	

Würden Sie für Informationen zahlen, die Sie von MELANI erhalten?

Anwort	Bemerkungen
<input type="checkbox"/> nein	
<input type="checkbox"/> ja	
<input type="checkbox"/> Bezahlung pro Meldung	<i>bis max. CHF ...</i>
<input type="checkbox"/> «Abonnement» pro Jahr	<i>bis max. CHF ...</i>
<input type="checkbox"/> ja, aber nur, wenn ich selber keine Informationen an MELANI liefere	
<input type="checkbox"/> weiss nicht	

27. Wie soll die Melde- und Analysestelle Informationssicherheit Schweiz geführt, bzw. organisiert sein?

Bitte markieren die zutreffende(n) Antwort(en) und ergänzen Sie bei Bedarf die Spalte Bemerkungen. Bei ausführlichen Ergänzungen verwenden Sie bitte ein Beiblatt.

Anwort	Beschreibung
<input type="checkbox"/> MELANI muss eine staatlich geführte Organisation sein	
<input type="checkbox"/> MELANI muss eine privatwirtschaftlich geführte Organisation sein	
<input type="checkbox"/> MELANI muss von Staat und Privatwirtschaft getragen werden	
<input type="checkbox"/> MELANI muss eine internationale Vernetzung anstreben (Informationsaustausch, gegenseitige Unterstützung)	
<input type="checkbox"/> weitere Aspekte	<i>nämlich ...</i>
<input type="checkbox"/> spielt keine Rolle	

Welche Bedingungen müssen dabei erfüllt sein?

Anwort	Bemerkungen
<input type="checkbox"/> keine	
<input type="checkbox"/> Nur wer selber Informationen liefert, erhält von MELANI Informationen	
<input type="checkbox"/> MELANI muss die Vertraulichkeit der Informationen in jedem Fall gewährleisten	
<input type="checkbox"/> MELANI muss klar vom militärischen Nachrichtendienst getrennt sein	
<input type="checkbox"/> MELANI muss anbieter- und produkteneutral sein	
<input type="checkbox"/> MELANI soll sich auch an die Öffentlichkeit wenden können	
<input type="checkbox"/> andere	<i>nämlich ...</i>
<input type="checkbox"/> weiss nicht	

Verteiler

Der Fragebogen zu Kundenbedürfnissen einer Melde- und Analysestelle (31. August 2001) richtete sich an die folgenden Personen:

<i>Name</i>	<i>Vorname</i>	<i>Firma</i>
Bauknecht	Kurt	Universität Zürich, Institut für Informatik
Bischofberger	Urs	Kantonsspital Winterthur, Leiter Informatik
Brossi	Mario	Nationale Alarmzentrale
Bürgi	Dr. Walter	ATEL
Christe	Philippe	Etat de Vaud, Office de la sécurité informatique cantonale
Convers	Claude	Etat de Genève, Département de l'intérieur, de l'agriculture, de l'environnement et de l'énergie (DIAE), Secrétaire général
Dufour	Dr. Michel	Gruppe Rüstung
Favre	René	Swiss Re
Fischer	Peter	Bundesamt für Kommunikation, Abteilung Telekomdienste
Foppa	Clau	Nordostschweizerische Kraftwerke
Forster	Peter	Kdt Info Rgt 1
Freiburghaus	Urs	AIOS/VBS
Genkinger	Peter	Novartis International AG
Griesser	Markus	Schweizerische Bundesbahnen, Abteilung Informatik
Gschwind	Daniel	Unique Zurich Airport, Leiter Strategische Projekte
Gygax	Patrik	Staatsanwaltschaft Basel
Hänsli	Markus	Bundesamt für Informatik und Telekommunikation
Häring	Kurt	Stiftung InfoSurance
Holthaus	Marcus	IMSEC
Keller	Alfred	Thomson CSF Schweiz
Kleiner	Paul	AWK Group AG
Koch	Robert	SUVA
Köppel	Thomas	Bundespolizei
Lagger	Anton	Bundesamt für wirtschaftliche Landesversorgung - Sektion Ausbildung und Spezialaufgaben
Lindemann	Werner	Orange Communications AG
Lingg	Hanspeter	SICTA
Lubich	Hannes	Bank Julius Bär & Co.
Metzger	Jan	Comprehensive Risk Analysis and Management Network
Mooser	Andre	Migros Genossenschaftsbund, Leiter Stabstelle Sicherheit M-Gemeinschaft
Nägeli	Hans-Peter	IT Architecture & Business Support
Nick	Thomas	sunrise Zürich
Peter	Max	BSP AG
Ramsauer	Matthias	Bundesamt für Kommunikation, Abteilung Telekomdienste
Redli	Marius	Bundesamt für Informatik und Telekommunikation
Rytz	Ruedi	Infomatikstrategieorgan Bund
Schwalm	Burkhard	Eidgenössischer Datenschutzbeauftragter
Spillmann	Jürg	Swiss Exchange
Stutzmann	Rolf	ABB
Trachsler	Walter	Erdgas Ostschweiz
Uehli	Hanspeter	Swiss ICT
Vaterlaus	Peter	Informatiksicherheit Swisscom
Vernez	Gérald	Generalstab / UG Op
Vögeli	Hans	Zürcher Kantonalbank, Logistik
von Däniken	Urs	Bundespolizei
Weiss	Peter	Bundesamt für Informatik und Telekommunikation
Zbinden	Reto	Swiss Infosec AG
Ziegler	Pius	Hochschule Technik + Architektur Luzern

A6 Einsatzszenarien Sonderstab Information Assurance (HTA Luzern)

Szenarien für MELANI und SONIA

MELANI : Melde- und Analysestelle Informationssicherheit

SONIA : Sonderstab Information Assurance

Autoren: Pius Ziegler, HTA Luzern

Prof. Dr. B. M. Hämmerli, HTA Luzern

Ort: Horw

Datum: 28. November 2001

Kriterien für den Einsatz des Sonderstabs Information Assurance

Der Sonderstab Information Assurance (nachfolgend SONIA) wurde geschaffen, um Krisen ausgelöst durch Störungen in der Informationsinfrastruktur (nachfolgend KASII) zu bewältigen. In den nachfolgenden Betrachtungen halten wir uns an folgende Definitionen⁶:

Krisenschwelle:	Grenze zwischen steuer- oder abgrenzbaren Ereignissen, auf die noch Einfluss genommen werden kann und Ereignissen mit Auswirkungen, die primär schwerwiegend und nicht mehr kontrollierbar sind.
Krise:	Eskalation eines Vorgangs oder von Ereignissen, so dass die Auswirkungen nicht mehr kontrollier- und steuerbar sind und die Ausmasse der Auswirkungen multidisziplinär, grossflächig und von nationalem Interesse sind.

Szenarien eignen sich für eine retrospektive Betrachtung der fiktiven Ereignisse mit anschließender Analyse und Definition von möglichen Einsatzspektren für SONIA. Es ist vergleichsweise einfach zu bestimmen, wann SONIA zum Einsatz kommen soll, wenn das Ausmass der Kompromittierung bekannt ist und das Eintreten der Ereignisse in einem Zeitraffer betrachtet werden kann.

Vorgehen

In einem ersten Schritt werden Kriterien aufgestellt werden, die der Melde und Analysestelle (nachfolgend MELANI) erlauben sollen, im Falle von Ereignissen in der Informationsinfrastruktur einen Einsatz von SONIA im Entwicklungsprozess des Ereignissen simultan zu beurteilen. Diese Kriterien sind nicht vollständig und müssen iterativ durch die Analyse der aktuellsten Ereignisse angepasst und ergänzt werden.

Die Szenarien dienen zur Überprüfung und Handhabbarkeit dieser Kriterien im konkreten Ereignisfall. Die Szenarien sollen nach Möglichkeit durch verschiedene Personen bearbeitet und die Erfahrungen dokumentiert werden.

Eine retrospektiven Betrachtung der Szenarien soll eine Diskussion eröffnen, wie allfällige Massnahmen (Information und deren Verbreitung) von MELANI mitgeholfen hätten, das Schaden ausmass einzudämmen. Ebenfalls können im Aktivierungsfall von SONIA Handlungsoptionen diskutiert werden.

⁶ Glossar, das im Rahmen der Entwicklung von INFORMO 2001 zusammengestellt wurde.

Abgrenzung und Schnittstellen

Krisen in der Informationsinfrastruktur haben oftmals sichtbare physikalische Wirkungen als Folge von Ereignissen in der Informationsinfrastruktur, die aber nicht direkt mit dem Ereignis in Verbindung gebracht werden können.

Nachfolgend sind einige Merkmale aufgelistet, die für Krisen im Informationsumfeld gelten, jedoch nicht unbedingt auf herkömmliche Krisen übertragbar sind:

Quantität von Ressourcen und Wirkung	Eine grosse Wirkung muss nicht zwingend mit dem Einsatz von viel Ressourcen korrelieren. Es kann durchaus der umgekehrte Fall eintreten, z.B. „I love you“-Virus
Vorwarnzeit	Das Schadenbild und das Schadenausmass ist grundsätzlich unabhängig von der Vorwarnzeit. Ereignisse im Informationsumfeld sind möglicherweise nicht unmittelbar erkennbar – die Krise kann sich anbahnen, ohne dass sie bemerkt wird.
Geografische und strukturelle Eingrenzbarkeit von Ereignissen	Die Wirkung eines Ereignisses in der Informationsinfrastruktur muss nicht geografisch und/oder strukturell (z.B. Departement/Sektor/Branche/Kanton) eingrenzbar sein. Es ist viel wahrscheinlicher, dass sich Ereignisse innerhalb von logischen Einheiten z.B. Router, Firewalls, Betriebssysteme etc. auftreten.

Folgende Eigenschaften sind prägend für Ereignisse in der Informationsinfrastruktur:

Ursache und Wirkung	Ein Zugsunglück, bei dem die Ursache in einem Softwarefehler liegt, zeigt deutlich, dass ein Schadenbild sich in einer völlig anderen Form präsentieren kann. Dies bedeutet, dass sich die Wirkung schlagartig in einen anderen Bereich verlagern kann. Eine Analyse muss dann nicht unmittelbar auf die Ursache hinweisen, was die Erkennbarkeit derartiger Krisen erschwert (vgl. Zugsunglück durch Leitsystemfehler). Weiter muss davon ausgegangen werden, dass zuerst die Wirkung bekannt ist und die Ursachenanalyse einige Zeit in Anspruch nehmen wird.
Schnittstellen	Die aufgeführten Eigenschaften von Krisen in der Informationsinfrastruktur eröffnen neue Schnittstellen zu anderen potentiellen Institutionen, die sich primär auf die Bekämpfung der Wirkung spezialisiert haben, z.B. Krisenstäbe, Feuerwehr. Diese Schnittstellen müssen im Praxisfall berücksichtigt werden.

Einsatzspektrum von SONIA

Die Analyse der Ereignisse bezüglich Ursache und Wirkung sowie das Abschätzen des Eskalationspotentials helfen, eine Aktivierung von SONIA zu beurteilen.

Die simultane Beurteilung der Ereignisse wird im Normalfall durch MELANI sichergestellt. Daher soll MELANI über ein Instrument verfügen, mit welchem auf die Ereignisse bezogen eine strukturierte Entscheidung über die Einberufung von SONIA herbeigeführt werden kann.

Es werden drei Aspekte zur Entscheidung über den Einsatz von MELANI berücksichtigt:

- Ursache- / Themenabgrenzung
- Wirkung
- Eskalationspotential

a) Ursachen- / Themenabgrenzung

Folgende Kriterien bezogen auf die Ursachen der Ereignisse sollen als Voraussetzung gelten, damit SONIA aktiv wird:

Themen von Ursachen

SONIA kann aktiv werden, wenn die Ursache der Ereignisse in der Informationsinfrastruktur liegt.

Informationsinhalte

Krisen, die durch Informationsinhalte ausgelöst werden und die über die einwandfrei funktionierende Informationsinfrastruktur übertragen werden, befinden sich ausserhalb des Einsatzspektrums von SONIA. Die Situation kann dann in den Zuständigkeitsbereich von SONIA fallen, wenn eine Kettenreaktion eines derartigen Ereignisses die Informationsinfrastruktur beeinträchtigt. Je nach Aufgaben- und Kompetenzdefinition kann MELANI die richtigen Stellen zeitgerecht avisieren.

b) Wirkung

Die Analyse der Wirkung eines Ereignisses hinsichtlich verschiedener Kriterien soll ebenfalls helfen, die Problemstellung in kurzer Zeit zu strukturieren und den Entscheid über die Einberufung von SONIA herbeizuführen. Dabei unterscheiden wir die Wirkung in folgende Kriterien:



Abbildung 1: Wirkung von Ereignissen in verschiedenen Dimensionen

Anzahl der Betroffenen

Die Ausdehnung eines Ereignisses in der Informationsinfrastruktur kann über die Anzahl der direkt und indirekt betroffenen Personen gemessen werden

Intensität der Betroffenheit

Die Art der Betroffenheit und deren Intensität in Hinblick auf die Grundbedürfnisse (Maslov'sche Pyramide) der Menschen oder die Grundfunktionen von Sektoren und Branchen kann Hinweise auf das mögliche Eskalationspotential des Ereignisses geben. Die Intensität der Betroffenheit wird in dieser Betrachtung auf die Fakten reduziert und nicht auf die individuelle Wahrnehmung

Wahrnehmungsintensität

Ereignisse im Umfeld von Informationssicherheit werden aus subjektiver Sicht meist indirekt wahrgenommen: Business Prozesse (Funktionen) werden blockiert oder Bedürfnisse können nicht mehr abgedeckt werden. Eine individuelle Analyse der Ereignisse durch die Betroffenen lässt in gewissen Fällen erste Rückschlüsse auf Probleme in der Informationsinfrastruktur zu z.B. Bankomat.

Die Wahrnehmungsintensität ist sehr oft das Resultat aus der Anzahl der Betroffenen und der Intensität der Betroffenheit. Über diese Faktoren definiert sich das Medieninteresse. Die Medien leisten in der Aufklärungsphase einen grossen Beitrag zur allgemeinen Information, sofern ein lokales wenn nicht sogar nationales Interesse besteht.

Derartige Informationen verbreiten sich durch die hohe Medienpräsenz im Alltag blitzartig. Je nach Dimension der Berichterstattung wird auch der politische Druck zunehmend grösser.

Eine Falschinformation über ein KKW-Unglück kann in der Bevölkerung grosse Verunsicherung und damit Betroffenheit durch Information auslösen. Menschen werden durch die Medien bewusst oder unbewusst beeinflusst. Die Intensität der Betroffenheit und das Interesse für das Ereignis kann durch eine entsprechende Information verändert werden.

c) Eskalationspotential

Ereignisse können auf folgende zwei Arten eskalieren:

Ein Ereignis kann weitere Fehlfunktionen im gleichen oder in anderen Systemen zur Folge haben, welche weitere Betroffene mit einer gewissen Intensität der Betroffenheit provoziert. In einem solchen Fall verlängern sich durch die Fehlfunktionen die Einzelvektoren in Abbildung 1 und die Gesamtwirkung vergrössert sich entsprechend.

Die Wahrnehmung einzelner oder summierter Ereignisse wird durch die Medien intensiviert, so dass weitere indirekt Betroffene provoziert werden. Bei genügend breitflächiger Informations-

verteilung und Wahrnehmungsintensivierung wird ein derartiges Thema auf politischer Ebene aufgegriffen, was den Einsatz von SONIA zur Folge haben kann.

Entscheidungshilfen

Folgende Tabellen bieten eine Entscheidungshilfe, die für die Beurteilung eines Einsatzes von SONIA herangezogen werden können. Diese Tabellen sind für den praktischen Einsatz von MELANI zu ergänzen und zu prüfen.

Ausgehend von der Primär- und Sekundärwirkung⁷ wird versucht Rückschlüsse auf die Ursache zu ziehen. Allerdings müssen sich die Analysten bewusst sein, dass zwischen Wirkung und Finden der Ursache einige Zeit verstreichen kann. Dies hat zur Folge, dass bereits aufgrund der Wirkung über ein Engagement von SONIA zeitgerecht entschieden werden muss.

⁷ Unter Primärwirkung verstehen die Autoren die Summe der Wirkungen, die durch Einzelereignisse im gleichen Bereich auftreten. Betrifft die Wirkung durch weitere Fehlfunktionen einen anderen Bereich, wird diese zur Sekundärwirkung. Die Grenze zwischen Primär- und Sekundärwirkung ist unscharf.

Tabelle 1: Thematische Bestimmung des Einsatzspektrums von SONIA

Nr	Ursache	Primärwirkung	Sekundärwirkung	Aufgebot SONIA
1	Informationssicherheit /- infrastruktur	Informationsinfrastruktur	Informationsinfrastruktur oder andere Bereiche	Ja
	<i>z.B. logischer Betriebssystem- fehler</i>	<i>z.B. Ausfall von IT- Infrastrukturkomponenten</i>	<i>z.B. Business Prozesse fallen aus</i>	
2	Informationssicherheit /- infrastruktur	Andere Bereiche	Andere Bereiche	Ursachenabhängig – relevant ist der Störungsgrad der Informationsinfra- struktur
	<i>z.B. Fehler in Bahnleitsystem- software</i>	<i>z.B. Zugsunglück</i>	%	
3	Informationssicherheit /- infrastruktur	Andere Bereiche	Informationsinfrastruktur	Ursachen- und Wirkungsabhängig – relevant ist der Störungsgrad der Informationsinfra- struktur
	<i>z.B. Energieversorgungs- Steuerungssoftware</i>	<i>z.B. Stromversorgung</i>	<i>z.B. Ausfall von Informations- Infrastrukturkompo-nenten</i>	
4	In anderen Bereichen	Informationsinfrastruktur oder andere Bereiche	Informationsinfrastruktur oder andere Bereiche	Nein
	<i>z.B. Energieversorgung</i>	<i>z.B. Ausfall von Informations- Infrastrukturkompo-nenten</i>	%	

Falls die simultane Beurteilung der Ereignisse gemäss obiger Tabelle grundsätzlich auf eine Aktivierung von SONIA hinweist, soll durch die Abschätzung der Wirkung und des Eskalationspotentials eine Entscheidung über den Einsatz von SONIA herbeigeführt werden können.

Tabelle 2: Komponentenbasierte Analyse der Wirkung

Nr	Anzahl Betroffene			Intensität der Betroffenheit		Wahrnehmung	Eskalationspotential	Aufgebot SONIA
	Sektorübergreifend	Unternehmensübergreifend	Viele Einzelpersonen	Grundfunktionen	Grundbedürfnisse			
5	X	X	X	Nein	Nein	1	Nein	Nein
6	X	X	X	Nein	Nein	2	Ja	Eventuell im Sinne der Prävention
7	X	X	Ja	X	Ja	1-4	X	Ja
8	Ja	X	X	Ja	X	1-4	X	Ja
9	Nein	Ja	Nein	Ja	Nein	1-2	Nein	Nein
10	Nein	Ja	Nein	Ja	Nein	2	Ja	Ja, im Sinne der Prävention

Erläuterungen:

Generell:

- X: Ja oder Nein: In der gegebenen Konstellation nicht mehr relevant, Entscheid über den Einsatz von SONIA wird bereits gefällt

Wahrnehmungsintensität:

- 1: nur direkt Betroffene nehmen das Ereignis wahr
- 2: Lokale Medien (Druck, Lokalradio) interessieren sich für das Ereignis
- 3: Nationale Medien (Druck, nationale Radiosender und Fernsehen) interessieren sich für das Ereignis
- 4: globale Medienpräsenz, Stellungnahmen werden erwartet, Pressekonferenzen

Eskalationspotential:

Ja: Wahrnehmungsintensivierung durch die Medien oder weitere logische Fehlfunktionen

Nein: Es werden keine weiteren logischen Fehlfunktionen erwartet und das Medieninteresse bleibt gleich oder nimmt ab

Wichtig beim Analyseprozess ist die Fähigkeit, die Informationen über Ereignisse richtig zu interpretieren und das Eskalationspotential richtig abzuschätzen. Fehlalarme werden unumgänglich sein, um erste Erfahrungen aufzubauen.

Überprüfung der Entscheidungshilfe anhand von drei Szenarien

In diesem Abschnitt versuchen die Autoren die Szenarien anhand der aufgeführten Kriterien zu untersuchen und einen Einsatz von SONIA zu beurteilen. Die detaillierten Szenarien sind im Anhang A6 aufgeführt. Da sich SONIA ausschliesslich Ereignissen im Informationsinfrastrukturbereich annimmt, müssen die Ereignisse speziell auf deren Relevanz für MELANI und SONIA untersucht werden.

Szenario 1: Inhaltliche Bedrohung über E-Mails

Fall a) Im diesem Szenario handelt es sich um eine Einschüchterungskampagne, welche das Internet als Medium verwendet.

Die Aktivierung von SONIA ist nicht notwendig, da nur Inhalte über eine einwandfrei funktionierende Informationsinfrastruktur übertragen werden. In dieser Phase könnte MELANI als Triagestelle dienen und z.B. die Bundespolizei informieren, damit diese vom Ausmass der Massensendungen informiert ist und dadurch Massnahmen einleiten kann.

Fall b) Aus der allgemeinen Verunsicherung in der Bevölkerung entsteht auch in der Informationsinfrastruktur ein Problem. Die Internetbenutzer verschicken unzählige E-Mails mit grossen Attachments, welche in dieser Ansammlung das Internet zu überlasten beginnen (Szenario 1, Abschnitt 12). Damit nimmt auch die Performance des Internets langsam ab. Für diesen Fall wäre ein Einsatz von SONIA thematisch grundsätzlich denkbar.

Tabelle 3: Themenrelevanz Szenario 1

<i>Nr</i>	<i>Ursache</i>	<i>Primärwirkung</i>	<i>Sekundärwirkung</i>	<i>Aufgebot SONIA</i>
1	Informationssicherheit /infrastruktur	Informationsinfrastruktur	Informationsinfrastruktur oder andere Bereiche	Ja
4	In anderen Bereichen	Informationsinfrastruktur oder andere Bereiche	Informationsinfrastruktur oder andere Bereiche	Nein

In der Analyse der Wirkung zeigt der Fall a (Zeile Nr. 5), dass eine grosse psychologische Wirkung in der Bevölkerung erzielt wird, dass aber auf die Informationsinfrastruktur bezogen keine Wirkung spürbar ist. SONIA muss deshalb nicht aufgegeben werden. Dieses Szenario hat ein kleines Eskalationspotential (Zeile Nr. 6). Das Aufgebot von SONIA ist aber auch in diesem Fall nicht zwingend, da die Ursache der Internet-Überlastung in den Userinteraktionen (E-Mails) liegt.

Tabelle 4: Wirkungsrelevanz Szenario 1

<i>Nr</i>	<i>Anzahl Betroffene</i>			<i>Intensität der Betroffenheit</i>		<i>Wahrnehmung</i>	<i>Eskalationspotential</i>	<i>Aufgebot SONIA</i>
	Sektorübergreifend	Unternehmensübergreifend	Viele Einzelpersonen	Grundfunktionen	Grundbedürfnisse			
5	X	X	X	Nein	Nein	1	Nein	Nein
6	X	X	X	Nein	Nein	2	Ja	Eventuell im Sinne der Prävention

Szenario 2: Illegale Banktransaktionen

Im Szenario 2 nutzen Mafia-ähnliche Gruppierungen bekannte Schwächen in der „Sandbox“ der Java Virtual Machine, um Login-Versuche von Bankkunden abzufangen und selber Transaktionen auf fremde Konten durchzuführen.

MELANI als zentrale Sammelstelle hat den Überblick über alle Meldungen, die bezüglich Hacking der Banken auftauchen. Die Anhäufung von Hacking Attacken (Szenario 2, Abschnitte 1, 4, 6) lässt bereits vermuten, dass es sich um gezielte Angriffe handelt. Falls nicht schon initiiert, müsste MELANI durch einen Informationsaustausch die betroffenen Firmen zusammenbringen und / oder koordinieren. Zu diesem Zeitpunkt hat MELANI jedoch noch keine Kenntnis über die Wirkung des Ereignisses.

Tabelle 5: Themenrelevanz Szenario 2

<i>Nr</i>	<i>Ursache</i>	<i>Primärwirkung</i>	<i>Sekundärwirkung</i>	<i>Aufgebot SONIA</i>
1	Informationssicherheit /- infrastruktur	Informationsinfra- struktur	Informationsinfra- struktur oder andere Bereiche	Ja

Kurz nach den Hacking Attacken ist die Primärwirkung noch nicht bekannt. Spätestens nach der Fernsehsendung über die aufgebrachtten Bürger zeigt sich erstmals die Wirkung. Sie kann jedoch noch nicht unbedingt in Zusammenhang mit den Hacking-Attacken gebracht werden. Die Wahrnehmungsintensität in der Bevölkerung nimmt mit den auftretenden Medienmeldungen stetig zu, so dass der Einsatz von SONIA in Erwägung gezogen werden muss (Szenario 2, Abschnitt 8-10). Es scheinen viele Einzelpersonen in Kombination mit einem spezifischen Sektor betroffen zu sein. Zudem sind Einzelpersonen in ihren Grundbedürfnissen unbefriedigt, wenn sie an den Bankomaten falsche Kontomutationen feststellen und kein Geld beziehen können.

Spätestens zu dem Zeitpunkt, wo das modifizierte Applet auftaucht, kann davon ausgegangen werden, dass die Hacking Attacken mit den jüngsten Medienmeldungen in Zusammenhang stehen. Die Softwareanalyse des Applets bestätigt, dass das Applet auf die Ressourcen zugreifen kann (Ursache). Die Tragweite dieser Feststellung provoziert ein Aufgebot von SONIA (Szenario 2, Abschnitt 14), da nun auch weitere Sektoren betroffen sein könnten und eCommerce und eGovernment Anwendungen überprüft werden müssen.

Tabelle 6: Wirkungsrelevanz Szenario 2

Nr	Anzahl Betroffene			Intensität der Betroffenheit		Wahrnehmung	Eskalationspotential	Aufgebot SONIA
	Sektorübergreifend	Unternehmensübergreifend	Viele Einzelpersonen	Grundfunktionen	Grundbedürfnisse			
7	X	X	Ja	X	Ja	1-4	X	Ja
8	Ja	X	X	Ja	X	1-4	X	Ja

Szenario 3: Krise aufgrund von Indizien

Das Szenario 3 versucht, aufgrund von Indizien eine Reaktion zu provozieren. Die hohen Übertragungsgeschwindigkeiten haben in Fällen von Fehlerübertragungen sehr kurze Reaktionszeiten zur Folge. In diesem Szenario ist die Ursache zunächst nicht bekannt. Sichtbar sind allerdings die Auswirkungen im Informationsinfrastrukturbereich, dessen Funktionen beeinträchtigt sind.

Tabelle 7: Themenrelevanz Szenario 3

Nr	Ursache	Primärwirkung	Sekundärwirkung	Aufgebot SONIA
1	Informationssicherheit /-infrastruktur	Informationsinfrastruktur	Informationsinfrastruktur oder andere Bereiche	Ja

Die Wirkung zeigt sich sehr schnell, indem innerhalb von rund 30 Minuten der Netzwerkverkehr auf gegen null geht. Sobald der Netzwerkverkehr abnimmt, kann davon ausgegangen werden dass mehrere Sektoren betroffen sind und daher auch Grundfunktionen (über Internet) nicht mehr funktionieren. Die Wahrnehmungsintensität wird in naher Zukunft stark zunehmen und es ist noch nicht abzuschätzen, welches Eskalationspotential diese Ereignisse haben. Ein Aufgebot von SONIA ist unumgänglich (Szenario, Abschnitt 8).

Tabelle 8: Wirkungsrelevanz Szenario 3

Nr	Anzahl Betroffene			Intensität der Betroffenheit		Wahrnehmung	Eskalationspotential	Aufgebot SONIA
	Sektorübergreifend	Unternehmensübergreifend	Viele Einzelpersonen	Grundfunktionen	Grundbedürfnisse			
8	Ja	X	X	Ja	X	1-4	X	Ja

Nach der Feststellung der technischen Ursachen muss SONIA als Koordinator auftreten, um die Netzwerkinfrastruktur auf definierte Weise wieder hochzufahren. Es werden mit grosser Wahrscheinlichkeit Stellungnahmen verlangt.

Die Autoren gehen davon aus, dass die Reaktionszeit von 30 Min. zu kurz ist, um präventive Entscheide treffen zu können, zumal die Entwicklung der Netzbelastung nicht voraussehbar ist.

Fazit

Die Analyse der Szenarien auf der Basis der definierten Kriterien hat gezeigt, dass sich Ereignisse gut strukturieren lassen. Es sind folgende Problembereiche aufgetreten:

- Bei komprimiert auftretenden Ereignisse ist es schwierig, zeitgerecht die korrekten Schlussfolgerungen zu ziehen, da die Richtigkeit der Meldungen sowie mögliche Wahrnehmungsverfälschungen überprüft werden müssen. Richtige Entscheide sind zudem schwierig zu fällen, wenn wenige Fakten vorliegen.
- Die Erfahrungen der Testpersonen mit den Szenarien müssen aufgezeichnet und ausgewertet werden, damit dieser Erfahrungsschatz im Ernstfall zur Verfügung steht.
- Die ersten Erfahrungen mit den vorliegenden Szenarien haben eine Grauzone aufgezeigt, in der unklar ist, ob und ab welchem Zeitpunkt SONIA einberufen werden soll. Weitere Testpersonen würden helfen, einerseits die Entscheidungshilfen zu überprüfen und andererseits die Grenze für ein Aufgebot von SONIA schärfer zu definieren.
- Weitere Szenarien, die bewusst diese Grauzone adressieren, unterstützen ebenfalls den Prozess zur schärferen Gestaltung dieser Grenze.

Szenarien

Einleitung

Die Notwendigkeit des Schutzes der schweizerischen Informationsinfrastrukturen und damit auch der Bundesverwaltung wurde sowohl als Schlussfolgerung der Strategischen Führungsübung 97 (SFU 97) als auch im sicherheitspolitischen Bericht 2000 klar festgehalten. Der Bundesrat hat zudem mit der Unterstützung der Stiftung InfoSurance die Bedeutung des Themas Informationssicherheit unterstrichen. Als Massnahme zur Gewährleistung der Aktionsfähigkeit der Bundesverwaltung in Krisensituationen wurde das Informatikstrategieorgan Bund (ISB) mit der Bildung eines Sonderstabes Information Assurance (SONIA) beauftragt. Während der Führungsübung 97 (SFU97) und INFORMO 2001 wurden das Bedürfnis nach einer koordinierenden Stelle für die Anliegen der Informationssicherheit und zum Schutz der Informationsinfrastrukturen geäussert.

Als zentrales Element des Konzepts Sonderstab Information Assurance wurde in verschiedenen Gesprächen und insbesondere im Rahmen der Übung INFORMO 2001 die Schaffung einer permanenten Melde- und Analysestelle Informationssicherheit (MELANI) genannt. Die Melde- und Analysestelle soll über ein breit gefächertes Sensorennetz verfügen, um möglichst viele relevante Informationen in möglichst kurzer Zeit sammeln und auswerten zu können. Diese Stelle soll im Ereignisfall im direkten Kontakt zum Sonderstab stehen und diesen mit Meldungen zu den neuesten Entwicklungen versorgen.

MELANI existiert zum heutigen Zeitpunkt noch nicht. Die Anforderungen, Zuständigkeiten und Kompetenzen werden aktuell in einem Einsatzkonzept erarbeitet. Es fehlen weitgehend die Erfahrungen im Umgang mit Ereignissen dieser Art.

Ziele der Szenarien

Erfahrungsaufbau für MELANI

Die vorliegenden Szenarien zielen darauf ab, Erkenntnisse und Erfahrungen über die notwendigen Spezifikationen, das Einsatzspektrum und die notwendigen Kompetenzen von MELANI und SONIA zu gewinnen, um diese in das Einsatzkonzept von MELANI einfließen zu lassen.

Krisenschwelle

Ein weiteres Ziel ist es, Erkenntnisse und Erfahrungen mit potentiellen Gefahren im Umfeld von Krisen in der Informationsverarbeitung und deren Erscheinungsbild zu sammeln. Auswertungen über die subjektive Wahrnehmung der Szenarien können unter Umständen wichtige Hinweise über die zukünftige Wertung von einzelnen und korrelierenden Ereignissen ergeben – die Krisenschwelle wird adressiert, die in der Vergangenheit die unterschiedlichsten Definitionen an den Tag gebracht haben.

Grenzen von Szenarien

Bei der Arbeit mit Szenarien dieser Art ist zu berücksichtigen, dass jeweils nur einzelne Facetten aus einer Fülle von möglichen Erscheinungsbildern adressiert werden.

Die vorliegenden drei Szenarien helfen, einen Basis-Erfahrungsschatz aufzubauen, der gezielt weiterentwickelt werden kann.

Aufbau der Szenarien

Die nachfolgend dargestellten Szenarien sind folgendermassen strukturiert:

Ausgangslage	Alle Szenarien finden in der Gegenwart statt. Dies soll dem Lesern ermöglichen, sein Hintergrundwissen bestmöglichst in die Beurteilung der Situation einfließen zu lassen.
Einleitung	In der Einleitung wird jeweils kurz auf das Umfeld des Szenarios eingegangen. Spezielle Gegebenheiten und Voraussetzungen, die einen Einfluss auf das Verhalten von MELANI oder SONIA haben, werden einleitend aufgeführt.
Szenarioteil	Das Szenario wird aus der Perspektive von MELANI beschrieben. Einzelne Nachrichten werden tropfenweise eingespielt. Die Leserschaft baut sich aufgrund der subjektiven Wahrnehmung unterschiedliche Informationslandschaften auf, die die einzelnen Leser zu unterschiedlichen Reaktionen verleiten werden.
Massnahmen des Leser (Zusatzblatt)	Auf einem Zusatzblatt kann der Leser zu den einzelnen Ereignissen seine Gedanken und Reaktionen notieren. Dabei ist wichtig, dass der Leser allfällige Massnahmen und speziell den Zeitpunkt des Aufgebots des Sonderstabs festhält. Aus der Analyse der Resultate lassen sich Erfahrungswerte aufbauen, die zu Beginn des operativen Betriebs von MELANI herangezogen werden können.
Motive	Im Anschluss an das Szenario geben die Autoren das Motiv bekannt. Die Gegenüberstellung der subjektiven Einschätzung des Motivs und der wirklichen Absicht der Autoren wird die Schwierigkeit der Online-Beurteilung von Ereignissen aufzeigen. Daraus lassen sich Erfahrungen im Umgang mit Schwellenwerten und Eskalationspotentialen sammeln, die im operativen Betrieb leider immer erst rückblickend erkannt werden.
Vorgehen aus Sicht der Täterschaft	Die Informationen zum genauen Hergang sollen schliesslich die Lücken zwischen beabsichtigter Planung und Wahrnehmung der Ereignisse füllen.
Zweck	Mit einem Szenario werden immer nur Ausschnitte eines möglichen Gesamtspektrums abgedeckt. Aus diesem Grund wird hier beschrieben, welche Themen mit dem Szenario speziell adressiert werden sollten.

Leseanleitung

Rolle des Lesers

Sie als Leser werden gebeten, in den Szenarien die Rolle der supponierten MELANI zu übernehmen.

Analyse der Lage bezüglich Informationssicherheit

Die Ereignisse treten sequentiell auf. Sie beurteilen die Einzelereignisse zum Meldezeitpunkt auf mögliche Auswirkungen und das Entwicklungspotential bezüglich der Gesamtlage Informationssicherheit im Rahmen des nationalen Interesses.

Dokumentation der Erkenntnisse

Wir bitten Sie als Leser, ein Ereignis nach dem anderen zu lesen, sich für jedes Ereignis kurz Zeit zu nehmen und Ihre Notizen zur Auswertung des spezifischen Ereignisses abzuschliessen, bevor Sie zum nächsten Ereignis weitergehen.

Bitte dokumentieren Sie die Resultate Ihrer Lagebeurteilung sowie Massnahmen, die Sie im Rahmen von MELANI einleiten würden, synchron zum Ereignis auf dem Beiblatt unter der Ereignisnummer. Erkenntnisse, die Sie simultan zu einem spezifischen Ereignis dokumentiert haben und die im Verlauf der Ereignisse und im neuen Kontext der Gesamtereignisse revidiert werden, bitten wir Sie nicht zu korrigieren.

Im Rahmen Ihrer Beurteilung interessieren folgende Punkte:

- Beurteilung der aktuellen Lage, wie sie sich aus Ihrer Sicht zum Auftretenszeitpunkt des Ereignisses präsentiert
- Entwicklung der Motive aus subjektiver Lesersicht
- Information / Massnahmen von Seiten MELANI und/oder SONIA
- Zeitpunkt des Aufgebots des Sonderstabs Informationssicherheit

Auswertung der Erkenntnisse

Die subjektiven Lagebeurteilungen sowie die eingeleiteten Massnahmen möchten wir zum Erfahrungsaufbau sammeln und auswerten. Aus diesem Grund bitten wir Sie, die Beiblätter zur Auswertung und zum Aufbau von Erfahrungen an folgende Adresse zu senden:

Informatikstrategieorgan Bund

Leistungsbereich Informationssicherheit

Friedheimweg 14

3003 Bern

Ausgangslage der Szenarien

Die nachfolgende Ausgangslage gilt für alle Szenarien.

Weltgeschehen

Die Situation nach den Terroranschlägen vom 11. September 2001 auf die World Trade Center von New York hat die Hackergemeinde der westlichen Welt gespalten. „Ethische“ Hacker verzichten bewusst auf Attacken und damit die Lancierung eines Cyber-Kriegs gegen die IT-Systeme der nahöstlichen Länder, währenddem rechtsradikale Gruppierungen lautstark gegen den Terror aus dem nahen Osten auch mit IT-Attacken wehren wollen.

Die nahöstlichen Ländern, von denen ausgehend verschiedene Terrorangriffe vermutet werden, wurden in der jüngsten Vergangenheit vermehrt Opfer von Internetangriffen auf die IT-Infrastruktur.

Die westliche Welt ist sich bewusst, dass die IT-Durchdringung im nahen Osten nicht weit fortgeschritten ist. Studenten der Universitäten bilden den Kern an IT-Spezialisten; deren Kompetenzen sind nur schwer abzuschätzen. Man weiss allerdings, dass das Kontaktnetz zu gleichgesinnten Studenten anderer Hochschulen auch in der Schweiz gut ausgebildet ist.

MELANI

Seit der Gründung hat sich MELANI ein breites Know-how im Bereich Netzwerkinfrastrukturen und Viren aufgebaut. Das Image von MELANI als kompetente Institution im Bereich Informationssicherheit hat sich in der Schweizer Wirtschaft und auch im Ausland etabliert. Speziell im Virenbereich konnte MELANI in der Vergangenheit grössere Schadenausmasse durch Sofortinformationen verhindern.

Das Vertrauen von ISP's gegenüber MELANI wurde über mehrere Jahre aufgebaut. MELANI hat dadurch die Möglichkeit, den Verlauf der Datenvolumina in Knotenpunkten der ISP zu analysieren und mit Werten ausländischer Knotenpunkte zu vergleichen.

Die organisatorischen Abläufe sind etabliert und das Kontaktnetzwerk im In- und Ausland ist breit angelegt und wird aktiv unterhalten. Im Falle von Recherchen und Analysetätigkeiten fungiert MELANI als zentrale Koordinationsstelle für die dezentrale Problemlösung.

Das Vertrauen in die Institution MELANI ist gegeben und die Unternehmungen haben begonnen, MELANI als Ansprechpartner in ihre Notfallverfahren zu integrieren.

MELANI hat seit der Gründung eine Datenbank aufgebaut, in der alle Vorkommnisse indexiert archiviert werden. In der Zwischenzeit ist so eine Datensammlung von mehreren 1000 Ereignissen und einigen Gigabyte Daten entstanden – der Zugriff darauf ist sehr komfortabel und die Suchergebnisse sind sehr gut.

Aus diesem Grund und im Wissen um das breite Know-how wird MELANI auch ausserhalb der normalen Melde und Analysetätigkeit um Beratungsdienste angefragt. Sofern die Kapazitäten dies zulassen, nimmt MELANI diese Beratungstätigkeit wahr.

Szenario 1: Inhaltliche Bedrohung über E-Mails

Einleitung		<p>Das Datenvolumen des Internets ist am heutigen Tag wieder normal, nachdem gestern ein Virus mit dem Namen „Turbo“ entdeckt wurde, dessen Verbreitung ohne Zutun des Users direkt auf dem Mailserver erfolgt. Durch die schnelle Reaktion von MELANI konnte auf den zentralen Knotenpunkten ein Filter auf den Header des Emails gesetzt werden. Die Email-Server einiger Firmen waren aber trotzdem stark betroffen. Das Datenvolumen nahm sprunghaft zu.</p> <p>Es gehen wie üblich Warnungen über das Virus ein, zu denen MELANI bereits am Vortag Stellung genommen und Ratschläge erteilt hat.</p>
Nr.	Meldungseingang	<i>Bei MELANI eingehende Meldungen</i>
1.	31.11.01 12:34h	<p>Lebensmittelproduzent „Genshop“</p> <p>Ein Schweizer Grossproduzent der Lebensmittelindustrie meldet einen erfolgreichen Hackerangriff, bei dem die Angreifer offenbar Zugriff auf geheime Dokumente über Spezialverfahren zur Lebensmittelherstellung erhalten haben.</p> <p>Bereits sind Erpressungsversuche eingegangen. Die Kriminalpolizei hat sich diesem Vorfall angenommen. Die Erpresser fordern 10 Mio. CHF, andernfalls werden diese Dokumente den direkten Konkurrenten in die Hände gespielt. Die Frist zur Übergabe des Geldes beträgt drei Tage.</p>
2.	1.12.01 15:01h	<p>Die Netzsensoren von MELANI verzeichnen ein erhöhtes Datenvolumen eines Teilnetzes im Raum Aarau, welches vor allem für die Mobilkommunikation eingesetzt wird.</p> <p>Gleichzeitig verzeichnen die Sensoren in Luzern eine massive Datenvolumenzunahme zwischen Bern und Zürich.</p>
3.	1.12.01 17:43h	<p>Meldung einer unbekanntem Antiviren-Firma</p> <p>Eine unbekanntem Antiviren-Firma schickt einen neuen Virenschutz, der direkt auf die Mailserver geladen werden kann. Die Analyse der Software lässt nicht eindeutig erkennen, wie die Antivirensoftware funktioniert.</p>

4.	1.12.01 18:25h	<p>Meldung des Telekommunikationsunternehmens „Directconnect“: Störung im Raum Gösgen</p> <p>Das schweizerisch tätige Telekommunikationsunternehmen „Cableconnect“ meldet den Ausfall eines regionalen Mobilnetzes im Raum Niedergösgen. Der Fehler liegt vermutlich in der Software und konnte bisher noch nicht eruiert werden.</p>
5.	2.12.01 10:12h	<p>Unter der Menge an Spawn Mail gehen bei MELANI beinahe gleichzeitig 20 in Englisch abgefasste Emails ein mit dem Header „poisoned food in swiss malls“ – der Absender hat unterschiedliche Absender Email-Adressen und kann technisch weder einer Person (Synonym) noch einem Land zugeordnet werden.</p> <p>Der Inhalt dieser Mails besagt, dass mehrere Schweizer Lebensmittelproduktionsstrassen von Grossproduzenten über Nacht mit flüssigem Nervengift verseucht wurden. Mit dieser Attacke werden die westlichen Länder dazu aufgefordert, Ihre Nahostpolitik und die Unterstützung im Nordatlantikpakt zu überdenken.</p>
6.	2.12.01 13:10h	<p>Ein spezifischer Server des EFD muss aufgrund einer Denial of Service Attacke vom Netz genommen werden. Es ist feststellbar, dass die Absender-IP-Adressen von der Grossbank „Swissmoney“ im Raum Zürich stammen. Allerdings geht man hier von einem Attacken-Spoofing aus – Vertreter des EFD sind daran, Kontakt mit der Grossbank aufnehmen</p>
7.	2.12.01 13:35h	<p>MELANI erhält in der Folge mehrere hundert Anfragen von besorgten Bürgern, die das entsprechende Email mit dem Titel „poisoned food in swiss malls“ ebenfalls in mehrfacher Ausführung erhalten haben. Sie erwarten eine Stellungnahme der zuständigen Stellen.</p>
8.	2.12.01 13:40h	<p>Meldung von Hans. M. – Vertreter des ISP „Luzernensis“</p> <p>Beinahe gleichzeitig geht von Hans M. - ein Vertreter des ISP „Luzernensis“ und Partner von MELANI - die Meldung ein, dass die Zürcher Grossbank „Swissmoney“ das Ziel einer Denial of Service Attacke geworden ist. Der Angreifer hat Hans M. mit dem EFD eindeutig identifiziert.</p>
9.	2.12.01 15:00h	<p>Meldung des Telekommunikationsunternehmens „Directconnect“: Störung im Raum Gösgen behoben</p> <p>Die Störung des Mobilfunknetzes konnte schneller behoben werden als ursprünglich angenommen. Aufgrund einer Störung auf einer HW-Platine hat das redundante System die fehlerhaften Funktionen nicht kompensiert. Die Region rund um Gösgen ist wieder über das Mobilnetz erreichbar.</p>

10.	2.12.01 15.20h	<p>Meldung von „Swissmoney“</p> <p>Die Grossbank aus dem Raum Zürich teilt mit, dass Sie das Ziel einer Denial of Service Attacke geworden ist. Die Trading Services sind über Internet während mehrerer Stunden nicht mehr verfügbar.</p> <p>Aufgrund der Absenderadressen scheint es, dass der Angriff aus der Verwaltung lanciert wurde. Im Moment ist man daran, eine Kontaktperson im EFD zu suchen.</p>
11.	2.12.01 16:53h	<p>Nachricht des welschen Nachrichtensenders „Radio West“</p> <p>Im Raum Yverdon sind mehrere Personen mit Vergiftungserscheinungen im Krankenhaus eingeliefert worden. Die Symptome deuten auf ein Nervengift hin. Die Betroffenen klagen über starke Übelkeit, Brechreiz und Nasenfluss. Stark Betroffene müssen teilweise beatmet werden. Es scheint, als ob die Gifte über die Nahrungskette aufgenommen wurden.</p> <p>Der Nachrichtensender stellt diese Vergiftungserscheinungen in Zusammenhang mit den anonymen Emails, die in den letzten Tagen eingegangen sind. Die Polizei hat einen Supermarkt in Yverdon geschlossen, in denen einzelnen Betroffene in den letzten Tagen eingekauft haben. Die Spezialisten sind daran, die Produkte zu untersuchen.</p> <p>Weitere Lebensmittelläden rund um Yverdon bleiben weitgehend leer, währenddem die Einkaufscenter von Neuenburg und Freiburg erhöhte Frequenzen verzeichnen.</p>

12.	2.12.01 16:55h	<p>Netzsensoren von MELANI haben eine deutliche Zunahme des Netzwerkverkehrs festgestellt. Einzelne Knotenpunkte sind an der Kapazitätsgrenze angelangt und drohen zu kollabieren.</p> <p>Eine Schnellanalyse des Datenverkehrs hat ergeben, dass die Benutzer Reihenweise Emails an die Bekannten verschicken, denen eine Dokumentation zur Verhaltensanleitung gegenüber Vergiftungsfällen als Attachment angehängt ist. Das Email hat eine Grösse von 980KB und fällt damit durch die meisten Datenvolumenfilter der Mailserver.</p> <div data-bbox="507 674 1406 1272" style="text-align: center;"> <p>Netzwerk-Datenvolumen im Knoten Schweiz der letzten 30 Minuten</p> <table border="1"> <caption>Data points for the network utilization graph</caption> <thead> <tr> <th>Zeit</th> <th>Auslastung des Netzwerkknotens</th> </tr> </thead> <tbody> <tr><td>16:25</td><td>0.55</td></tr> <tr><td>16:27</td><td>0.55</td></tr> <tr><td>16:29</td><td>0.57</td></tr> <tr><td>16:31</td><td>0.55</td></tr> <tr><td>16:33</td><td>0.55</td></tr> <tr><td>16:35</td><td>0.68</td></tr> <tr><td>16:37</td><td>0.78</td></tr> <tr><td>16:39</td><td>0.82</td></tr> <tr><td>16:41</td><td>0.95</td></tr> <tr><td>16:43</td><td>0.98</td></tr> <tr><td>16:45</td><td>0.95</td></tr> <tr><td>16:47</td><td>0.97</td></tr> <tr><td>16:49</td><td>0.99</td></tr> <tr><td>16:51</td><td>0.98</td></tr> <tr><td>16:53</td><td>0.97</td></tr> <tr><td>16:55</td><td>0.98</td></tr> </tbody> </table> </div>	Zeit	Auslastung des Netzwerkknotens	16:25	0.55	16:27	0.55	16:29	0.57	16:31	0.55	16:33	0.55	16:35	0.68	16:37	0.78	16:39	0.82	16:41	0.95	16:43	0.98	16:45	0.95	16:47	0.97	16:49	0.99	16:51	0.98	16:53	0.97	16:55	0.98
Zeit	Auslastung des Netzwerkknotens																																			
16:25	0.55																																			
16:27	0.55																																			
16:29	0.57																																			
16:31	0.55																																			
16:33	0.55																																			
16:35	0.68																																			
16:37	0.78																																			
16:39	0.82																																			
16:41	0.95																																			
16:43	0.98																																			
16:45	0.95																																			
16:47	0.97																																			
16:49	0.99																																			
16:51	0.98																																			
16:53	0.97																																			
16:55	0.98																																			
13.	2.12.01 17:00h	<p>Meldung von Radio 2000</p> <p>Die Zürcher Grossbank „Swissmoney“ wurde in den letzten Stunden Opfer einer Attacke auf die Internet-Trading-Services. Gemäss den Aussagen eines Insiders ist der Ursprung der Attacke bei der Verwaltung zu suchen. Vom EFD war niemand für eine Stellungnahmen zu erreichen.</p>																																		
14.	2.12.01 17:15h	<p>Email „poisoned food in swiss malls“</p> <p>Es gehen weiterhin mehrere Emails pro Stunde mit diesem Titel bei MELANI ein.</p> <p>Gleichzeitig nimmt die Anzahl besorgter Anfragen zu, ob dies als HOAX zu bewerten ist oder nicht und wie dieses Email mit Yverdon nun tatsächlich in Verbindung steht.</p>																																		

15.	2.12.01 18:03	<p>Meldung von „Swissmoney“</p> <p>Nachdem die Server der Grossbank vom Netz genommen wurden, haben die Denial of Service Attacken sowohl bei Swissmoney wie auch beim EFD aufgehört. Die direkten Kontakte mit den Vertretern des EFD haben ergeben, dass die Attacke weder vom EFD noch von „Swissmoney“ gestartet wurde.</p> <p>Man vermutet, dass aussenstehende mittels IP-Spoofing gezielt versucht haben, die Internet-Services von „Swissmoney“ zu beeinträchtigen.</p>
16.	2.12.01 18:10h	<p>Medienmitteilung der Zürcher Stadtpolizei gesendet von Tele 7000</p> <p>Einzelne Personen im Glattzentrum sind mit Vergiftungserscheinungen in die Zürcher Klinik für Toxikologie eingeliefert worden. Laut den ersten Untersuchungen handelt es sich um schwache Nervengifte, die zu Übelkeit, Brechreiz und Nasenfluss führen – in seltenen Fällen zum Tod.</p> <p>Die Bürger und Bürgerinnen werden gebeten, Einkaufszentren zu meiden und bis zur Aufklärung der Vorfälle Notvorräte zu essen. Die Einwohner und Einwohnerinnen werden gebeten, Ihre Einkäufe in kleineren Läden zu tätigen und sowie Büchsenvorräte mit einem Abfülldatum von 1 Monat und älter zu kaufen.</p>
17.	2.12.01 18:30h	<p>Live-Beitrag von Tele 7000</p> <p>Es scheint eine Verbindung zu bestehen zwischen den Emails und den Vergiftungen im Raum Zürich und Yverdon. Es ist unklar, welche Lebensmittel betroffen sind. Ebenfalls gibt es unbestätigte Anzeichen, dass das Grundwasser verseucht sein könnte.</p> <p>In Zürich und Luzern werden die kleineren Läden panikartig leergekauft. Die Einkaufszentren in den grösseren Agglomerationen bleiben leer.</p>
18.	2.12.01 18:45h	<p>Bekennernachricht per Fax</p> <p>Gleichzeitig geht bei MELANI und mehreren Fernseh- und Radiostationen per Fax ein Bekenner schreiben zu den Emails und zu den Vergiftungen ein. Die Terroristen verlangen, dass die Schweizer und andere Regierungen ihre politische Haltung gegenüber dem nahen Osten und die Unterstützung der NATO überdenken. Die Schweiz sei nur ein Beispiel. Die gleichen Vergiftungen können in beliebigen anderen Ländern wiederholt werden – die Infrastruktur sei einsatzbereit.</p>

Hintergrund

<p>Motiv</p>	<p>Verunsicherung und Einschüchterung durch Falschinformationen werden dazu verwendet, einen Gegner zum politischen Umdenken zu bewegen.</p> <p>Kleinere Gruppierungen der verunsicherten Länder des nahen Ostens haben in eigener Initiative eine Abschreckungskampagne auf Terrorbasis gestartet. Es ist Ihre Absicht, dass sie von den westlichen Ländern als ernstzunehmende Gegner behandelt werden, so dass sie mit Verhandlungen eine friedensversprechende Nahost-Politik durch die westlichen Länder erreichen können.</p>
<p>Vorgehensplan</p>	<p>Die Gruppierungen zielen darauf ab, durch gezielte Informationen mit einer breiten Verteilung, welche mit wenigen physischen Aktionen zusammenhängen, Hysterie und Panik in der Bevölkerung auszulösen und damit die Führungsfähigkeit eines ganzen Staates zu beeinträchtigen. Um ihre Absicht zu untermauern, beabsichtigen Sie folgendes Vorgehen:</p> <p>Sie wählen die Schweiz, welches als Beispiel für alle umliegenden Länder dienen soll und welches als „neutrales“ Land nicht mit einer solchen Aktion rechnet.</p> <p>Beschaffung von Informationen über Lebensmittel-Produktionsstrassen von drei Schweizer Grossproduzenten über Einbrüche in die Computernetze. Diese Aktion soll möglichst verdeckt geschehen und nicht an die Öffentlichkeit gelangen, um die Aktion nicht zu gefährden.</p> <p>Falls die Ergebnisse dieser Informationsbeschaffung genügend Informationen darüber geben, wie auf einfache Art und Weise bereits in der Lebensmittelproduktion die Produkte mit toxikologischen Präparaten versetzt werden können, dann werden Sie dies direkt in den Produktionsstrassen machen. Andernfalls erfolgt die Vergiftung der Produkte in einzelnen Filialen.</p> <p>Mit einer gezielten Informationskampagne über Email wird ein Grossteil der Bevölkerung erreicht und verunsichert. Es wird erwartet, dass die ersten Meldungen als Hoax keine Beachtung finden. Dazu sollen mehrere unabhängige Server von mehreren Standorten aus über mehrere Tage Meldungen mit ähnlichen Inhalten generieren und an die wichtigsten und grössten Firmen schicken.</p> <p>Der Kummulationseffekt der Emails zusammen mit einigen wenigen Vergiftungserscheinungen in mehreren Ballungszentren soll in der breiten Bevölkerung Hysterie und Panik auslösen. Die Wirkung des Gifts soll nicht primär tödende Wirkung haben, die Betroffenen jedoch für mehrere Tage ausser Gefecht setzen.</p>

Zweck	Das Szenario zielt darauf ab zu erkennen, wie MELANI mit inhaltlichen Risiken umgehen kann und was für Möglichkeiten MELANI in den verschiedenen Stadien der Eskalation hat. Dabei ist vorallem rückblickend von Interesse, was bei einer zeitgerechten Intervention vermeidbar gewesen wäre.
-------	---

Szenario 2: Illegale Banktransaktionen

Einleitung		<p>Es zeigt sich, dass in Krisenzeiten aufgrund der starken Frankenwährung grosse Geldströme in die Schweiz fliessen.</p> <p>Aus diesem Grund werden in der Schweiz immer wieder Konten von mutmasslichen Kriminellen festgestellt und blockiert. Im Anschluss an die Attentate wurden umfangreiche Abklärungen initiiert, welche die Konten und Geldflüsse von Kriminellen aufspüren sollen. Im Rahmen dieser Kontrollmechanismen hat man schweizweit festgelegt, dass einzelne Transaktionen über 500'000.—CHF, mehrere über 100'000.—CHF vom gleichen Konto und Konten über 15 Mio. CHF überprüft werden müssen.</p> <p>Die Kooperation zwischen der Bankenkommission und ausländischen Geheimdiensten funktioniert gut – das Bankgeheimnis ist aufgrund der guten Zusammenarbeit im Moment kein Thema.</p> <p>Die letzten paar Tage hat MELANI keine ausserordentlichen Vorkommnisse feststellen können. Die Datenvolumina in den ISP Knotenpunkten sind normal.</p>
Nr.	Meldungseingang	<i>Meldungen, welche bei MELANI eingehen</i>
1.	4.12.01 13.15h	<p>Mitteilung der Grossbank „Tradequotes“</p> <p>Das Finanzportal von Tradequotes wurde Ziel einer erfolgreichen Hacking-Attacke. Die Angreifer haben es geschafft, die Firewall und den Proxy-Server zu überwinden. Die Einbrecher sind jedoch durch ein Intrusion Detection System erfasst worden. Es wurden sofort Gegenmassnahmen eingeleitet. Der Schaden konnte vollends abgewehrt werden. Die technischen Verantwortlichen garantieren nach wie vor eine einwandfreie Funktionalität des Finanzportals. Sie geben zudem eine Garantie ab, dass durch den Einbruch keine illegalen Transaktionen getätigt wurden.</p> <p>Die Polizei wurde eingeschaltet. Sie sind im Moment daran, die Angreifer aufzuspüren</p>

2.	4.12.01 13.35h	<p>Mitteilung der Betreiberin des Kernkraftwerks „Powerline“</p> <p>Die Regelung des Kernkraftwerks ist für Sekundenbruchteile komplett ausgefallen. Aufgrund von Unsicherheiten über den weiteren Verlauf der Regelung durch das System haben die verantwortlichen Techniker eine Notabschaltung eingeleitet.</p> <p>Es wird vermutet, dass die Korrelation eines Hardwarefehlers mit dem bekannten Redundanzaktivierungsproblem die Ursache für diesen kurzzeitigen Ausfall gewesen ist. Die Hersteller wurden kontaktiert. Die Betreiberin geht davon aus, dass das Kernkraftwerk in zwei Tagen wieder ans Netz gehen kann.</p>
3.	4.12.01 16:30h	<p>Pressecommuniqué der Bankenkommission</p> <p>Die Bankenkommission veröffentlicht einen Bericht über die Nachforschungen bezüglich der kriminellen Transaktionen. Gemäss Aussage des Ausschussleiters hat man einige Konten sicherstellen können. Man ist zur Zeit daran, mehrere Tausend Transaktionen zu überprüfen.</p> <p>Zum aktuellen Zeitpunkt sind sehr viele Transaktionen mit sehr hohen Summen im Gange, die laufend überprüft werden. Allerdings sind bisher keine Indizien aufgetaucht, die auf illegale Transaktionen hinweisen.</p>
4.	4.12.01 21:00h	<p>Mitteilung der Grossbank „Rentability“</p> <p>Das Finanzportal von Rentability wurde Ziel einer Hacking-Attacke. Der Einbruch wurde durch das Einbruchsüberwachungssystem entdeckt. Es wurden Sofortmassnahmen eingeleitet, bevor der Angreifer merklichen Schaden anrichten konnte. Laut den Aufzeichnungen wurde der Einbrecher gestoppt, als er in das zentrale Authentifizierungssystem einbrechen wollte.</p> <p>Die Bank hat daraufhin die Services vom Netz genommen und hat die Überprüfung der internen Systeme angeordnet. Ausser dass das Loggfile der Aktivitäten manipuliert wurde, konnten keine Veränderungen am internen System festgestellt werden. Es gibt Anzeichen, dass gezielte Lächer im Firewall-System den Zugriff ermöglicht haben. Der Patch für die Firewall wurde bereits installiert. Die Systeme werden voraussichtlich in zwei Stunden wieder ans Netz gehen.</p> <p>Es wurden polizeiliche Ermittlungen eingeleitet, die auf den Ursprung des Angriffs führen sollen. Der Angriff scheint über mehrere Relaisstationen geführt zu sein. Die Nachforschungen gestalten sich schwierig.</p>

5.	5.12.01 09:15h	<p>Mitteilung der Handelsfirma „Counter“</p> <p>Gemäss Aussagen der Geschäftsleitung hat sich die Finanzabteilung mehrere Millionen CHF unterschlagen. Mehrere Mitarbeiter sind in Untersuchungshaft genommen worden.</p> <p>Die Mitarbeiter beteuern ihre Unschuld. Die Bank ist daran, im Rahmen ihrer Nachforschungen mehrere hundert Zielkonten im In- und Ausland überprüfen und allenfalls sperren zu lassen. Die Arbeit wird einige Wochen Zeit in Anspruch nehmen.</p>
6.	5.12.01 13.10h	<p>Mitteilung de Finanzportals „Cashpay“</p> <p>Das Finanzportal hat aufgrund einer Denial of Service Attacke den Betrieb vorübergehend eingestellt. Die Angreifer haben es vor allem auf die externe Firewall abgesehen, welche dann gezielt attackiert wurde.</p> <p>Die IT-Verantwortlichen haben den Notfallplan anlaufen lassen und organisieren einen Ersatz der Firewall, so dass das System in vier Stunden wieder lauffähig ist.</p>
7.	5.12.01 13.30h	<p>Reportage von Tele 7000</p> <p>Zürich: Es werden aufgebrachte Kunden gezeigt, die mit Ihren Kontoauszügen vor der Bank „Cashpay“ stehen und sich beschweren. In Interviews mit den Kunden wird erklärt, dass auf den Kundenkonten illegale Mutationen durchgeführt wurden und dass die Bank von legalen Transaktionen spricht.</p>
8.	5.12.01 15:00h	<p>Mitteilung der Grossbank „Cashpay“</p> <p>Einige Benutzer des Finanzportals haben sich bei der Bank beschwert, dass über ihre Konten mehrere Transaktionen von x-tausend CHF getätigt wurden, welche sie sich nicht erklären können. Die Transaktionen wurden so oft wiederholt, bis das Konto saldiert war.</p> <p>Beinahe gleichzeitig haben sich Firmenkunden über Konten-Mutationen beschwert. Den betroffenen Banken sind keine Angriffe bekannt. Die Auswertung der Loggfiles ergibt, dass ausschliesslich rechtmässige Transaktionen getätigt wurden. Sie lassen die aufgebrachten Kunden abblitzen und verweisen auf die Sorgfaltspflicht zur Aufbewahrung von Konteninformationen.</p>

9.	5.12.01 17:00h	<p>Pressemitteilung der Zentralschweizerischen Bus AG</p> <p>Aufgrund von plötzlichen und unerklärlichen Liquiditätsproblemen muss die sonst schon angeschlagene Bus AG den Betrieb vorübergehend einstellen. Es werden interne Untersuchungen angeordnet. Die Angestellten können sich diese Situation nicht erklären und belagern den Hauptsitz der Bus AG. Es droht der Konkurs.</p>
10.	6.12.01 10:00h	<p>Reportage Radio „Allnight “</p> <p>Luzern: Auch in der Innerschweiz stehen aufgebrachte Bürger vor den Banken „Tradequotes“ und „Richmond“ und sorgen sich um ihre Guthaben. Die Banken haben noch keine Stellung zum Vorwurf der illegalen Konten-Mutationen genommen.</p> <p>Zug: Vor den Bankomaten bilden sich zu später Abendstunde grosse Menschaufläufe, welche sich Bargeld beschaffen wollen. Die Bankomaten sind jedoch kurze Zeit später leer.</p> <p>Basel: Auch in Basel sind Menschengeschlangen vor den Bankomaten zu sehen, welche sich kurze Zeit später wieder auflösen, da der spezifische Bankomat leer ist. Prügeleien um die Reihenfolge an den Bankomaten häufen sich. Die Bürger sehen sich in ihrer Existenz bedroht und werden handgreiflich. Die Polizei hat Mühe, die aufgebrachten Bürger zu beruhigen.</p>
11.	6.12.01 13:20h	<p>Mitteilung der Grossbank „Rentability“</p> <p>Bei der Überprüfung der internen Systeme ist ein modifiziertes Applet aufgefallen, welches scheinbar durch die Angreifer bewusst auf den Applikationsservern platziert wurde. Die Funktionalität der Software konnte noch nicht ausgewertet werden. MELANI bietet sich an, die Koordination der Softwareanalyse zu übernehmen.</p>
12.	6.12.01 14:00h	<p>Live Reportage Tele 7000</p> <p>Es werden Agglomerationen gezeigt, in denen randaliert wird. Fensterscheiben von Shops werden eingeschlagen und Vitrinen werden ausgeraubt.</p> <p>Die Polizei reagiert mit einem erhöhten Aufgebot an Beamten.</p>

13.	6.12.01 16:00h	<p>Die IT-Firma „Halter“ informiert MELANI</p> <p>Einige der Mitarbeiter sind ebenfalls Opfer der jüngste Vorkommnisse geworden.</p> <p>Nun machen Gerüchte die Runde, dass einzelne Betroffene ein Email erhalten haben, welches ein Tool enthält, mit dem der Zugriff auf andere Konten ermöglicht wird. Dadurch sind sie in der Lage, Geld-Transaktionen auf fremden Konten zu ihren eigenen Gunsten zu tätigen.</p> <p>Die Betroffenen sitzen nun vor ihrem Email-Tool und warten, dass sie die Möglichkeit erhalten, solche illegalen Transaktionen auf anderen Konten durchführen zu können. Der Verteilmechanismus der Emails ist nicht klar.</p>
14.	6.12.01 19:20h	<p>MELANI stellt fest, dass dieses Applet fähig ist, die Sandbox der Java Virtual Machine im Browser zu verlassen und die Browserkonfiguration zu verändern. Beim nächsten Mal aufstarten wird im Browser auf die bekanntesten Websites von Finanzportalen getriggert und im Falle einer Übermittlung die Verbindung abgebrochen. Die Daten im Inhalt der Website werden verschlüsselt an eine externe Stelle übertragen.</p>

Hintergrund

Motiv	<p>Die jüngsten Terrorereignisse haben eine Welle an Untersuchungen ausgelöst, von denen auch die Bankbranche in der Schweiz betroffen ist. Verschiedene Mafia-ähnliche Organisationen haben umfassende finanzielle Mittel bei Schweizer Finanzinstituten in der Schweiz platziert und befürchten, dass diese Gelder aufgrund des zentralen Transaktionspunktes „Schweiz“ gefährdet sein könnten.</p> <p>Aus Insiderquellen wissen diese Gruppierungen, dass Transaktionen über 500'000 CHF überprüft werden. Ebenso ist ihnen bewusst, dass es eine Frage der Zeit ist, bis ihre Konten aufgespürt werden. Aus diesem Grund wagen sie es nicht, diese Transaktionen in Millionenhöhe auf andere Banken im Ausland zu übertragen.</p> <p>Das Ziel ist es, ein Ablenkungsmanöver zu starten, welches die Prioritäten der Analysen verlagert, so dass Zeit gewonnen werden kann, die benötigt wird, um das Anlagekonzept so anzupassen und umzusetzen, dass sie durch die Maschen der Kontrollkonzepts fallen.</p>
Vorgehensplan	<p>Vor wenigen Tagen haben Studenten an einer Universität in Bruxelles herausgefunden, dass die Sandbox⁸ der Java-Virtual-Maschine fehlerhaft ist und die Sicherheitsmassnahmen durch gezielte Applet-Codesequenzen umgangen werden können.</p> <p>Die Studenten pflegen Kontakt zu spezifischen Untergrundbewegungen.</p> <p>Sie spielen ihren Landsleuten ein modifiziertes Applet in die Hände, die auf Anwendungsservern von Finanzportalen installiert werden müssen. Die von den Clients geladenen Applets interceptieren die Loginversuche der Kunden (Vertragsnummer, Pincode, und Streichlistennummer oder Secure-Id) und schicken die Informationen verschlüsselt an einen fremden Server. Die Verbindung zum Finanzportal wird daraufhin abgebrochen, bevor der Login-Versuch abgeschickt wurde.</p> <p>In den Programmverzeichnissen der Browser wird zudem der Programmcode so geändert, dass ein zukünftiger Aufruf des Finanzportals auf eine Seite verwiesen wird, die so aussieht, als ob es eine offizielle Meldung des Finanzinstituts wäre, dass das Portal im Moment nicht zur Verfügung steht. In allen anderen Fällen ist der Browser normal bedienbar.</p> <p>Vorgehen:</p> <ol style="list-style-type: none"> 1. Möglichst gleichzeitige Attacke auf mehrere Applikationsservern von Finanzinstituten. Öffnen einer Verbindung auf den Applikationsser-

⁸ Sandbox: Die Java-Virtual-Maschine der Browser erlaubt Applets keine Zugriffe auf die Hardware. Diese Sicherheitseigenschaften nützen die meisten Applikationen im eCommerce und eBusiness aus.

	<p>ver.</p> <ol style="list-style-type: none">2. Installation eines modifizierten Applets mit einer spezifischen Code-sequenz, welches die Java Virtual Machine als Sandbox unbrauchbar macht. Die Integritätsdatenbank muss im Anschluss daran aufdatiert werden und alle Logaktivitäten gelöscht werden, so dass die Veränderungen nicht detektiert werden können.3. Die Verbindungen von Kunden (Privat und Firmenkunden) werden abgefangen. Daraufhin wird die Verbindung mit dem Kunden abgebrochen. Die Login-Informationen werden unmittelbar selber verwendet, um in das System einzuloggen. Mehrere Transaktionen mit vorgegebenen Zielkonten werden gestartet.4. Hotline Anrufe besorgter Kunden werden die Hotlines damit beantworten, dass die Site problemlos funktioniert und dass sie doch den hausinternen Administrator kontaktieren sollen. Pendente Zahlungen werden erst am folgenden Tag ausgeführt, welche die Kunden über die Hotline kaum überprüfen werden. Den Kunden fehlen die Kontrollinstrumente, um zu wissen, was auf Ihrem Konto abgeht.5. Falls die Kunden sogleich auf einem anderen Computer probieren, die Verbindung zum Finanzportal aufzubauen, wird die Session wieder geklaut und man hat die nächste Streichlistennummer oder Secure-Id Nummer.6. Nach einigen Tagen werden die Benutzer neugierig und verlangen von den Finanzportalen Erklärungen zu den Ausfällen. Man wird die Ursache jedoch nicht im System sondern vielmehr bei den Usern suchen.7. Sobald genügend Transaktionen durch diese Gruppierung getätigt und die eigenen Gelder umgeschichtet wurden, wird das Tool zusammen mit neuen individuellen Konteninformationen (nur Kontoinformationen mit Streichlistennummer) an diejenigen Personen versendet, welche durch vorgängige Transaktionen geschädigt wurden. Damit wird erreicht, dass die unrechtmässig Geschädigten die Möglichkeit erhalten, sich auch unrechtmässig bereichern zu können. Damit können sie aus subjektiver Sicht die Gerechtigkeit wieder herstellen. Das Tool wird mit der Anweisung verschickt, wie das Tool anzuwenden ist, um auf fremde Konten zugreifen zu können.
--	---

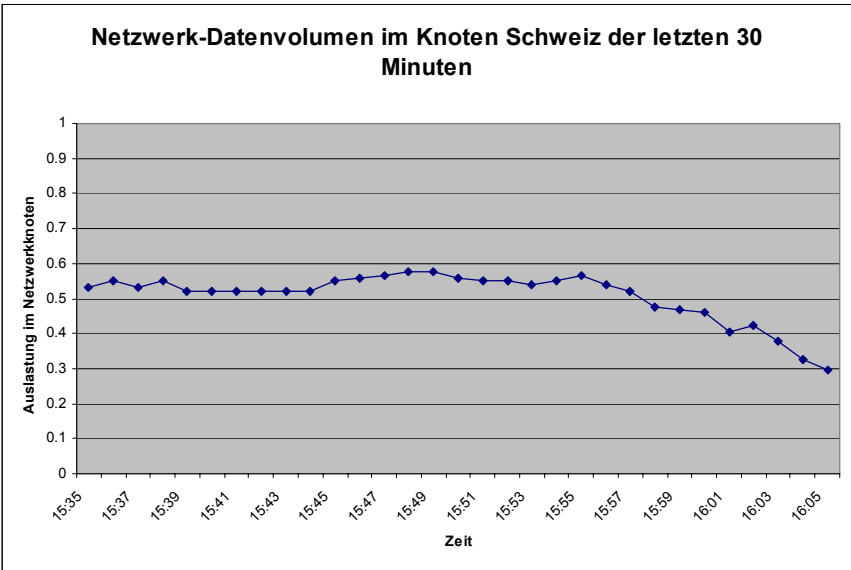
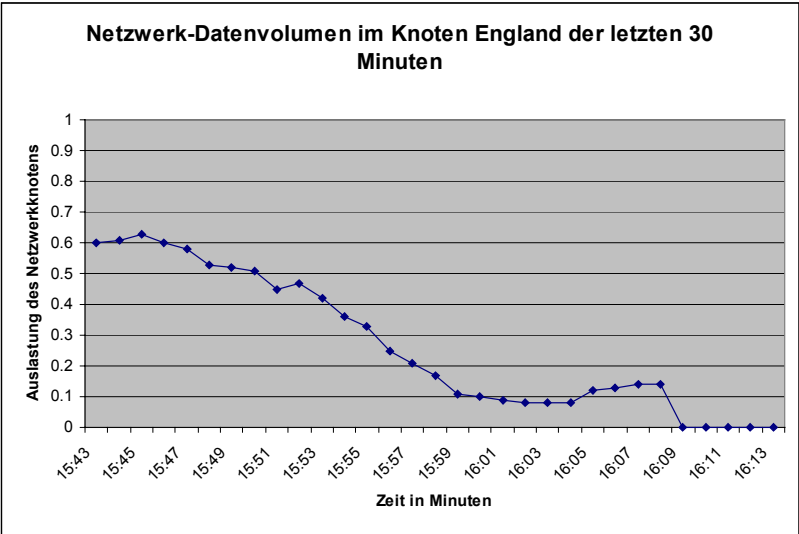
Zweck	<p>Dieses Szenario zielt darauf ab, ein aufgebautes Axiom zu widerlegen. Die „Sandbox“ der Java Virtual Machine, auf deren Eigenschaften wichtige Webapplikationen basieren, erfüllt die Sicherheitsanforderungen für Transaktionen nicht gemäss Definition.</p> <p>Die Bankbranche als einer der wichtigsten Sektoren in unserem Land soll diskreditiert werden. Die Folgen ist ein immenser Vertrauensverlust und ein sehr grosser Imageschaden.</p>
-------	--

Szenario 3: Krise aufgrund von Indizien

<p>Einleitung</p>	<p>MELANI pflegt Kontakte zu internationalen Betreibern von Netzwerkinfrastrukturen und hat dadurch Zugriff auf die aktuellen Statistiken der Datenvolumen in den Netzknoten.</p> <div data-bbox="507 577 1321 1126" style="text-align: center;"> <p>Netzwerk-Datenvolumen im Knoten England der letzten 30 Stunden</p> <table border="1"> <caption>Data points for the line chart (approximate values)</caption> <thead> <tr> <th>Zeit</th> <th>Auslastung des Netzknoten</th> </tr> </thead> <tbody> <tr><td>09:00</td><td>0.60</td></tr> <tr><td>10:00</td><td>0.60</td></tr> <tr><td>11:00</td><td>0.55</td></tr> <tr><td>12:00</td><td>0.50</td></tr> <tr><td>13:00</td><td>0.55</td></tr> <tr><td>14:00</td><td>0.60</td></tr> <tr><td>15:00</td><td>0.60</td></tr> <tr><td>16:00</td><td>0.60</td></tr> <tr><td>17:00</td><td>0.60</td></tr> <tr><td>18:00</td><td>0.60</td></tr> <tr><td>19:00</td><td>0.55</td></tr> <tr><td>20:00</td><td>0.50</td></tr> <tr><td>21:00</td><td>0.40</td></tr> <tr><td>22:00</td><td>0.40</td></tr> <tr><td>23:00</td><td>0.45</td></tr> <tr><td>00:00</td><td>0.45</td></tr> <tr><td>01:00</td><td>0.40</td></tr> <tr><td>02:00</td><td>0.50</td></tr> <tr><td>03:00</td><td>0.60</td></tr> <tr><td>04:00</td><td>0.75</td></tr> <tr><td>05:00</td><td>0.70</td></tr> <tr><td>06:00</td><td>0.70</td></tr> <tr><td>07:00</td><td>0.68</td></tr> <tr><td>08:00</td><td>0.68</td></tr> <tr><td>09:00</td><td>0.68</td></tr> <tr><td>10:00</td><td>0.70</td></tr> <tr><td>11:00</td><td>0.75</td></tr> <tr><td>12:00</td><td>0.80</td></tr> <tr><td>13:00</td><td>0.75</td></tr> <tr><td>14:00</td><td>0.65</td></tr> <tr><td>15:00</td><td>0.60</td></tr> </tbody> </table> </div> <p>In den letzten Tagen sind einige Schwankungen in den Netzvolumen aufgetreten, die durch Belastungstests aufgetreten sind. Diese Tests wurden von verschiedenen CERTS über Nacht aufgrund von Gerüchten über Instabilitäten im Internet durchgeführt. Die Tests sind offiziell abgeschlossen. Die Resultate widerlegen die Gerüchte und der Betrieb aus Sicht von MELANI läuft wieder normal.</p>	Zeit	Auslastung des Netzknoten	09:00	0.60	10:00	0.60	11:00	0.55	12:00	0.50	13:00	0.55	14:00	0.60	15:00	0.60	16:00	0.60	17:00	0.60	18:00	0.60	19:00	0.55	20:00	0.50	21:00	0.40	22:00	0.40	23:00	0.45	00:00	0.45	01:00	0.40	02:00	0.50	03:00	0.60	04:00	0.75	05:00	0.70	06:00	0.70	07:00	0.68	08:00	0.68	09:00	0.68	10:00	0.70	11:00	0.75	12:00	0.80	13:00	0.75	14:00	0.65	15:00	0.60
Zeit	Auslastung des Netzknoten																																																																
09:00	0.60																																																																
10:00	0.60																																																																
11:00	0.55																																																																
12:00	0.50																																																																
13:00	0.55																																																																
14:00	0.60																																																																
15:00	0.60																																																																
16:00	0.60																																																																
17:00	0.60																																																																
18:00	0.60																																																																
19:00	0.55																																																																
20:00	0.50																																																																
21:00	0.40																																																																
22:00	0.40																																																																
23:00	0.45																																																																
00:00	0.45																																																																
01:00	0.40																																																																
02:00	0.50																																																																
03:00	0.60																																																																
04:00	0.75																																																																
05:00	0.70																																																																
06:00	0.70																																																																
07:00	0.68																																																																
08:00	0.68																																																																
09:00	0.68																																																																
10:00	0.70																																																																
11:00	0.75																																																																
12:00	0.80																																																																
13:00	0.75																																																																
14:00	0.65																																																																
15:00	0.60																																																																
Nr.	Meldungseingang	<i>Ereigniszeitpunkt / Meldungen, welche bei MELANI eingehen</i>																																																															
1.	15.12.01 08:13h	Ein Logistikunternehmen meldet, dass drei zentrale interne Server, auf denen ein Workflow Management System läuft, beinahe gleichzeitig heruntergefahren wurden. Die Geschäftsprozesse stehen still. Eine erste Analyse hat ergeben, dass die Ursache nicht in der Notstromversorgung liegt, die die Server heruntergefahren haben. Die effektive Ursache ist weiterhin unbekannt. Der Notfallplan ist angelaufen – man steht in Kontakt mit ASP's, um die gesamte Rechenzentrum-Funktionalität auf einem Alternativsystem aufzubauen.																																																															

2.	15.12.01 15:53h	<p>Der Netzwerkknoten in England, der zusammen mit drei anderen Knoten in Belgien und Spanien die Triage des Netzwerkverkehrs mit Amerika durchführen, hatte in den letzten Minuten folgenden Verlauf:</p> <div data-bbox="507 443 1348 1003" style="text-align: center;"> <p>Netzwerk-Datenvolumen im Knoten England der letzten 30 Minuten</p> <table border="1"> <thead> <tr> <th>Zeit</th> <th>Auslastung des Netzwerkknotens</th> </tr> </thead> <tbody> <tr><td>15:23</td><td>0.65</td></tr> <tr><td>15:25</td><td>0.62</td></tr> <tr><td>15:27</td><td>0.58</td></tr> <tr><td>15:29</td><td>0.62</td></tr> <tr><td>15:31</td><td>0.58</td></tr> <tr><td>15:33</td><td>0.58</td></tr> <tr><td>15:35</td><td>0.58</td></tr> <tr><td>15:37</td><td>0.62</td></tr> <tr><td>15:39</td><td>0.65</td></tr> <tr><td>15:41</td><td>0.62</td></tr> <tr><td>15:43</td><td>0.60</td></tr> <tr><td>15:45</td><td>0.62</td></tr> <tr><td>15:47</td><td>0.60</td></tr> <tr><td>15:49</td><td>0.55</td></tr> <tr><td>15:51</td><td>0.52</td></tr> <tr><td>15:53</td><td>0.42</td></tr> </tbody> </table> </div> <p>Nachdem man um 15:51LT einen markanter Abfall des Netzwerk-Verkehrsvolumen festgestellt hat, hat MELANI erfolglos versucht mit den zuständigen Personen in England über Internet Kontakt aufzunehmen. Es ist jedoch kein Netzwerkverkehr möglich. Das Internet scheint in England nicht verfügbar zu sein. Einzelne Ping-Versuche an bekannte IP Adressen funktionieren.</p>	Zeit	Auslastung des Netzwerkknotens	15:23	0.65	15:25	0.62	15:27	0.58	15:29	0.62	15:31	0.58	15:33	0.58	15:35	0.58	15:37	0.62	15:39	0.65	15:41	0.62	15:43	0.60	15:45	0.62	15:47	0.60	15:49	0.55	15:51	0.52	15:53	0.42
Zeit	Auslastung des Netzwerkknotens																																			
15:23	0.65																																			
15:25	0.62																																			
15:27	0.58																																			
15:29	0.62																																			
15:31	0.58																																			
15:33	0.58																																			
15:35	0.58																																			
15:37	0.62																																			
15:39	0.65																																			
15:41	0.62																																			
15:43	0.60																																			
15:45	0.62																																			
15:47	0.60																																			
15:49	0.55																																			
15:51	0.52																																			
15:53	0.42																																			
3.	15.12.01 16:01h	<p>Meldung des Schweizer Telekommunikationsunternehmens „Swissun“</p> <p>Die Verbindung nach Amerika und England ist abgebrochen. Der Routing-Prozess für englische und amerikanische Datenpakete endet jeweils mit Fehlermeldungen.</p>																																		
4.	15.12.01 16:04h	<p>Bei MELANI läuft das Telefon heiss. Firmen, die stark auf den Bereich eCommerce und eBusiness setzen, verlangen Auskunft über die jüngsten Vorfälle. Von Seiten der Firmen wird gleichzeitig mitgeteilt, dass einige Verbindungspartner mit .com und .net nicht mehr im Internet erreichbar sind.</p>																																		

5.	15.12.01 16:10h	<p>MELANI stellt fest, dass auch im Schweizer Knoten ein markanter Netzwerk-Datenvolumenabfall zu verzeichnen ist. Der Verlauf ähnelt dem des Knoten in England. Allerdings hat die Verkehrsabnahme von England auch einen Einfluss auf das Schweizer Volumen. Die zeitliche Verzögerung zeigt auf, dass das Problem langsam von Amerika herkommend in Richtung Europa wandert.</p> <div data-bbox="507 562 1386 1140" data-label="Figure"> <p style="text-align: center;">Netzwerk-Datenvolumen im Knoten England der letzten 30 Minuten</p> <table border="1"> <caption>Data points for the network data volume graph</caption> <thead> <tr> <th>Zeit</th> <th>Auslastung im Netzwerknoten</th> </tr> </thead> <tbody> <tr><td>15:38</td><td>0.65</td></tr> <tr><td>15:40</td><td>0.64</td></tr> <tr><td>15:42</td><td>0.61</td></tr> <tr><td>15:44</td><td>0.61</td></tr> <tr><td>15:46</td><td>0.63</td></tr> <tr><td>15:48</td><td>0.58</td></tr> <tr><td>15:50</td><td>0.52</td></tr> <tr><td>15:52</td><td>0.46</td></tr> <tr><td>15:54</td><td>0.42</td></tr> <tr><td>15:56</td><td>0.33</td></tr> <tr><td>15:58</td><td>0.21</td></tr> <tr><td>16:00</td><td>0.10</td></tr> <tr><td>16:02</td><td>0.08</td></tr> <tr><td>16:04</td><td>0.08</td></tr> <tr><td>16:06</td><td>0.12</td></tr> <tr><td>16:08</td><td>0.14</td></tr> </tbody> </table> </div>	Zeit	Auslastung im Netzwerknoten	15:38	0.65	15:40	0.64	15:42	0.61	15:44	0.61	15:46	0.63	15:48	0.58	15:50	0.52	15:52	0.46	15:54	0.42	15:56	0.33	15:58	0.21	16:00	0.10	16:02	0.08	16:04	0.08	16:06	0.12	16:08	0.14
Zeit	Auslastung im Netzwerknoten																																			
15:38	0.65																																			
15:40	0.64																																			
15:42	0.61																																			
15:44	0.61																																			
15:46	0.63																																			
15:48	0.58																																			
15:50	0.52																																			
15:52	0.46																																			
15:54	0.42																																			
15:56	0.33																																			
15:58	0.21																																			
16:00	0.10																																			
16:02	0.08																																			
16:04	0.08																																			
16:06	0.12																																			
16:08	0.14																																			
6.	15.12.01 16:12h	<p>Meldungen diverser eCommerce-Firmen</p> <p>Auf dem Internet geht beinahe nichts mehr. Die Verbindungen können nur noch über direkte IP-Adressen aufgebaut werden.</p>																																		

7.	15.12.01 16:20h	<p>MELANI stellt fest, dass keine Datenpakete aus England und Amerika mehr eintreffen. Das Verkehrsvolumen im Knoten England nimmt weiter ab. Einzelne Ping-Kommando's sind immer noch möglich. Das Datenvolumen steigt am Ende leicht an, was zu Hoffnungen führt, dass es nur eine vorübergehende Instabilität des Internet war.</p>																																		
<p style="text-align: center;">Netzwerk-Datenvolumen im Knoten Schweiz der letzten 30 Minuten</p>  <table border="1"> <caption>Data for Netzwerk-Datenvolumen im Knoten Schweiz</caption> <thead> <tr> <th>Zeit</th> <th>Auslastung im Netzwerkknoten</th> </tr> </thead> <tbody> <tr><td>15:35</td><td>0.55</td></tr> <tr><td>15:37</td><td>0.56</td></tr> <tr><td>15:39</td><td>0.54</td></tr> <tr><td>15:41</td><td>0.53</td></tr> <tr><td>15:43</td><td>0.53</td></tr> <tr><td>15:45</td><td>0.52</td></tr> <tr><td>15:47</td><td>0.56</td></tr> <tr><td>15:49</td><td>0.58</td></tr> <tr><td>15:51</td><td>0.55</td></tr> <tr><td>15:53</td><td>0.55</td></tr> <tr><td>15:55</td><td>0.54</td></tr> <tr><td>15:57</td><td>0.56</td></tr> <tr><td>15:59</td><td>0.52</td></tr> <tr><td>16:01</td><td>0.46</td></tr> <tr><td>16:03</td><td>0.42</td></tr> <tr><td>16:05</td><td>0.30</td></tr> </tbody> </table>			Zeit	Auslastung im Netzwerkknoten	15:35	0.55	15:37	0.56	15:39	0.54	15:41	0.53	15:43	0.53	15:45	0.52	15:47	0.56	15:49	0.58	15:51	0.55	15:53	0.55	15:55	0.54	15:57	0.56	15:59	0.52	16:01	0.46	16:03	0.42	16:05	0.30
Zeit	Auslastung im Netzwerkknoten																																			
15:35	0.55																																			
15:37	0.56																																			
15:39	0.54																																			
15:41	0.53																																			
15:43	0.53																																			
15:45	0.52																																			
15:47	0.56																																			
15:49	0.58																																			
15:51	0.55																																			
15:53	0.55																																			
15:55	0.54																																			
15:57	0.56																																			
15:59	0.52																																			
16:01	0.46																																			
16:03	0.42																																			
16:05	0.30																																			
8.	15.12.01 16:30h	<p>Währenddem die Netzwerk-Datenvolumen auf dem Schweizer Knoten ähnlich den Vorgaben aus England fallen, bricht die Kommunikation mit dem Knoten in England vollends ab. Gleichzeitig sind keine Verbindungen über das Internet mehr möglich. Auch ping-Befehle sind ausserhalb der Grenzen von MELANI blockiert</p>																																		
<p style="text-align: center;">Netzwerk-Datenvolumen im Knoten England der letzten 30 Minuten</p>  <table border="1"> <caption>Data for Netzwerk-Datenvolumen im Knoten England</caption> <thead> <tr> <th>Zeit in Minuten</th> <th>Auslastung des Netzwerkknotens</th> </tr> </thead> <tbody> <tr><td>15:43</td><td>0.60</td></tr> <tr><td>15:45</td><td>0.65</td></tr> <tr><td>15:47</td><td>0.60</td></tr> <tr><td>15:49</td><td>0.55</td></tr> <tr><td>15:51</td><td>0.52</td></tr> <tr><td>15:53</td><td>0.48</td></tr> <tr><td>15:55</td><td>0.42</td></tr> <tr><td>15:57</td><td>0.35</td></tr> <tr><td>15:59</td><td>0.25</td></tr> <tr><td>16:01</td><td>0.15</td></tr> <tr><td>16:03</td><td>0.10</td></tr> <tr><td>16:05</td><td>0.10</td></tr> <tr><td>16:07</td><td>0.12</td></tr> <tr><td>16:09</td><td>0.13</td></tr> <tr><td>16:11</td><td>0.00</td></tr> <tr><td>16:13</td><td>0.00</td></tr> </tbody> </table>			Zeit in Minuten	Auslastung des Netzwerkknotens	15:43	0.60	15:45	0.65	15:47	0.60	15:49	0.55	15:51	0.52	15:53	0.48	15:55	0.42	15:57	0.35	15:59	0.25	16:01	0.15	16:03	0.10	16:05	0.10	16:07	0.12	16:09	0.13	16:11	0.00	16:13	0.00
Zeit in Minuten	Auslastung des Netzwerkknotens																																			
15:43	0.60																																			
15:45	0.65																																			
15:47	0.60																																			
15:49	0.55																																			
15:51	0.52																																			
15:53	0.48																																			
15:55	0.42																																			
15:57	0.35																																			
15:59	0.25																																			
16:01	0.15																																			
16:03	0.10																																			
16:05	0.10																																			
16:07	0.12																																			
16:09	0.13																																			
16:11	0.00																																			
16:13	0.00																																			

9.	15.12.01 16:45h	Status MELANI Das Telefon sowie der Fax funktionieren nicht mehr. Die Fehlersuche gestaltet sich sehr schwierig, da es scheint, als ob die Probleme ausserhalb von MELANI und auch ausserhalb der Firmen liegen und deshalb nicht direkt analysiert werden können.
10.	15.12.01 17:30h	Aktion MELANI MELANI nimmt nach einer internen Krisensitzung vor Ort Kontakt auf mit den Telekommunikationsanbietern. Diese teilen MELANI mit, dass sie gleichzeitig mit zwei Problemen zu kämpfen haben. <ol style="list-style-type: none">1. Einerseits müssen sie dringend einen Patch für die defekte Software von neuralgischen Routern haben, damit zumindest die Routingfunktionalität wieder gewährleistet ist. Wie gelangt man zu diesem Patch, wenn das Internet keine Download-Möglichkeiten zur Verfügung stellt?2. Es besteht ein DNS-Problem. Die DNS-Server können keine Namen auflösen.

Hintergrund

<p>Motiv</p>	<p>Die Kluft in der Geisteshaltung zwischen den Regierungen und den Bevölkerungen im asiatischen Raum wird in Hinblick auf die Aktivitäten im nahen Osten zunehmend grösser.</p> <p>Kompetente Mitglieder von verschiedenen regionalen Computerclubs haben sich zusammengeschlossen und planen verdeckte Massnahmen. Dies einerseits um ihren Unmut Ausdruck zu verleihen und andererseits um ihre schwache Wirtschaftslage gegenüber der westlichen besser zu positionieren.</p> <p>Sie planen einen Anschlag gegen die IT-Infrastruktur der westlichen Länder. Die Prozesse der Firmen, die über das Internet ablaufen, sollen massiv eingeschränkt werden. Die Massnahmen zielen primär auf die Verfügbarkeit der IT-Infrastruktur, wobei sich der Effekt sofort auf andere Bereiche (Business Prozesse, Notdienste, Telefondienste) ausdehnen soll.</p> <p>Als Folge davon soll die Wirtschaft in den betroffenen Ländern durch diese Aktionen kurzfristig empfindlich geschwächt werden, indem die Kommunikation lahmgelegt wird.</p> <p>Die Regierungen sollen gezwungen werden, sich auf die Innenpolitik und auf die Wirtschaft zu konzentrieren. Die betroffenen Länder sollen keine Zeit und keine Energie haben, um sich um kriegerische Handlungen zu kümmern.</p>
<p>Vorgehensplan</p>	<p>Absicht:</p> <ol style="list-style-type: none"> 1. Informationsbeschaffung: Aus dem enormen Know-how werden Angriffsszenarien konstruiert, die Aussicht auf einen grossflächigen Effekt haben. 2. In einer weiteren Phase sollen die Angriffe auf die Verfügbarkeit des Internets umgesetzt werden. <p>Vorgehen:</p> <ol style="list-style-type: none"> 1. Im Rahmen dieser Nachforschungen entdeckt ein Entwickler von Routersoftware in einem Reverse Engineering die geheimen Backdoors von bekannten Routertypen, die von Nachrichtendiensten implementiert wurden. Er entwickelt ein Konzept, um in einer definierten Reihenfolge die Hauptknotenpunkte im Internet zu kompromittieren und lahmzulegen. Die Reihenfolge wird nach Beendigung wiederholt, so dass neu aufgesetzte Router automatisch wieder kompromittiert werden. 2. Ein anderer Spezialist hat zusammen mit anderen Hackern eine Möglichkeit gefunden, über gezielte Abfragen in einen spezifischen Typ von DNS Server (80% weltweiter Marktanteil) einzudringen. Mit einem Script bringt er anschliessend die DNS-Server dazu, Namen falsch auf-

	<p>zulösen und den Zugriff auf das System nach Beendigung des Scripts zu löschen.</p> <ol style="list-style-type: none">3. Die Codesequenz zur Kompromittierung der DNS-Server wird auf mehrere Standorte verteilt und für den Einsatz bereitgehalten4. Die Attacke auf die zentralen DNS-Server wird gestartet. Durch den kontinuierlichen Austausch der Routingtabellen pflanzt sich dieser Fehler langsam fort. Nach und nach sind die DNS Namen nicht mehr verfügbar und der Netzwerkverkehr ist nur noch über die direkten IP-Adressen möglich.1. Während dieser Zeit wird die Attacke auf die Router gestartet, deren Routingkonzept auf direkten IP Adressen basiert. Die neuralgischen Router werden dadurch kurzzeitig unbrauchbar gemacht. Der Fehler wird vorerst beim DNS gesucht, während der „Doppelfehler“ erst nach der Behebung der DNS Panne zeigt. Einzelne werden feststellen, dass die Router wohl laufen, aber nicht mehr routen.2. Ein neuer Softwarepatch dürfte nicht innert nützlicher Frist verfügbar sein, da das Internet grösstenteils nicht verfügbar ist und keine Softwarepatches per Internet-Download erhältlich sind. Der Ausfall wird voraussichtlich mehrere Tage bis Wochen dauern.
Zweck	<p>Dieses Szenario zielt darauf ab, die Verfügbarkeit des Internets weltweit und nicht nur in der Schweiz durch logische Fehler stark einzuschränken. Ebenfalls zeigt dieses Szenario auf, wie schnell sich logische Fehler fortpflanzen können.</p> <p>Ein weiteres Thema bildet der Entscheidungsprozess aufgrund von Indizien. Das Szenario soll zeigen, wie schwierig es ist, aufgrund von Indizien innert kurzer Zeit einen brauchbaren Entscheid herbeizuführen. Die Zeit spielt daher in diesem Szenario eine entscheidende Rolle, da sich – wie dargestellt - logische Probleme sehr schnell ausbreiten können.</p>

Ereignis	Beurteilung der aktuellen Lage Informationssicherheit, wie sie sich aus Ihrer Sicht zum Auftretenszeitpunkt des Ereignisses präsentiert (mögliche Ziele, unkritisch, kritisch, sehr kritisch für welche Bereiche, Eskalationspotential, Gegner etc)	Vermutete Motiv(e)	Eingeleitete Massnahmen	Zeitpunkt für das Aufgebots des Sonderstabs Informationen mit X bezeichnen
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

11				
12				
13				
14				
15				
16				
17				
18				
19				
20				