

al infrastructure
nformation assurance
n kritische
mation

sicherung
vitalité assurance

Verletzliche

Informationsgesellschaft

Herausforderung Informationssicherung



Informatikstrategieorgan Bund ISB
Unité de stratégie informatique de la Confédération USIC
Organo strategia informatica della Confederazione OSIC
Organ da strategia informatica da la confederaziun OSIC

Inhalt

Einleitung und Überblick 4

Informationssicherung –
eine Führungsaufgabe
für den Bund 8

Schutz kritischer Infrastrukturen im Wandel der Zeit
Informationssicherung (Information Assurance)
Bedeutung und Entwicklung der IKT
Bedrohungen

Informationssicherung –
das Schweizer Modell 20

Die letzten fünf Jahre
Das Vier-Säulenmodell

Beurteilung und Ausblick 32

Beurteilung
Ausblick

Begriffe 36

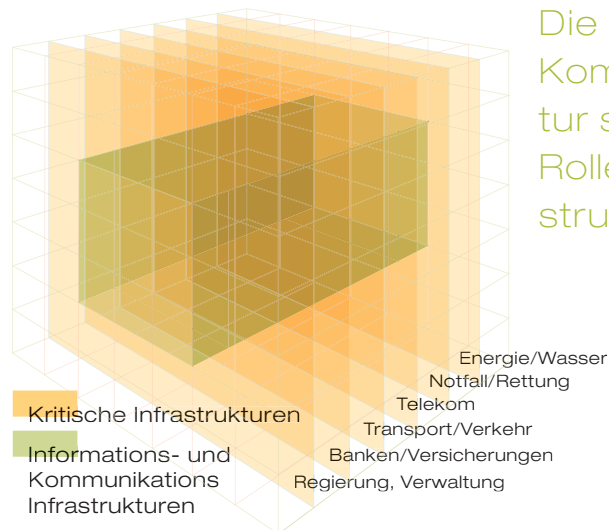
Einleitung und Überblick

Unter den OECD-Staaten gibt die Schweiz am meisten Geld pro Kopf und Jahr für Informations- und Kommunikationstechnologien aus – gefolgt von den USA und den skandinavischen Ländern. Das verschafft uns Markt- und Standortvorteile, ist aber auch mit grossen Abhängigkeiten und Risiken verbunden.

Softwarefehler in Verkehrsleitsystemen, Ausfälle von Mobiltelefonnetzen oder Betriebsunterbrüche bei Geldausgabeautomaten sind Ereignisse, die uns schon heute die Schattenseiten der Informations- und Kommunikationstechnologien vor Augen führen. Technische Pannen, aber auch gezielte Angriffe auf die Informations- und Kommunikationsinfrastruktur, wie etwa das unbefugte Eindringen in oder das vorsätzliche Schädigen von Systemen, können dazu führen, dass beispielsweise die Strom-, Geld- oder Wasserversorgung massiv gestört werden. In Zukunft wird Führen, Verwalten, Transportieren oder Steuern und somit das reibungslose Funktionieren von Staat und Wirtschaft noch stärker vom «digitalen Nervensystem» abhängen.

Diese Erkenntnis hat in den letzten Jahren zur Entwicklung des Fachgebiets der Informationssicherung (Information Assurance) geführt. Analog zur Qualitätssicherung, welche die Qualität eines Produkts sicherstellen soll, sorgt die Informationssicherung dafür, dass die zur Erfüllung einer definierten Aufgabe notwendige Information in erforderlicher Qualität (Korrektheit, rechtzeitige Verfügbarkeit, Vertraulichkeit) sichergestellt ist.

Obwohl Informationen heute meist mit Mitteln der Informations- und Kommunikationstechnologien erstellt, bearbeitet und übertragen werden, ist Informationssicherung keine rein technische Aufgabe. Sie umfasst vielmehr die Gesamtheit von aufeinander abgestimmten Massnahmen, wie z.B. Arbeitsabläufe, Organisationsanweisungen, Schulung und Ausbildung, Informationssicherheit (*information security*), Sicherheitspolitik (*security policy*), so dass die erforderliche Qualität der Information erreicht werden kann. Diese ist Voraussetzung nicht nur für das Funktionieren von Geschäftsprozessen in der Wirtschaft, sondern auch für die sogenannten kritischen Infrastrukturen eines Landes. In diesem Kontext wird Informationssicherung auch zu einer Staatsaufgabe.



Die Informations- und Kommunikationsinfrastruktur spielt eine zentrale Rolle in den kritischen Infrastrukturen

Zu diesen kritischen Infrastrukturen zählen die Energie- und Wasserversorgung, das Notfall- und Rettungswesen, die Telekommunikation, der Transport und Verkehr, Banken und Versicherungen sowie die Regierung und die öffentlichen Verwaltungen. Da der weitaus grösste Teil der Informations- und Kommunikationsinfrastrukturen privatwirtschaftlich betrieben wird, kann die Informationssicherung nur in enger Partnerschaft zwischen Staat und Wirtschaft gelingen.

Die Bedeutung dieser Zusammenarbeit hat man auch in anderen Ländern erkannt. So steht im Vorwort zum US-amerikanischen «National Plan for Information Systems Protection»:

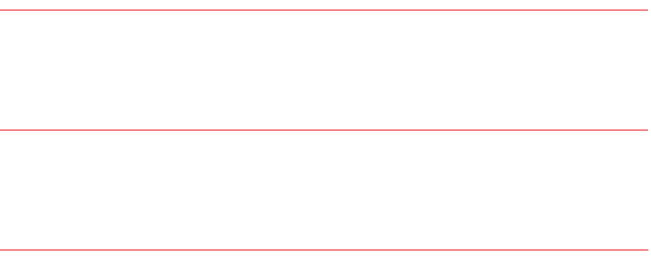
«For this plan to succeed, government and the private sector must work together in a partnership unlike any we have seen before.» William Jefferson Clinton, 42nd President of the United States of America, in: *Protecting America's Cyberspace*

Ziel der vorliegenden Broschüre ist es, eine Einführung in das Thema Informationssicherung aus der Sicht des Staates, respektive des Schutzes der kritischen Infrastrukturen zu geben und einen Einblick in die Geschichte der Informationssicherung der Schweiz zu gewähren. Zudem werden die beteiligten Organisationen vorgestellt.

Eine zentrale Stellung nimmt dabei das vom Informatikstrategieorgan Bund entwickelte gesamtheitliche «Einsatzkonzept Information Assurance Schweiz» ein. Es beruht auf den Vorarbeiten der Koordinationsgruppe Informationsgesellschaft bzw. auf den Resultaten der Untergruppe «Sicherheit» unter der Federführung des Bundesamts für wirtschaftliche Landesversorgung und bezieht alle betroffenen Bundesstellen sowie die Privatwirtschaft mit ein. Das Einsatzkonzept sieht die folgenden vier Säulen vor:

- 1 Durch geeignete Massnahmen ist **präventiv** dafür zu sorgen, dass sich nur wenige Vorfälle ereignen.
- 2 Durch eine Melde- und Analysestelle Informationssicherung (MELANI) sollen Gefahren und Bedrohungslagen möglichst **früh erkannt** werden, so dass entsprechende Abwehrdispositive bereitgestellt oder gewisse mit Risiken behaftete Technologien gemieden werden können.
- 3 Der Sonderstab Information Assurance (SONIA) ist als Instrument des strategischen Krisenmanagements dafür verantwortlich, dass die **Auswirkungen** von Störungen auf Gesellschaft und Staat auf ein Minimum **beschränkt werden** können.
- 4 Schliesslich müssen die **technischen Ursachen** für die Störungen **eruiert** und **behooben** werden.

Mit MELANI und SONIA sieht dieses Modell beträchtliche Leistungen des Staats vor. Trotzdem kann es nur erfolgreich sein, wenn auch die Wirtschaft zu einem aktiven Mitwirken bereit ist. Erste Anzeichen sind erfreulich und ermutigend. Alle Entscheidungsträger sollten sich rechtzeitig mit der Informationssicherung auseinandersetzen, da im Krisenfall dazu keine Zeit mehr bleiben wird.



Informationssicherung – eine Führungsaufgabe für den

Die Bedrohung der kritischen Infrastrukturen ist real, wie die folgenden Beispiele zeigen:

Wasserversorgung



In den Monaten März und April 2000 drang ein 49-jähriger Mann mehrmals in die durch Computer gesteuerte Wasserversorgung von Maroochy Shire in Queensland, Australien ein. Von seinem Laptop aus konnte er sich als «Pumpstation 4» anmelden und in der Folge sämtliche Alarmmeldungen unterdrücken. Er erlangte die uneingeschränkte Befehlsgewalt über 300 Kontrollknoten des Trink- und Abwassersystems. So gelang es ihm, Millionen Liter Abwasser in Parks, Flüsse ja sogar in die Anlage eines Erstklasshotels ausfliessen zu lassen. Die Meeresfauna wurde schwer geschädigt, das Flusswasser färbte sich schwarz und der Gestank war über lange Zeit unerträglich. Beim 46. Versuch konnte der Mann von der Polizei gefasst werden. Offenbar hatte er seinen Arbeitsplatz beim Lieferanten des Kontrollsystems aufgegeben und versuchte, sich einen Consulting-Vertrag bei der Wasserversorgung der Region zu verschaffen, indem er versprach, die Probleme zu lösen, die er selbst verursacht hatte.

Transport und Logistik

Am 15. und 19. Juni 2001 legte ein Softwarefehler das operative Betriebszentrum für den Bahnhof Basel SBB für jeweils mehrere Stunden lahm. Züge konnten weder ein- noch ausfahren und die Reisenden mussten beträchtliche Verspätungen in Kauf nehmen.

Banken und Versicherungen

Ebenfalls im Juni 2001 wurde aus Angst vor möglichen Krawallen geplant, das Treffen der Weltbank in Barcelona ins Internet zu verlegen. Kurz nach dieser Ankündigung drohten Globalisierungsgegner bereits mit virtuellen Sit-ins. Da virtuelle Konferenzen schon von einzelnen Personen lahmgelegt werden können, sind diese viel empfindlicher als solche in der «realen Welt». Letztlich blieb es bei den Drohungen, die aber im Vorfeld grosse Verunsicherung ausgelöst haben.

Telekommunikation

Am 27. Juli 2001 kam es bei der Swisscom zu einer massiven Störung mit stundenlangem Ausfall des Mobiltelefonienetzes. Aufgrund eines Softwarefehlers war der Zentralrechner in Lausanne ausgefallen. Wie in solchen Fällen vorgesehen, übernahm der redundante Rechner in einer anderen Lokalität («hot site») vorerst für eine Stunde die Last. Bedingt durch einen anderen

Softwarefehler in diesem System kam es jedoch zu einer Art Kettenreaktion und im Laufe des Nachmittags zu einem fast vollständigen Erliegen des Schweizer NATEL-Netzes. Ein Swisscom-Problem? Nein, denn wenig später fiel das Sunrise-Netz aus und auch bei Orange beklagte man Schwierigkeiten. Mobiltelefone von in der Schweiz weilenden Personen mit Verträgen bei ausländischen Anbietern suchten im Zehntelsekunden-Rhythmus automatisch das am besten empfangbare Netz. Nach dem Wegfall des Swisscom-Netzes hatten diese auf die Ausweichnetze geschaltet, was im Fall von Sunrise zum Kollaps der Zentrale führte. Die Probleme blieben nicht auf die Mobiltelefonie beschränkt. Kunden des grössten Schweizer Car-Sharing-Unternehmens Mobility fanden zwar ihre vorbestellten Autos wie gewohnt auf dem Parkplatz vor. Nur die Zentralverriegelung liess sich nicht öffnen, weil die Reservationsdaten fehlten, die dem Bordcomputer der Wagen normalerweise per SMS übermittelt werden. Grosse Probleme bekundete auch die damalige Swissair, deren Einsatzleiter mit den Bordmannschaften der Flugzeuge unter anderem via SMS kommunizierten.

Diese willkürlich ausgewählten Ereignisse zeigen exemplarisch, womit wir uns bei der Bedrohung der kritischen Infrastrukturen auseinandersetzen müssen: Durch den hohen Grad der Vernetzung von Systemen breiten sich negative Auswirkungen von Ereignissen unter Umständen sekundenschnell aus; sie treten sektorübergreifend auch an Orten auf, wo wir sie nicht erwarten und sie betreffen sowohl die Wirtschaft als auch die Verwaltung.

Trotzdem stellt man fest, dass die Bedeutung der Informations- und Kommunikationsinfrastruktur für unsere Gesellschaft erst in Ansätzen in das Bewusstsein der Leute eingedrungen ist. Viren-attacken oder das «Hacken» in fremden Datennetzen werden in der Bevölkerung weniger als Bedrohung, denn als spannendes Entertainment und dankbarer Stoff für Kinofilme wahrgenommen. Für den Einzelnen sind Störungen in der Informationsinfrastruktur allenfalls lästig, erscheinen aber kaum als Bedrohung an Leib und Leben. Firmen, bei denen Information der zentrale Produktionsfaktor darstellt, schützen sich selber zwar intensiv, neigen aber dazu, den informationstechnischen Schutz ihres Umfeldes als *not our business* zu betrachten. Ein Land, welches «die gemeinsame Wohlfahrt» seiner Bürger zum Ziel hat, wie es in Artikel 2, Absatz 2 der Schweizerischen Bundesverfassung festgehalten ist, muss diese Gefährdungen erkennen und – in Zusammenarbeit mit der Wirtschaft – Antworten auf diese neuen Bedrohungsformen fin-

den. Nicht die öffentliche Meinung drängt den Staat zum Handeln, sondern die ihm in der Verfassung zugewiesene Führungsrolle: *Gouverner, c'est prévoir.*

Schutz kritischer Infrastrukturen im Wandel der Zeit

Zum Schutz kritischer Infrastrukturen (*critical infrastructure protection, CIP*) werden sowohl strategische als auch operative Mittel eingesetzt. Auf der strategischen Seite kann man die Prävention durch Ausbildung und Sensibilisierung, die Sicherheitspolitik, das Schaffen internationaler Netzwerke sowie die Nachrichtendienste nennen.

Mit operativen Aufgaben sind die Polizei, die Feuerwehr, der Zivilschutz, die Wirtschaftliche Landesversorgung sowie die Armee betraut. Auch heute noch sind diese Stellen die bewährten Mittel für Bedrohungen, wie sie z.B. von Lawinenabgängen, Unwettern oder wochenlangen Hochwassern am Rhein ausgehen.

Der Einsatz der Informations- und Kommunikationstechnologien (*information and communication technologies*) hat in den letzten Jahren allerdings weitere Risiken und Bedrohungsformen für die kritischen Infrastrukturen gebracht, die sich in verschiedener Hinsicht von den vorigen unterscheiden. So sind die Informations- und Kommunikationstechnologien bis heute fehleranfälliger als andere Technologien und bieten breite und teilweise noch ungenügend verstandene Angriffsflächen, um den kritischen Infrastrukturen Schaden zuzufügen. Ausserdem werden diese heute meist privatwirtschaftlich betrieben (Beispiele: Internet Service Provider, Privatisierung der ehemaligen PTT), was neue Formen und Modelle der Zusammenarbeit zwischen Staat und Wirtschaft (*public private partnership*) nötig macht. Am wesentlichsten ist jedoch, dass die Informations- und Kommunikationstechnologien die kritischen Infrastrukturen untereinander vernetzen und so in einer bisher noch nie dagewesenen Weise voneinander abhängig und auch verletzlich machen.

Informationssicherung (Information Assurance)

Die vorgängig geschilderten Ereignisse in den kritischen Infrastrukturen beruhen darauf, dass Informationen im entscheidenden Moment entweder falsch oder gefälscht, fehlerhaft, für Berechtigte nicht zugänglich oder gar nicht vorhanden waren.

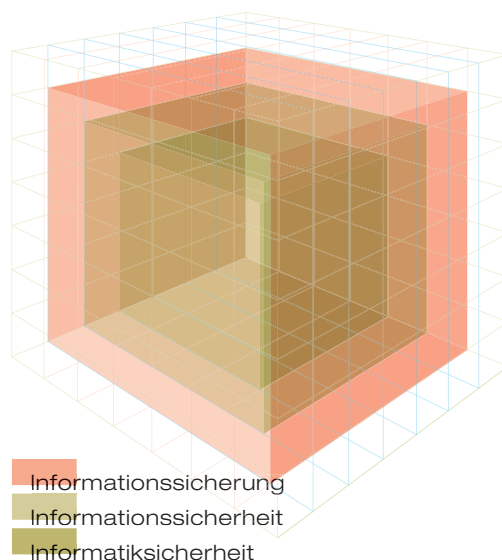
Informationssicherung (Information Assurance) umfasst die Gesamtheit von aufeinander abgestimmten Massnahmen, wie Arbeitsabläufe, Organisationsanweisungen, Schulung und Ausbildung, Informationssicherheit (*information security*), Sicherheitspolitik (*security policy*), so dass die zur Erfüllung einer Aufgabe erforderliche Qualität der Information erreicht werden kann.

Das Fachgebiet, das sich dieser Problematik annimmt, nennt sich Informationssicherung. Ziel der Informationssicherung ist es, die zur Erreichung bestimmter Aufgaben benötigte Information zu jeder Zeit und in der erforderlichen Qualität sicherzustellen. Es spielt dabei keine Rolle, ob die Qualität der Information durch das Versagen von Informationssystemen, durch schlecht geschultes Personal oder durch mutwillige Zerstörung beeinträchtigt wird. Informationssicherung ist ein junges Fachgebiet, so dass sich dieser Begriff noch nicht richtig etabliert hat.

Anhand von ein paar Beispielen versuchen wir, Informationssicherung verständlich zu machen und von anderen Fachgebieten abzugrenzen.

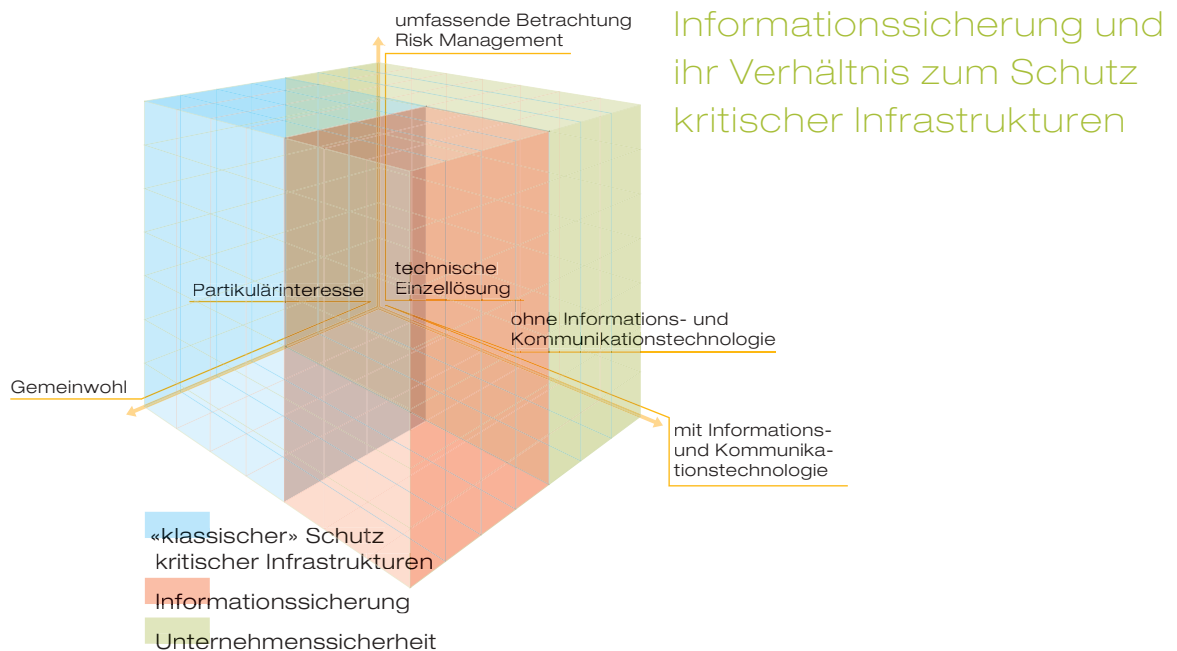
Häufig werden Informationssicherung und Informationssicherheit (*information security*) synonym verwendet. Informationssicherheit fokussiert aber auf Aspekte, wie Authentifizierung, Integrität, Vertraulichkeit, Verfügbarkeit oder Verbindlichkeit von Informationen. Sind diese nur in elektronischer Form vorhanden, spricht man von Informatiksicherheit.

Folgendes Beispiel diene der Verdeutlichung dieser drei Begriffe: Wir nehmen an, eine Abstimmung werde elektronisch (E-Voting), per Post und an der Urne durchgeführt. Die **Informatiksicherheit** sorgt beim E-Voting dafür, dass die Abstimmungsserver verfügbar sind, dass sie sich gegenüber dem Stimmbürger korrekt authentifizieren, dass Manipulationen auf dem Computer des Stimmdenden (z.B. durch Viren) verhindert werden und dass die abgegebene Stimme für andere unlesbar (verschlüsselt) zum Abstimmungs-server übertragen wird. Die **Informationssicherheit** erweitert die oben beschriebenen Aspekte der Abstimmung auf die briefliche Stimmabgabe oder das Einlegen des Wahlzettels in eine Urne. Die **Informationssicherung** garantiert zusätzlich, dass alle Stimmbürger die Abstimmungsunterlagen rechtzeitig erhalten, dass die Ergebnisse aus E-Voting und brieflicher Stimmabgabe richtig miteinander verrechnet und korrekt bekanntgegeben werden und dass das Abstimmungsergebnis z.B. durch Plausibilitätstests so abgesichert wird, dass es auch einer Anfechtung vor Gericht standhalten kann. Kurz: Informationssicherung umfasst alle Massnahmen zur ordnungsgemässen Durchführung der Abstimmung.



Informationssicherung und ihr Umfeld

Manchmal wird auch die Meinung vertreten, dass Informationssicherung nur im Zusammenhang mit dem Schutz kritischer Infrastrukturen gebraucht wird. Wie obiges Beispiel zeigt, ist das nicht richtig. Informationssicherung garantiert die erforderliche Qualität von Informationen, wie sie zur Erledigung einer definierten Aufgabe (z.B. die Ermittlung eines Wahlergebnisses) gebraucht wird. Aus dem Blickwinkel eines Landes ist es allerdings so, dass das Funktionieren der kritischen Infrastrukturen eine zentrale Aufgabe ist, bei der die Informationssicherung einen wesentlichen Beitrag zu leisten vermag. Hier kommt dem Staat auch die Führungsrolle zu, wie das beim Schutz kritischer Infrastrukturen schon seit jeher der Fall ist. Trotzdem sollte man nicht vergessen, dass Informationssicherung bei jedem einzelnen Bürger oder jeder einzelnen Firma beginnt. Erst wenn man sein eigenes Haus in Ordnung gebracht hat, kann man daran gehen, das ganze Land zu schützen.



Informationskrieg und Informationssicherung Unter Informationskrieg (die Begriffe *information operations* oder *information warfare* werden oft synonym verwendet) versteht man die Gesamtheit der Massnahmen, um die Entscheidungsfindungsprozesse eines Gegners zu stören, zu beeinflussen oder zu verunmöglichen, währenddessen die eigenen Entscheidungsfindungsprozesse geschützt oder verbessert werden. Zu den verschiedenen Mitteln des Informationskriegs gehören (unter anderem):

- Psychologische Operationen
- Täuschung, Gegentäuschung und Tarnung
- Elektronische Kriegführung und Waffen gerichteter Energie (directed energy weapon)
- Nachrichtendienst oder Spionage (und entsprechende Gegenmassnahmen)
- Informationssicherung (der Schutz der kritischen Informations-Infrastrukturen ist hier eingeschlossen)

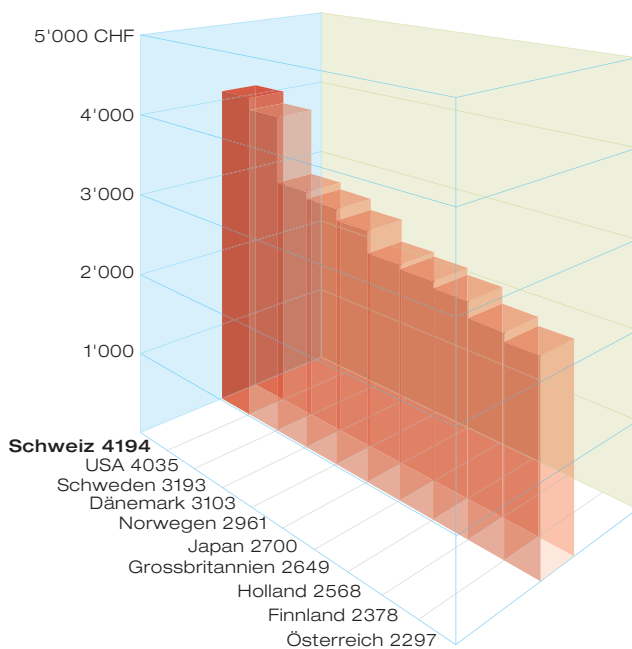
Die Informationssicherung stellt ein Schlüsselement dar, das jedoch alleine nicht ausreicht, um die Ziele des Informationskriegs zu erreichen. Dazu braucht es die Kombination und Abstimmung der verschiedenen oben aufgeführten Mittel. Die Konzeptstudie Information Operations (KS IO), welche unter der Federführung des VBS (Untergruppe Operationen des Generalstabs) und in Zusammenarbeit mit zahlreichen Partnern aus Verwaltung und Wirtschaft durchgeführt wird, hat zum Ziel, einen gemeinsamen doktrinalen Grundsatz zu Gunsten der nationalen Sicherheitspolitik zu finden.

Im nächsten Kapitel beschreiben wir das Modell für die Informationssicherung in der Schweiz, d.h. wir stellen die Organisationen mit ihren Aufgaben vor, die sich der Bedrohungen der kritischen Infrastrukturen im Informationszeitalter annehmen. Da die Bedro-

hungsformen neu sind, nicht aber das Problem (nämlich der Schutz der kritischen Infrastrukturen), wird es sich als sinnvoll erweisen, die bereits benannten Organisationen (Polizei, Wirtschaftliche Landesversorgung, Armee) mit diesen Aufgaben zu betrauen und deren Tätigkeitsfeld so zu erweitern, dass sie auch den neuen Aufgaben gerecht werden können.

Zuvor wollen wir die Bedeutung der Informations- und Kommunikationstechnologie für Wirtschaft und Staat sowie die von ihnen ausgehenden Bedrohungsformen stichwortartig in Erinnerung rufen.

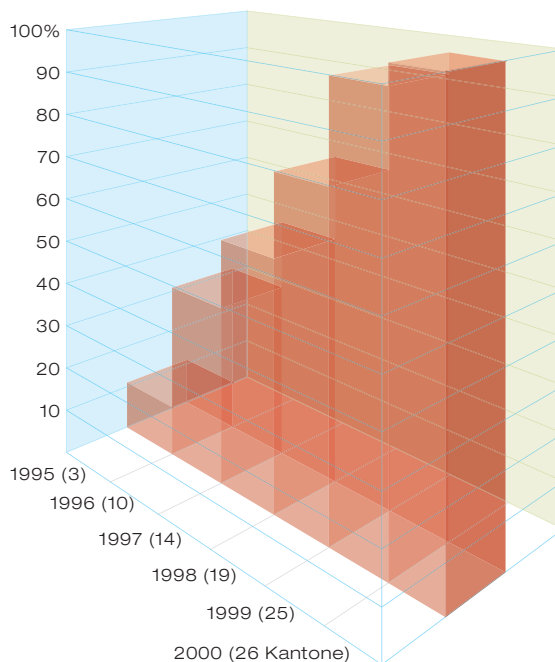
Bedeutung und Entwicklung der IKT



Ausgaben pro Kopf für Informations- und Kommunikationstechnologie im Jahr 2000

Die Schweiz hat im Jahr 2000 pro Kopf rund 4'200 CHF für Informations- und Kommunikationstechnologie ausgegeben. Innerhalb der OECD liegt sie damit an der Spitze, knapp vor den Vereinigten Staaten und deutlich vor Schweden.

Während im Jahr 1996 nur gerade 3% aller KMU über einen Internetanschluss verfügten, wuchs dieser Anteil sprunghaft an und erreichte im Jahr 2001 rund 68%. Parallel dazu hat sich die Webpräsenz der Kantone entwickelt. 1995 verfügten erst drei Kantone über einen Webauftritt; seit dem Jahr 2000 sind alle Kantone online. Künftig sollen im Rahmen von *E-Government* die Interaktionsmöglichkeiten über Internet zwischen Verwaltung und Bürger noch stark erweitert werden. Dabei ist das *electronic voting* nur eine der anspruchsvollen Schlüsselapplikationen, die im Mittelpunkt des Interesses stehen. Gerade solch heiklen Anwendungen werden ohne entsprechende Informationssicherung nicht realisiert und von Stimmbürgerinnen und Stimmbürgern auch nicht akzeptiert werden können.



1995 verfügten erst 3 Kantone über einen Webauftritt; seit dem Jahr 2000 sind alle Kantone online.

In den meisten Branchen der Wirtschaft hat eine Entwicklung hin zur elektronischen Unterstützung oder sogar Ablösung von Prozessen stattgefunden. Ob es sich um elektronisch gesteuerte Lagerbewirtschaftung, Produktion, Vertrieb oder Dokumentenflusssysteme handelt, immer sind auch neue Abhängigkeiten von Informatikmitteln geschaffen worden. Die zunehmende Digitalisierung der Prozesse hat zu einer stärkeren Vernetzung der verschiedenen Systeme geführt. Erst diese Entwicklung hat unternehmensübergreifende Abläufe möglich gemacht und stellt

Bedrohungen

die Basis für die *just-in-time* Produktion oder die Anbindung von Kunden, Lieferanten und Partnern in Extranets dar. Die heutige Wertschöpfungskette ist auf das störungsfreie Funktionieren der Informations- und Kommunikationstechnologien angewiesen.

Durch die hohe Marktgeschwindigkeit verkürzen sich die Reaktionszeiten. Damit ergeben sich grosse Anforderungen an die Verfügbarkeit von Systemen und Informationen. Ausfälle kritischer Informationsinfrastrukturen haben in der modernen Welt ein enormes wirtschaftliches Schadenspotential.

Die Informations- und Kommunikationstechnologie ist noch jung und darf noch nicht in allen Teilen als ausgereift bezeichnet werden. Für manch einen Softwarehersteller ist die Geschwindigkeit, mit der ein neues Produkt auf den Markt gebracht wird, wichtiger als die effektive Marktreife – der Kunde wird häufig zum Beta-Tester. Trotz verschiedener Bekenntnisse von Herstellern zum hohen Stellenwert, den sie der Sicherheit und der Zuverlässigkeit ihrer Produkte beimessen, werden wir uns wohl noch lange mit fehlerhafter Software beschäftigen müssen, mindestens so lange, bis sich entstandene Schäden mit guten Erfolgsaussichten vor Gericht einklagen lassen. Neben dem technischen Versagen können auch menschliches Fehlverhalten oder Naturereignisse (z.B. Wasserschäden, Erdbeben) zum Ausfall von kritischen Informations- und Kommunikationsinfrastrukturen führen.

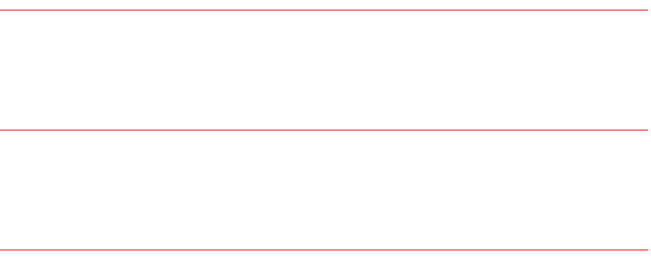
Daneben können die kritischen Informationsinfrastrukturen – und damit auch die kritischen Infrastrukturen – durch sogenannte *malware* (z. B. Viren, Würmer) bedroht sein, welche von verschiedener Seite und mit unterschiedlichen Motiven in Umlauf gebracht werden:

- Einzeltäter, wie gelangweilte oft jugendliche Script-Kiddies, Cracker oder Hacker
- Gruppierungen, die aus politischen Motiven handeln
- Unternehmen, die aus wirtschaftlichen Motiven handeln
- Nationalstaaten mit kriegerischen Absichten

Mit Ausnahme des letztgenannten Informationskriegs sind die anderen Bedrohungsformen nicht auf Aktionen einzelner Staaten beschränkt. Prinzipiell stehen solche Mittel jedermann zur Verfügung und sind auch schon genutzt worden – der beschriebene Fall der Wasserversorgung in Queensland (Australien) sei hier stellvertretend genannt. Die weitaus meisten Vorfälle sind aber nach wie vor entweder auf technisches oder menschliches Versagen zurückzuführen.

Auch wenn der grosse Kollaps kritischer Infrastrukturen als Folge technischer Pannen oder von Angriffen auf die Informations- und Kommunikationsinfrastruktur – wie wir glauben – nicht unmittelbar bevorsteht, tut man gut daran, sich auf solche Fälle vorzubereiten.

Im nachfolgenden Kapitel wird die Antwort der Schweiz auf diese neuen Bedrohungsformen dargestellt.



Informationssicherung – das Schweizer Modell

Die Anstrengungen, die die Schweiz in Bezug auf Informationssicherung unternommen hat, wurzeln einerseits im klassischen Schutz der kritischen Infrastrukturen (Militär, Zivilschutz, Polizei), andererseits aber auch in Ereignissen der letzten fünf Jahre, welche das Thema Informationssicherung entscheidend mitgeprägt haben.

Die letzten fünf Jahre

1997: Strategische Führungsübung Im November 1997 hat die Strategische Führungsausbildung SFA der Bundeskanzlei die Strategische Führungsübung '97 (SFU '97) durchgeführt. Ziel war die Schulung der Bundesverwaltung und von Teilen der Privatwirtschaft im Krisenmanagement. Im durchgespielten Übungsszenario wurde die schweizerische Informationsinfrastruktur verschiedensten elektronischen Attacken ausgesetzt. Dabei wurden die Gefahren erkannt, welche von der Abhängigkeit der kritischen Infrastrukturen von der Informations- und Kommunikationstechnologien ausgehen. Erstmals kam die Idee auf, durch die Entwicklung eines Frühwarnsystems, solche Gefahren möglichst rasch zu erkennen.

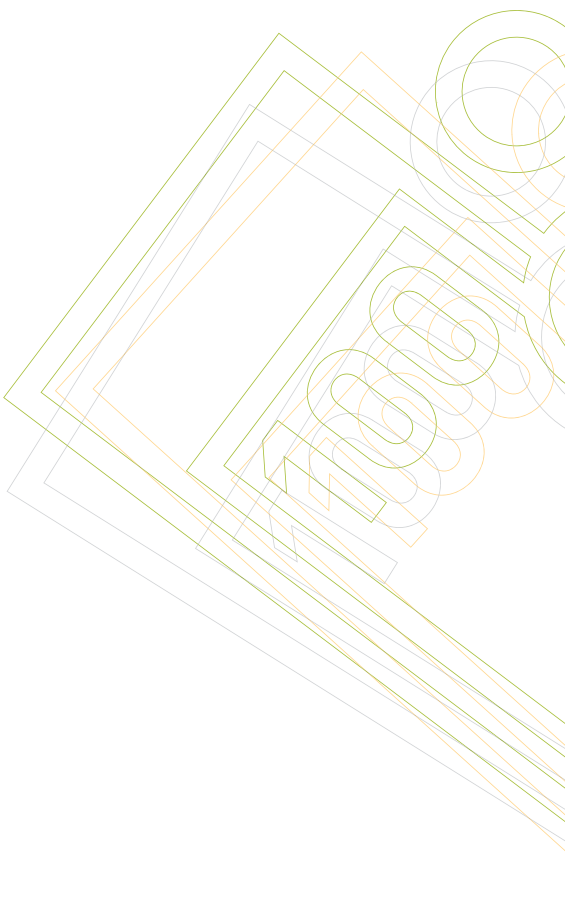
1997- 1998: Sicherheit Informations-Infrastruktur Schweiz (SI²CH) Das an der Strategischen Führungsübung '97 gebildete Beziehungsnetzwerk wird genutzt und Vertreter aus Wirtschaft, Wissenschaft und Verwaltung bilden unter Leitung der wirtschaftlichen Landesversorgung die Gruppe SI²CH. Diese erarbeitet erste Bedrohungsanalysen und definiert Mittel und Massnahmen. Die Grundlagen zur Gründung der Stiftung InfoSurance und für das Konzept «Information Assurance» werden gelegt.

1998: Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz In seinem Strategiepapier hat der Schweizerische Bundesrat Grundsätze für die Förderung einer Informationsgesellschaft definiert und die Gebiete mit dem dringenden Handlungsbedarf bezeichnet. Dem Thema Sicherheit ist ein eigenes Kapitel gewidmet, in dem es wörtlich heisst: «Es ist sicherzustellen, dass die Informationen auch in ausserordentlichen Lagen und zur Bewältigung derselben genützt werden können. Dies bedingt neue Formen der Zusammenarbeit zwischen den Institutionen, welche Informationen produzieren, verteilen, sammeln oder archivieren».

1998 - 1999: Ausarbeitung des Konzepts «Information Assurance»

Am 1. Juli 1998 erteilt der Bundesrat der Koordinationsgruppe Informationsgesellschaft den Auftrag, ein Konzept «Information Assurance» auszuarbeiten, welches anschliessend unter Federführung des Bundesamts für wirtschaftliche Landesversorgung erstellt und am 22. Juni 2000 vom Bundesrat genehmigt wurde. Es sieht folgende Massnahmen vor:

- 1 Die Stiftung InfoSurance wird vom Bund massgeblich finanziell unterstützt.
- 2 Die Wirtschaftliche Landesversorgung baut einen neuen Bereich «Informations- und Kommunikationsinfrastrukturen (ICT-I)» auf.
- 3 Das Informatikstrategieorgan des Bundes wird mit der Bildung eines Sonderstabs Information Assurance und eines Koordinationsorgans zum Zweck des Informationsaustauschs zwischen den verschiedenen im Umfeld der Informationssicherung tätigen Bundesstellen betraut.



1998 – 2000: Task Force Millennium Bug

Im Zusammenhang mit dem sogenannten Millennium Bug wird der Bund im Juni 1998 durch die Wahl eines Jahr-2000-Delegierten und das Einrichten einer Task Force mit rund zehn Personen aktiv. Die Ziele waren die Sensibilisierung, der Erfahrungsaustausch und der Support für die verschiedenen Jahr-2000-Zuständigen in Verwaltung und Privatwirtschaft. Die Aktivitäten haben sich stark auf die Bedürfnisse der KMU sowie diejenigen in den kritischen Infrastrukturen ausgerichtet. Dank des frühen Starts und den grossen Anstrengungen wurde der Jahrtausendwechsel gut überstanden. Zum ersten Mal hat sich gezeigt, wie erfolgreich eine Zusammenarbeit zwischen Verwaltung und Wirtschaft zur Lösung eines Problems in der Informations- und Kommunikationstechnologie sein kann.

1999: Gründung der Stiftung InfoSurance

Dank der Vorarbeit der Gruppe SI²CH kann im Dezember 1999 die Stiftung InfoSurance gegründet werden. Aufgaben und Ziele der Stiftung wurden weitgehend von dem sich damals in Arbeit befindlichen Konzept «Information Assurance» übernommen.

2000: Aufbau des Sonderstabs Information Assurance

Gestützt auf Artikel 7, Absatz 3 der Bundesinformatikverordnung beginnt das Informatikstrategieorgan Bund mit dem Aufbau des Sonderstabs Information Assurance (SONIA).

Stiftung InfoSurance An der Stiftung InfoSurance sind der Bund sowie namhafte Firmen aus der Privatwirtschaft, wie z.B. Microsoft, Siemens, Credit Suisse Group oder die Swisscom beteiligt. Neben einer Geschäftsstelle umfasst InfoSurance einen Stiftungsrat sowie einen Beirat. InfoSurance sensibilisiert die Öffentlichkeit und Wirtschaft im Bereich der Informationssicherheit. Durch den Austausch von *best practices* und als «Hilfe zur Selbsthilfe» richtet die Stiftung besonderes Augenmerk auf das Gewerbe und die KMU. In Abstimmung und enger Zusammenarbeit mit der Wirtschaftlichen Landesversorgung arbeitet InfoSurance im Rahmen sogenannter *round tables* an sektorspezifischen Risikoanalysen.

2000: Schaffung des Bereichs ICT-I der Wirtschaftlichen Landesversorgung Wie im Konzept «Information Assurance» vorgeschlagen, hat der Bundesrat am 1. August 2000 einen neuen fünften Bereich ICT-Infrastrukturen (*ICT-I: Information and Communication Technology Infrastructure*) geschaffen. Aufgabe des Bereichs ICT-I ist es, für die kritischen Wirtschaftsbereiche Notfallstrategien zu erarbeiten sowie geeignete Mittel und Massnahmen vorzubereiten, um Störungen zu verhindern oder deren Folgen zu mindern und um einen allfälligen Wiederaufbau zu ermöglichen.

2001: Übung INFORMO An der von der Strategischen Führungsausbildung organisierten zweitägigen Übung INFORMO wird der Sonderstab Information Assurance beübt. Er erhält Gelegenheit, eine Krise in der Informationsinfrastruktur zu bewältigen und damit seine Stabstätigkeit zu schulen und zu verfeinern. Die Übung zeigt, dass ein partnerschaftlicher Ansatz zwischen Staat und Wirtschaft funktionieren kann. Die Idee einer permanenten Melde- und Analysestelle Informationssicherung, die in unterschiedlichen Varianten seit der SFU '97 diskutiert wurde und auch im Konzept «Information Assurance» festgehalten ist, wird erneut aufgegriffen.

Wirtschaftliche Landesversorgung (WL) Sie hat den verfassungs- und gesetzmässigen Auftrag, die Versorgung des Landes mit lebenswichtigen Gütern und Dienstleistungen für den Fall schwerer Mangellagen sicherzustellen. Zu den lebenswichtigen Gütern und Dienstleistungen zählt auch das Fernmeldewesen. Die WL ist eine Milizorganisation, die aus einem vollamtlichen Stab (Bundesamt, 35 Etatstellen), den drei Grundversorgungsbereichen (Ernährung, Energie, Heilmittel) und den vier Infrastrukturbereichen (Transport, Industrie, ICT-I, Arbeit) besteht. Jeder Bereich verfügt über ein eigenständiges Milizkader (total ca. 300 Personen). Die wichtigsten Mittel und Massnahmen der WL sind: Pflichtlager (Lebensmittel, Brenn- und Treibstoffe, Medikamente, etc), Rationierungs- und Kontingentierungssysteme und Notfalldispositive.

2001: Das Modell für die Informationssicherung in der Schweiz («Vier-Säulenmodell») Im Dezember 2001 definiert das Informatikstrategieorgan des Bundes das Vier-Säulenmodell (siehe unten) der Informationssicherung. Das im Juni 2000 vom Bundesrat verabschiedete Konzept «Information Assurance» behält in weiten Teilen seine Gültigkeit. Es wird jedoch in wesentlichen Punkten präzisiert und zu einem gesamtheitlichen System zum Schutz der kritischen Infrastrukturen zusammengefügt, insbesondere dort, wo diese von einer funktionierenden Informations- und Kommunikationsinfrastruktur abhängig sind. Die endgültige Struktur des Sonderstabs Information Assurance wird definiert und das Kooperationsmodell zwischen Verwaltung und Wirtschaft wird festgelegt. Zu diesem Zweck werden im Bereich ICT-I der Wirtschaftlichen Landesversorgung durch Rekrutierung von Milizkadern sektorspezifische Teams aufgebaut. Diese Teams oder Coordination Centers (CCs) delegieren im Krisenfall Vertreter in den Sonderstab und sorgen somit für eine effiziente Anbindung der Wirtschaft – ein Konzept übrigens, das aus den Erfahrungen mit dem Millennium Bug übernommen wurde. Auf völlig neue Grundlagen wird die permanente Melde- und Analysestelle Informationssicherung MELANI gestellt. Die Verantwortung für deren

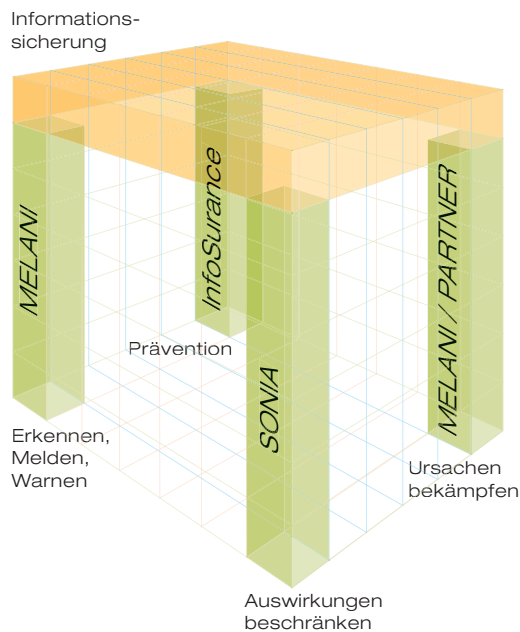
Aufbau liegt nun beim Informatikstrategieorgan Bund, wo zur Zeit (Herbst 2002) deren Aufgaben definiert sowie ein Betriebsmodell ausgearbeitet werden. Mit SONIA und MELANI verantwortet das Informatikstrategieorgan Bund zwei tragende Säulen des Modells. Zwei weitere werden von der Stiftung InfoSurance, respektive der Wirtschaftlichen Landesversorgung beigesteuert.

Informatikstrategieorgan Bund (ISB) Das Informatikstrategieorgan Bund wurde am 1. Juli 1999 operativ. Als Stabs-, Planungs- und Koordinationsorgan des Informatikrat Bund liefert es die Grundlagen für die strategische Steuerung und Koordination der Informatik in der Bundesverwaltung. Organisatorisch untersteht es dem Generalsekretariat des Eidgenössischen Finanzdepartements und ist in fünf Leistungsbereiche aufgeteilt. Der Bereich Informatiksicherheit ist für den Aufbau und die Definition der Aufgaben des Sonderstabs Information Assurance (SONIA) und der Melde- und Analysestelle Informationssicherung (MELANI) zuständig. Ferner leitet es in Zusammenarbeit mit der Wirtschaftlichen Landesversorgung das Advisory Board on Information Assurance (ADINA) und koordiniert somit die verschiedenen Anstrengungen in der Bundesverwaltung im Bereich Informationssicherung.

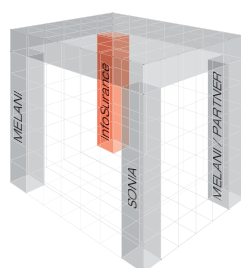
Das Vier-Säulenmodell

Ein gesamtheitliches System zum Schutz der kritischen Infrastrukturen im Informationszeitalter muss folgende vier Punkte berücksichtigen:

- 1 Durch geeignete Massnahmen ist **präventiv** dafür zu sorgen, dass sich nur wenige Vorfälle ereignen.
- 2 **Gefahren** und Bedrohungslagen sind möglichst früh zu **erkennen**, so dass entsprechende Abwehrdispositive bereitgestellt oder gewisse mit Risiken behaftete Technologien gemieden werden können.
- 3 Die **Auswirkungen** von aufgetretenen Störungen auf Gesellschaft und Staat sind auf ein Minimum zu **beschränken**.
- 4 Schliesslich müssen die technischen **Ursachen** für die Störungen eruiert und **behooben** werden.



Vier Säulen tragen die Informationssicherung

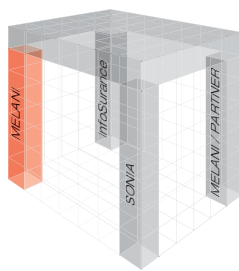


Die vier Säulen umfassen unterschiedliche Aufgaben und Zuständigkeiten, die von verschiedenen Organisationen wahrgenommen werden und im folgenden beschrieben sind.

1) Prävention – InfoSurance InfoSurance sensibilisiert die Öffentlichkeit und Wirtschaft im Bereich der Informationssicherung. Durch die Weitergabe von *best practices* und als «Hilfe zur Selbsthilfe» richtet die Stiftung besonderes Augenmerk auf das Gewerbe und die KMU und unterstützt diese insbesondere beim

Aufbau von notwendigen Strukturen (z.B. *Computer Security Incident Response Teams*). Es kann nicht genug betont werden, wie wichtig es ist, dass sich alle Unternehmen mit Fragen der Informationssicherung (oder mindestens der Informationssicherheit) auseinandersetzen.

Neben der Sensibilisierung arbeitet InfoSurance im Rahmen sogenannter *round tables* an sektorspezifischen Risikoanalysen. Dies geschieht in enger Zusammenarbeit mit der Wirtschaftlichen Landesversorgung.

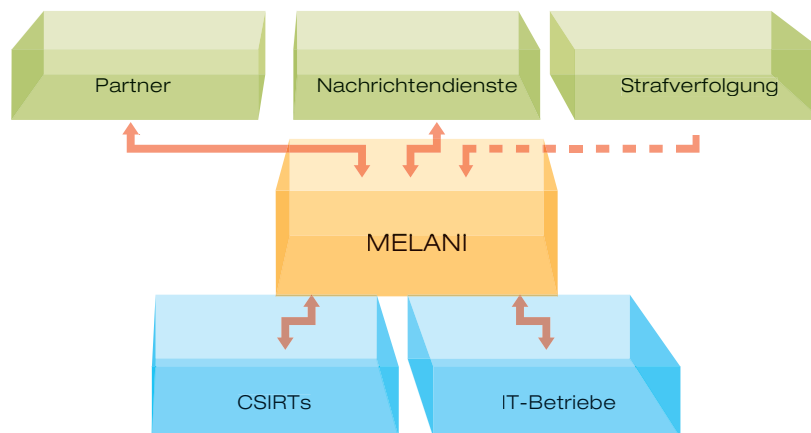


2) Weit mehr als Frühwarnung – MELANI Die Melde- und Analysestelle Informationssicherung (MELANI) soll ein permanentes Lagezentrum im Bereich der kritischen Infrastrukturen sein, insbesondere dort, wo diese von den Informations- und Kommunikationsinfrastrukturen abhängig sind. Die fortwährende Beobachtung und Darstellung der Lage dient einerseits der Prävention, andererseits der Früh-, respektive Vorwarnung.

Frühwarnsysteme sind uns aus verschiedenen militärischen und zivilen Bereichen bestens bekannt. Beispiele sind das amerikanisch-kanadische Luftraumüberwachungskommando (NORAD) oder die schweizerische Nationale Alarmzentrale (NAZ), welche unter anderem für die Frühwarnung bei erhöhter Radioaktivität zuständig ist. Da die Begriffe «Frühwarnung» und «Alarm» sehr unterschiedlich verstanden werden können, ist es wichtig, an dieser Stelle auf die Frühwarnung im Bereich der Informationssicherung einzugehen. MELANI wird wohl eher mit dem Eidgenössischen Institut für Schnee- und Lawinenforschung (SLF) in Davos zu vergleichen sein als mit NORAD oder der NAZ. Im Gegensatz zum Eindringen eines fremden Flugzeugs in den eigenen Luftraum oder zum plötzlichen Anstieg der Radioaktivität ist eine Netzwerkattacke unmittelbar nur schwer zu erkennen. «Bösartiger Code» wird heute oft mittels gängiger Protokolle verbreitet. Das Aufspüren von solcher *malware* im Strom des gleichartigen Netzverkehrs wäre ungefähr so, als müsste NORAD aus Tausenden von anfliegenden «Flugobjekten», dasjenige finden, das tatsächlich mit Bomben bestückt ist und anzugreifen gedenkt.

Die entscheidenden Arbeiten von MELANI werden nicht unmittelbar vor oder während einer Netzwerkattacke geleistet. Sie soll vielmehr im In- und Ausland die neuesten Entwicklungen und Vorkommnisse im Bereich der Informationssicherheit untersuchen und – analog zum Lawinenbulletin – daraus eine Lagebeurteilung

in der Form eines «Informationssicherheitsbulletins» erstellen. Damit kann MELANI an Entscheidungsträger in Wirtschaft und Verwaltung herantreten und sie hoffentlich vom Einsatz risikoreicher oder unsicherer Technologien und Verfahren abhalten.



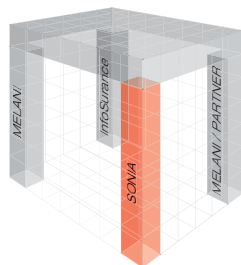
Informationsflüsse von und zu MELANI

MELANI wird auf ein breit gefächertes Sensorenetz angewiesen sein, um möglichst viele relevante Informationen sammeln und auswerten zu können. Dies bedingt Kontakte zu Betreibern von IT-Systemen in Wirtschaft und Verwaltung, zu IT-Herstellern, *Computer Security Incident Response Teams* sowie zu anderen in- und ausländischen Partnern mit ähnlichen Aufgaben wie z.B. das britische Unified Incident Reporting and Alert Scheme (UNIRAS) oder das amerikanische National Infrastructure Protection Center (NIPC). Weitere Informationen werden von den Nachrichtendiensten und gegebenenfalls von der Strafverfolgungsbehörden stammen. Wichtige Sensoren sind auch Quellen im Internet. Insbesondere dürfte es sich lohnen, die Aktivitäten der sogenannten *underground community*, welche aus Hackern, Crackern und Hacktivisten gebildet wird, zu verfolgen. Es gibt viele Sicherheitslücken auf verschiedenen Plattformen und in diversen Programmen – unter ihnen sind sicher besonders jene relevant, die in solchen Kreisen diskutiert werden.

Computer Security Incident Response Team

(CSIRT) Ein CSIRT ist eine Arbeitsgruppe zur Koordination und Ergreifung von Massnahmen im Zusammenhang mit sicherheitsrelevanten Vorfällen in der Informationstechnologie. Jedes CSIRT betreut eine in der Regel vertraglich definierte Gruppe von Kunden, welche diese Dienstleistung finanziell abgelden. Welche Dienste angeboten sowie die Art und Weise, wie diese in Anspruch genommen werden können (z.B. das Melden von Vorfällen), sind zwischen CSIRT und Kunde zu vereinbaren. Häufig wird ein CSIRT auch als IRT (*Incident Response Team*) oder als CERT (*Computer Emergency Response Team*) bezeichnet.

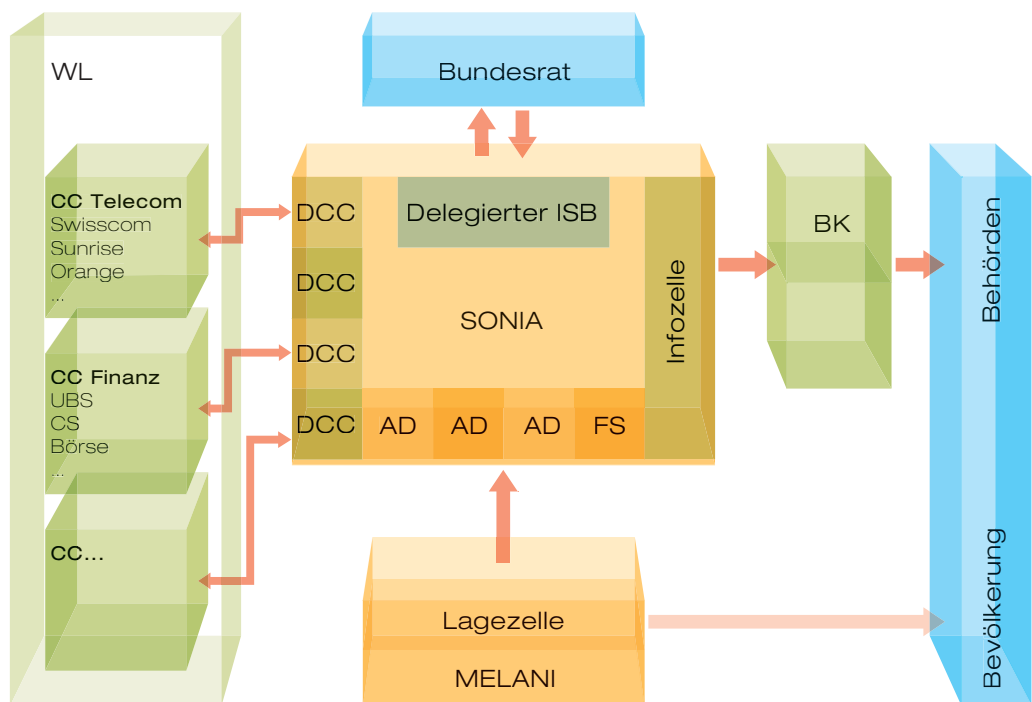
Sollte eine umfassende Lageanalyse ergeben, dass kritische Infrastrukturen z.B. durch weit verbreitete Sicherheitslücken in Informations- und Kommunikationsinfrastrukturen unmittelbar bedroht sind, wird MELANI unverzüglich die entsprechenden Stellen in Wirtschaft und Verwaltung warnen und gegebenenfalls auch die Bevölkerung benachrichtigen. Erfordert es die Lage, wird MELANI den Sonderstab (SONIA) alarmieren und nach dessen Einberufung eine seiner wichtigsten Informationslieferanten bleiben.



3) Schadensbegrenzung in der Krise – SONIA Sollte trotz präventiven Bemühungen eine Störung in der Informations- und Kommunikationstechnologie dazu führen, dass kritische Infrastrukturen beeinträchtigt werden, so müssen die Auswirkungen dieser Störung möglichst begrenzt und die Funktionstüchtigkeit so rasch wie möglich wieder hergestellt werden. Diese operative Aufgabe kann nur durch den betroffenen Sektor selbst wahrgenommen werden. Angesichts der grossen gegenseitigen Abhängigkeit ist allerdings zentral, dass die Entscheidungsvorbereitung in Absprache mit den übrigen Sektoren erfolgt. Zudem muss sichergestellt werden, dass nicht nur die Wirtschaftsführungen, sondern auch der Bundesrat seine Führungsrolle in einer solchen Krise wahrnehmen kann. Diese Aufgabe fällt dem Sonderstab Information Assurance (SONIA) zu. SONIA berät den Bundesrat und die Wirtschaftsführungen in solchen Krisen und funktioniert

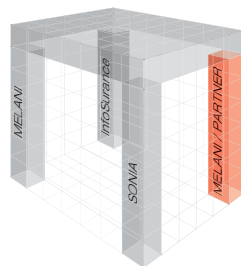
als Bindeglied zwischen Wirtschaft und Verwaltung. Zu unterstreichen ist, dass SONIA nicht an die Stelle der üblichen Entscheidungsträger tritt, sondern diese berät. Für Operation und Information behalten Bundesrat und Wirtschaftsführungen die Verantwortung.

Von besonderer Bedeutung für das Funktionieren von SONIA ist die Wirtschaftliche Landesversorgung. Ihr neu geschaffener Teilbereich ICT-I umfasst sektorspezifische Teams, welche durch Rekrutierung von Milizkadern aufgebaut werden. Im Krisenfall delegieren diese Teams oder Coordination Centers (CCs) Vertre-



Innerhalb MELANI wird die Lagezelle die Informationen für SONIA aufbereiten. Dem Sonderstab stehen die Delegierten der Coordination Centers (DCC), die Amsdirektoren (AD) und die Fachspezialisten (FS) zur Verfügung. Die Informationen nach aussen werden durch die Infozelle aufbereitet und gelangen via Bundeskanzlei (BK) zu den Adressaten.

ter in den Sonderstab und sorgen damit für eine effiziente Anbindung der Wirtschaft. Dadurch kann SONIA auf Risikoanalysen und Notfallplanung zurückgreifen, die von den CCs erarbeitet worden sind.



4) Bekämpfung der Krisenursache – MELANI und Partner

Schliesslich gilt es, die technischen Probleme zu analysieren und adäquate Lösungen vorzuschlagen. MELANI als professionelle, spezialisierte Organisation verfügt hier sowohl über den technischen Sachverstand als auch über das Kontaktnetz zu den wichtigsten IT-Betreibern aus Wirtschaft und Verwaltung sowie zu den einschlägigen *Computer Security Incident Response Teams*. Als einheitliche Ansprechstelle bildet MELANI die notwendige Informationsdrehscheibe zwischen den oben angesprochenen Stellen, die gemeinsam an der Problemlösung arbeiten.

Sobald technische Lösungen zu den Problemen vorliegen, sind die betroffenen Unternehmen gefordert. Sie tragen die operative Verantwortung für die Umsetzung der Massnahmen und sorgen damit für die Problembeseitigung. Die Verantwortung von MELANI beschränkt sich auf ihre Rolle als Informationsdrehscheibe.

Unterschiede zwischen MELANI und Computer Security Incident Response Teams (CSIRTs)

MELANI unterscheidet sich deutlich von den CSIRTs. Letztere bearbeiten die technischen Fragestellungen, beurteilen die Probleme und zielen bei der Lösung auf Spezialisten. Demgegenüber kümmert sich MELANI um die Lage, betrachtet die grossen Zusammenhänge, d.h. die kritischen Infrastrukturen und richtet ihre taktisch-strategischen Informationen eher an Entscheidungsträger in Wirtschaft und Verwaltung. MELANI und CSIRTs sind auch im Bezug auf allfällige Warnungen

verschieden. CSIRTs warnen vor technischen Sicherheitslücken und zwar aus verständlichen Gründen erst dann, wenn eine Lösung des Problems vorliegt. Bei MELANI rechtfertigt die Abstützung auf eine andere Wissensbasis und der Fokus auf die kritischen Infrastrukturen eine Warnung auch dann, wenn das zugrunde liegende technische Problem noch ungelöst ist.

Abschliessende Bemerkungen

Informationssicherung ist ein ausserordentlich breites Gebiet in dem verschiedene Organisationen zu berücksichtigen sowie deren Aktivitäten aufeinander abzustimmen sind. Auf Initiative des ISB und der WL wurde das «Advisory Board on Information Assurance (ADINA)» gegründet, welches als beratendes Fachgremium die Aktivitäten innerhalb der Bundesverwaltung koordiniert. ADINA wird auf Stufe der Entscheidungsträger durch das Koordinationsorgan Schweiz für Informationsoperationen (KOSIO) unter der Leitung des VBS ergänzt. Sowohl in ADINA als auch in KOSIO sind neben dem ISB und der WL insbesondere verschiedene Stellen im VBS, im EJPD, im UVEK sowie der Datenschutz vertreten. Ein weiteres Ziel von KOSIO wird es sein, Kontakte zu Forschung und Wissenschaft zu pflegen.

Ebenso wichtig wie das Networking nach innen ist der Kontakt mit dem Ausland. Dieser geschieht u.a. im Rahmen von Partnership for Peace (PfP) sowie in Projekten und an Anlässen mit dem deutschen Bundesamt für die Sicherheit in der Informationstechnik (BSI) und dem österreichischen Zentrum für sichere Informationstechnologie (A-SIT).

Beurteilung und Ausblick

Beurteilung

Die zunehmende Abhängigkeit unserer Gesellschaft von den Informations- und Kommunikationstechnologien birgt grosse Herausforderungen. Dies gilt in besonderem Mass für die Zusammenarbeit und das gegenseitige Vertrauen zwischen Wirtschaft und Staat. Dank dem tief verwurzelten Milizgedanken hält die Schweiz einen Trumpf in der Hand. Gleichwohl stösst das Milizsystem punktuell an seine Grenzen.

Mit dem Vier-Säulenmodell der Informationssicherung konnte in der Schweiz eine Lösung gefunden werden, die im Sinne eines *best of breed* auf Milizstrukturen zurückgreift (SONIA, WL), aber auch professionell geführte Organe (MELANI) einsetzt, was ein effizientes, flexibles und vor allem kostengünstiges System ermöglicht.

Während die Problemanalyse durch MELANI weit weg von der Quelle der Störung erfolgt, werden die Massnahmen zur Problemlösung so nahe als möglich bei den Betroffenen in Wirtschaft und Verwaltung erarbeitet und umgesetzt. Das ist richtig so. In einer vernetzten Welt kann die Ursache eines Problems nur durch Zusammentragen und Auswerten verschiedener Informationen erkannt werden. Wenn sich das Auto, welches beim Car-Sharing-Unternehmen Mobility vorbestellt wurde, wie geschildert nicht mehr wie gewohnt öffnen lässt, kann vom Betroffenen kaum erwartet werden, dass er den Zusammenhang zum Ausfall eines Zentralrechners der Swisscom in Lausanne herstellen kann. Erst die Kenntnis über diesen Vorfall, seine Auswirkungen sowie das Verstehen der Funktionsweise des Autos von Mobility, lässt so einen Schluss zu. Selbst wenn der Kunde dieses Wissen hätte, würde es ihm zur Problemlösung wohl wenig nützen, sich bei der Swisscom zu melden; ein Anruf (allerdings mit dem Festnetz!) bei Mobility wäre schon deutlich erfolgversprechender. Dauert dies zu lange, z.B. weil er einen wichtigen Termin im nächsten Dorf einhalten muss, könnte sich eine Lösung in der Form eines Taxis anbieten. Hier wäre SONIA die zentrale Drehscheibe, die solche «Taxidienste» vermitteln und – sollten mehrere Leute davon betroffen sein – ihre Einsätze koordinieren könnte.

Neben den Aufgaben im Bereich der Problemerkennung und Bewältigung ist und bleibt die Prävention von zentraler Bedeutung. In der Medizin, im Strassenverkehr, ja fast überall gilt: Vorbeugen ist besser als heilen! Anstatt möglichst schnell vor Computerviren zu warnen, ist es deutlich effizienter, rechtzeitig die betreffenden Sicherheitslöcher zu schliessen. In der Regel lässt man sich ja auch bereits im Spätherbst gegen die Grippe impfen und nicht erst dann, wenn die ersten Patienten mit Fieber im Bett liegen.

Die Informations- und Kommunikationstechnologien haben viele Vorteile und Annehmlichkeiten gebracht, an die wir uns gewöhnt haben und die aus unserem Leben nicht mehr wegzudenken sind. Leider haben sie nicht nur Probleme gelöst, sondern auch neue geschaffen. Daran müssen wir uns in Zukunft vielleicht vermehrt erinnern und die Vor- und Nachteile neuer Technologien gründlich abwägen. Wir müssen und dürfen es uns auch leisten, einmal «NEIN» zu sagen. Es mag zwar praktisch sein, wenn sich in Zukunft ein Garagist in das elektronische System unseres Autos «einloggen» und die Fehler mittels «Fernwartung» beheben kann. Weniger angenehm ist es, wenn ein «Hacker» die Gewalt über unser Fahrzeug erlangen sollte. Dort, wo man sich einer neuen Technologie nicht entziehen kann, muss man wenigstens versuchen, den Weg bewusst zu gehen und die Gefahren im Auge zu behalten.

Schliesslich sei noch darauf hingewiesen, dass der Staat gesetzliche Rahmenbedingungen und Infrastrukturen (z.B. MELANI) zur Verfügung stellen kann, jedoch unmöglich Probleme einzelner Unternehmen lösen wird. Er muss und soll nur dort handeln, wo es die Möglichkeiten des Einzelnen übersteigt.

Ausblick

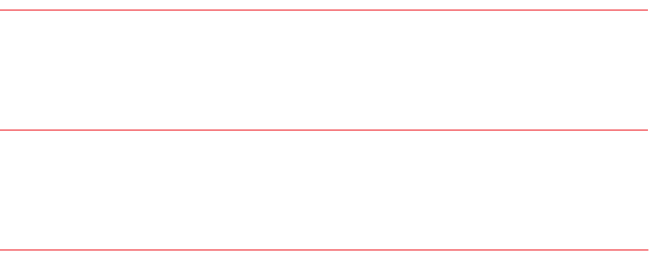
Ist die Schweiz für die Herausforderung Informationssicherung genügend gerüstet? Nein – aber sie ist auf gutem Weg.

Noch fehlen umfassende und gut abgestützte Risiko- und Gefährdungsanalysen der kritischen Infrastrukturen. Es sind zwar Arbeiten in Gang, doch gestalten sich diese als schwierig, nicht zuletzt auch deshalb, weil man kaum auf Erfahrungen zurückgreifen kann. Trotzdem stellt man fest, dass allein die Arbeit daran, weiter zur Sensibilisierung für das Thema Informationssicherung beiträgt.

Der Ansatz mit dem Vier-Säulenmodell bietet Gewähr, dass das Problem ganzheitlich und im Verbund mit allen Partnern angegangen wird. Das Fehlen der Melde- und Analysestelle MELANI ist allerdings eine Lücke, die möglichst rasch geschlossen werden muss. Die entsprechenden Arbeiten dazu sind beim Informatikstrategieorgan Bund im Gang und werden Ende 2002 in die bundesinterne Vernehmlassung gehen. Bei positiver Beurteilung sollte Anfang 2003 mit dem Aufbau der Stelle begonnen werden können.

Dass der Schutz der kritischen Infrastrukturen an der Landesgrenze nicht Halt macht, ist leicht einzusehen. Daher sind Kooperationen mit anderen Staaten erforderlich. In einem ersten Schritt wird es darum gehen, ein internationales Netzwerk zum Austausch von Erkenntnissen und Erfahrungen aufzubauen.

Alle Anstrengungen, die zur Informationssicherung unternommen werden, tragen letztlich zu einer sicheren und vertrauenswürdigen Schweiz bei. Und Sicherheit und Vertrauen gehören mithin zum Fundament menschlichen Zusammenlebens.



Begriffe

ADINA	Advisory Board on Information Assurance, koordiniert Aktivitäten innerhalb der Bundesverwaltung
CC	→ Coordination Centers
CERT	Computer Emergency Response Team → CSIRT
CIIP	Critical Information Infrastructure Protection (= Schutz kritischer Informations-Infrastrukturen)
CIP	Critical Infrastructure Protection (= Schutz kritischer Infrastrukturen)
Coordination Centers	sektorspezifische Teams von → SONIA
CSIRT	Computer Security Incident Response Team; Stelle zur Koordination und Ergreifung von Massnahmen im Zusammenhang mit sicherheitsrelevanten Vorfällen in der Informationstechnologie.
ICT	Information and Communication Technology → IKT
ICT-I	Bereich Informations- und Kommunikationsinfrastrukturen der Wirtschaftlichen Landesversorgung
IKT	Informations- und Kommunikationstechnologie
Informatikstrategieorgan Bund	Stabs-, Planungs- und Koordinationsorgan des Informatikrates Bund. Liefert Grundlagen für Steuerung und Koordination der Informatik in der Bundesverwaltung.
Information Assurance	→ Informationssicherung
Information Operations	→ Informationskrieg
Information Security	→ Informationssicherheit

Informationskrieg

Die Gesamtheit der Massnahmen, um die Entscheidungsfindungsprozesse eines Gegners zu stören, zu beeinflussen oder zu verunmöglichen, währenddessen die eigenen Entscheidungsfindungsprozesse geschützt oder verbessert werden.

Informationssicherheit

Fachgebiet, das sich mit der Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität und Verbindlichkeit von Informationen und Systemen befasst.

Informationssicherung

Ziel der Informationssicherung ist es, sicherzustellen, dass die zur Erreichung bestimmter Aufgaben benötigte Information zu jeder Zeit und in der erforderlichen Qualität vorhanden ist.

InfoSurance

Stiftung für die Sensibilisierung der Öffentlichkeit und der Wirtschaft im Bereich der Informationssicherung

IRT

Incident Response Team → CSIRT

ISB

→ Informatikstrategieorgan Bund

KIG

Koordinationsgruppe Informationsgesellschaft

KOSIO

Koordinationsorgan Schweiz für Informationsoperationen

MELANI

Melde- und Analysestelle Informationssicherung

PPP

Public Private Partnership;
Zusammenarbeit zwischen Wirtschaft und Staat

SFA

Strategische Führungsausbildung, Stelle der Bundeskanzlei zur Ausbildung von Departementsspitzen und Stäben des Bundesrates.

SFU

Strategische Führungsübung; Modul der → SFA

SONIA

Sonderstab Information Assurance

Wirtschaftliche Landesversorgung

Bundesstelle zur Sicherstellung der Versorgung der Schweiz mit lebenswichtigen Gütern und Dienstleistungen bei Mangellagen.

WL

→ Wirtschaftliche Landesversorgung

Impressum

Verfasser Informatikstrategieorgan Bund ISB
Friedheimweg 14
3003 Bern
Schweiz
www.isb.admin.ch

Kontaktperson
Dr. Ruedi Rytz
Tel. +41 31 323 45 07
Fax +41 31 322 45 66
E-Mail ruedi.rytz@isb.admin.ch

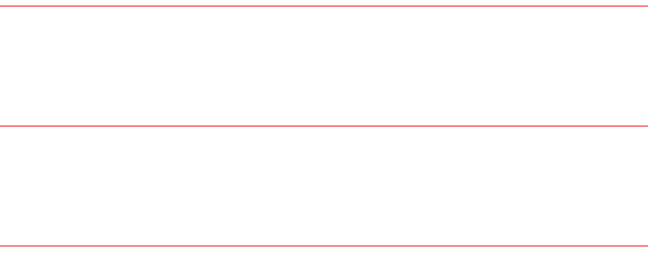
Mitwirkung Wirtschaftliche Landesversorgung
Generalstab Untergruppe Operationen

Gestaltung Ernst Basler + Partner AG, Zollikon

Druck Multicolor Print AG, Baar

Nachdruck Nur mit der Erlaubnis des Verfassers

Bern, Oktober 2002



critical infrastructure
critische infrastructuur
infrastructure vitale
information assurance
sigurete de inform
Informationss
critical infr
infrastructure v