Schutz kritischer Informationsinfrastrukturen – Aufgabe des Staates oder der Privatwirtschaft?

In den Neunzigerjahren tauchte in vielen modernen Staaten unter dem Schlagwort Critical Information Infrastructure Protection (CIIP) ein neues sicherheitspolitisches Thema auf. Der Schutz kritischer Informationsinfrastrukturen ist deshalb so bedeutsam, weil nicht nur das Funktionieren von Wirtschaft und Staat, sondern die Wohlfahrt aller Bürger immer stärker von der permanenten Verfügbarkeit dieser digitalen Nervensysteme abhängt. Durch die Privatisierung vieler lebenswichtiger Betriebe der öffentlichen Hand seit den Achtzigerjahren stellt sich die zentrale Frage, in welchen Situationen und Bereichen der Staat und in welchen der Privatsektor für Massnahmen und Vorkehrungen im Rahmen der nationalen Sicherheit verantwortlich ist.

Die Abhängigkeit des Staates, der Wirtschaft und der Gesellschaft von kritischen Informationsinfrastrukturen nimmt stetig zu. Gemäss Schätzungen würden bei einem Totalausfall der IT-Systeme 25% der Unternehmen Bankrott gehen, falls der Schaden nicht innerhalb kurzer Zeit behoben werden könnte. Bild: Photos.com

Wachsende Abhängigkeit von Informationsinfrastrukturen

Infolge der zügig voranschreitenden Informationsrevolution und der zunehmenden Vernetzung moderner Gesellschaften nimmt die Abhängigkeit von so genannten «kritischen Infrastrukturen» im Allgemeinen und «kritischen Informationsinfrastrukturen» im Speziellen zu. Die Informationsinfrastrukturen und -flüsse, die in diesen Netzwerken transportiert werden, sowie die dadurch ermöglichten Dienstleistungen und Prozesse bilden häufig die Grundlage für das Funktionieren aller anderen Infrastrukturen und verdienen deshalb besondere Beachtung (siehe *Kasten 1* und *2*).

Moderne Staaten haben bei einer grösseren Störung der Informationsinfrastruktur viel zu verlieren. Mehr als 70% der Erwerbstätigen in der Schweiz arbeiten im Dienstleistungssektor. Gemäss Schätzungen würden bei einem Totalausfall der IT-Systeme 25% der Unternehmen Bankrott gehen, falls der Schaden nicht innerhalb kurzer Zeit behoben werden könnte. Bei einer Bank zum Beispiel wäre dies schon nach zwei Tagen der Fall, bei einem Handelsunternehmen nach höchstens drei Tagen.[1] Diese Abhängigkeiten und die damit verbundenen Risiken und Gefahren für Ge-

Isabelle Abele-Wigert
Risikoanalyseteam,
Forschungsstelle für
Sicherheitspolitik
der ETH Zürich

1 Online-Interview mit Reto Stäheli, Head of Business Continuity Services, Swisscom IT Services.

Kasten 1

Was sind CIP und CIIP ?

Der Schutz kritischer Infrastrukturen (Critical Infrastructure Protection, CIP) ist kein neues Konzept und beschäftigt Staaten schon seit längerem. Als Teil nationaler Verteidigungspläne zum Schutz kritischer Objekte schon lange bekannt, hat sich der Fokus durch die zunehmende Abhängigkeit von Informations- und Kommunikationstechnologien insbesondere auf den Schutz kritischer *Informations*infrastrukturen (Critical Information Infrastructure Protection, CIIP) verschoben. Dabei geht es sowohl um den Schutz physischer Komponenten der Informationsinfrastruktur – wie zum Beispiel Computer oder Glasfaserkabel – als auch um den Schutz abstrakter Dinge wie vernetzte Systeme, Informationsflüsse oder das Internet. Das Ziel von CIIP ist es, dass Netz- und Systemunterbrechungen selten, von kurzer Dauer, beherrschbar, lokal begrenzt und von geringem Schadensausmass sind. Kurzum: Es geht um die Sicherstellung der Robustheit kritischer Dienstleistungen.

Kasten 2

Kritische (Informations-) Infrastrukturen der Schweiz

In der Schweiz gelten folgende *Infrastrukturen* als besonders kritisch: Regierung und öffentliche Verwaltung, Notfall- und Rettungswesen, (Tele-)Kommunikation, Energieversorgung, Finanz- und Versicherungswesen, Industrie und Gewerbe, Medien, Transport und Logistik, Gesundheitswesen und Wasserversorgung.

Zu den kritischen *Informationsinfrastrukturen* werden gemäss Experten beim Bund spezifisch gezählt: Telefon, Fax, Internet über Festnetz, Mobilnetz, Satelliten (GPS etc.), Kommunikationsnetze der SBB und der Elektrizitätswirtschaft, elektronische Medien, Kurzwellenfunk Bern-Radio, Funknetze der Behörden und Organisation für Rettungs- und Sicherheitswesen (Bors).

sellschaft, Wirtschaft und Staat werden von den Entscheidungsträgern und verantwortlichen Personen zunehmend erkannt.

Neue Ausgangslage durch Liberalisierung und Privatisierung

Durch die Liberalisierung und Privatisierung vieler lebenswichtiger Bereiche der öffentlichen Hand – wie Wasser, Strom, Transport oder Telefon – befindet sich auch in der Schweiz ein Grossteil der kritischen (Informations-)Infrastrukturen in privaten Händen. Somit stellt sich die zentrale Frage, in welchen Situationen und Bereichen der Staat für Massnahmen und Vorkehrungen im Rahmen der nationalen Sicherheit verantwortlich ist und wo der Privatsektor diese Aufgabe übernehmen muss.

Die Interessen der Privatwirtschaft und des Staates bei CIIP sind im Prinzip dieselben: Im Mittelpunkt stehen das reibungslose Funktionieren und die permanente Verfügbarkeit der Informationsinfrastrukturen. Die negativen Auswirkungen einer längeren Unterbrechung sind für beide Akteure gravierend. Unter dem steigenden Druck von Kostenminimierung und Gewinnmaximierung sind Firmen aber oft nicht bereit, über den informationstechnischen Schutz hinaus ausreichend Ressourcen für Sicherheit und Krisenmanagement zur Verfügung zu stellen.

Verschiedene Dimensionen des Problems

Es genügt nicht, CIIP als reines IT-Sicherheitsproblem zu behandeln, dem man alleine mit technischen Mitteln – wie etwa Anti-Virus-Software, Firewalls, Datenverschlüsselung und der Einhaltung von Standards – begegnen kann. Der Einbezug organisatorischer und personeller Faktoren sowie die Förderung von Public-Private Partnerships sind genauso bedeutend für die permanente Verfügbarkeit wichtiger Geschäftsprozesse.

Weiter ist die strafrechtliche Dimension zu erwähnen: Ohne die Hilfe von effektiven Strafverfolgungskonzepten, der Anpassung der nationalen Gesetzgebung und internationale Zusammenarbeit können die Gesellschaft und ihre kritischen Infrastrukturen nicht vor Internet- und Computerkriminalität geschützt werden.

Schliesslich kommt der sicherheitspolitische Aspekt hinzu, also Szenarien, welche die alltäglichen, routinemässigen Probleme privater Infrastrukturbetreiber übersteigen und eine landesweite Dimension annehmen – man denke etwa an die Stromausfälle in den USA. Um solche ausserordentlichen Fälle zu verhindern, sind Aktivitäten auf technischer, organisatorischer, gesetzgeberischer und internationaler Ebene notwendig.

Zentrale Bedeutung von Informationsaustausch und Kooperation

Diese verschiedenen Dimensionen von CIIP können zu Verständigungsproblemen und Interessenskonflikten zwischen den Akteuren bei der Suche nach effizienten Instrumenten und gemeinsamen Lösungen führen. Von zentraler Bedeutung ist dabei der kooperative Informationsaustausch zwischen privaten und staatlichen Akteuren sowie innerhalb der verschiedenen Sektoren.

Nicht immer zeigt die Privatwirtschaft aber Interesse an einer solchen Kooperation, auch wenn sie auf strategischer Ebene – z.B. im Bereich Terrorismusgefahr – unter Umständen Informationslücken hat, die der Staat füllen könnte. Dafür gibt es im Wesentlichen drei Gründe:

- Erstens wird befürchtet, dass sensible, mit dem Staat ausgetauschte Informationen über vorgefallene Sicherheitsprobleme nicht mit der nötigen Sorgfalt behandelt werden und dem eigenen Ruf schaden könnten.
- Zweitens wickeln viele in der Schweiz ansässige Firmen den Grossteil ihrer Geschäfte im Ausland ab.
- Drittens betrachtet die Privatwirtschaft CIIP aus einer betriebswirtschaftlichen Perspektive und interessiert sich weniger für die sicherheitspolitischen Aspekte als vielmehr für diejenigen der «Business Continuity».

Der Staat ist also vor die Herausforderung gestellt, die Privatwirtschaft davon zu überzeugen, dass CIIP auch über eine sicherheitspolitische Dimension verfügt, welche die Unternehmen zu ihrem eigenen Nutzen in ihren Risikoanalysen und Notfallplänen berücksichtigen sollten.

Das Vier-Säulen-Modell des Bundes

In der Schweiz beschäftigen sich auf Bundesebene eine Vielzahl von Verwaltungsstellen mit dem Schutz kritischer Informationsinfrastrukturen.[2] Kernstück der schweizerischen Informationssicherung bildet seit wenigen Jahren das sogenannte Vier-Säulen-Modell, das den verschiedenen Aspekten und Herausforderungen von CIIP Rechnung trägt. Es besteht aus den folgenden Säulen und Akteuren:

Prävention

Durch geeignete Massnahmen im technischen, organisatorischen, aber auch menschlichen Bereich (Ausbildung, Information) wird dafür gesorgt, dass sich möglichst wenige Vorfälle ereignen. Prävention erfolgt u.a. im Rah-

2 Vgl. Wigert (2005).

Kasten 3

Risiken und Gefahren

Zu den zahlreichen Risiken und Gefahren, welchen kritische Informationsinfrastrukturen ausgesetzt sind, gehört die höhere Gewalt. Dazu zählen Naturkatastrophen, zivilisatorische Katastrophen (z.B. Staudammbruch, AKW-GAU) und Personalausfall durch Streik oder Epidemie. Weitere Risiken sind organisatorische Mängel technischer oder personeller Natur, menschliches Fehlverhalten (aktiv oder passiv), technische Störungen, Abhängigkeiten und Versorgungsengpässe, (Cyber-)Terrorismus oder so genannte Information Operations[a]. Aber auch vor Gefahren durch die eigenen Mitarbeitenden für die Informationsinfrastrukturen und dem so genannten Social Engineering[b] müssen sich der Staat und die Unternehmen – unabhängig von ihrer Grösse – schützen.

a Einwirken auf gegnerische Informationssysteme bei gleichzeitigem Schutz eigener Systeme.
b Erlangen vertraulicher Informationen durch Annäherung an Geheimnisträger mittels sozialer Kontakte.

Kasten 4

Literaturverzeichnis

- Dunn, Myriam und Isabelle Wigert, The International Critical Information Infrastructure Protection (CIIP) Handbook. Zürich, Forschungsstelle für Sicherheitspolitik, 2004.
- Henriksen, Stein, The Shift of Responsibilities within Government and Society. Und: Andersson, Jan Joel und Andreas Malm, Minding the Gap: Reconciling Responsibilities and Costs in the Provision of Societal Security. In: CRN-Workshop Report. Societal Security and Crisis Management in the 21st Century. Stockholm 2004.
- Informatikstrategieorgan Bund ISB, Verletzliche Informationsgesellschaft. Herausforderung Informationssicherheit. Bern, Oktober 2002.
- Joint Economic Committee, United States Congress, Security in the Information Age. New Challenges, New Strategies. Washington, Mai 2002, S. 12. Internet: *www.fas.org/irp/congress/2002_rpt/jec-sec.pdf*.
- Metzger, Jan, The Concept of Critical Infrastructure Protection (CIP). In: A.J.K. Bailes / I. Frommelt (Hrsg.), Business and Security: Public-Private Sector Relationships in a New Security Environment. Oxford 2004.
- The President's Commission on Critical Infrastructure Protection (PCCIP), Critical Foundations: Protecting America's Infrastructures. Washington, Oktober 1997.
- The White House, The National Strategy to Secure Cyberspace .Washington, Februar 2003.
- Wigert, Isabelle, Der Schutz kritischer Informationsinfrastrukturen in der Schweiz: Eine Analyse von Akteuren und Herausforderungen. In: Wenger, Andreas (Hg.). Bulletin 2005 zur schweizerischen Sicherheitspolitik. Zürich, Forschungsstelle für Sicherheitspolitik, 2005.

men der sektorspezifischen Risikoanalysen, welche von den jeweiligen Betreibern der kritischen Infrastrukturen innerhalb der wirtschaftlichen Landesversorgung durchgeführt werden. Eine wichtige Rolle auf Bundesebene nimmt dabei die sei letztem Jahr operative Melde- und Analysestelle Informationssicherung (Melani) ein. Sie hat die Aufgabe, die Bevölkerung und kleine und mittlere Unternehmen sowie die Betreiber der kritischen Infrastrukturen vor dem Einsatz riskanter und unreifer Technologien zu warnen und auf Sicherheitslücken aufmerksam zu machen. Melani steht unter der Leitung des Informatikstrategieorgan Bund (ISB) und wird unterstützt vom Dienst für Analyse und Prävention des Bundesamtes für Polizei (Fedpol) und dem Computer Emergency Response Team (Cert) der Stiftung Switch. Während sich das ISB vor allem auf die Prävention konzentriert und Fedpol das nachrichtendienstliche Lagezentrum betreibt, kommt Switch-Cert die Bedeutung des technischen Support- und Kompetenzzentrums zu.

Früherkennung

Durch Melani sollen Gefahren und Bedrohungslagen möglichst früh erkannt werden, sodass Abwehrdispositive bereitgestellt beziehungsweise gewisse mit Risiken behaftete Technologien gemieden werden können.

Krisenmanagement

Der Sonderstab Information Assurance (Sonia) sorgt – zusammen mit dem Bereich Infrastruktur der Informations- und Kommunikationstechnologie (ICT-I) des Bundesamtes für Wirtschaftliche Landesversorgung (BWL) – als Instrument des strategischen Krisenmanagements dafür, dass die Auswirkungen von Störungen auf Staat, Wirtschaft und Gesellschaft auf ein Minimum beschränkt werden können.

Technische Problembehebung

Die technischen Ursachen für die Störungen müssen eruiert, analysiert und behoben werden. Dafür sind in erster Linie Melani und Partner aus Bund und Privatwirtschaft verantwortlich.

Balance zwischen Sicherheitsstandards und Wirtschaftlichkeit

Die Schweiz verfügt weder über eine umfassende nationale Strategie zum Schutz der kritischen Informationsinfrastrukturen noch über eine zentrale Stelle, die sich ausschliesslich mit CIIP befasst. Bestehende Kompetenzen und fundiertes Sachwissen werden traditionell da genutzt, wo sie bereits vorhanden sind, nämlich in den dafür spezialisierten Departementen und Stellen. Da CIIP ein derart breites Feld ist, werden die unterschiedlichen Teilaspekte sinnvollerweise von verschiedenen Organisationen abgedeckt. Allerdings kann dies mitunter zu Unklarheiten führen.

Von einigen Ausnahmen abgesehen bilden diejenigen Informationsinfrastrukturen, die der Staat aus der Perspektive nationaler Sicherheit schützen will, auch die Basis für die Wettbewerbsfähigkeit und Prosperität der Schweiz. Insofern ist nachvollziehbar, dass das ISB als einer der wichtigsten strategischen Akteure in der schweizerischen CIIP-Politik dem Eidgenössischen Finanzdepartement (EFD) unterstellt ist.

Dabei ist klar, dass bei kleinen, «alltäglichen» Gefahren für die Informationsinfrastrukturen – wie Viren, Hackerangriffe oder kurze Systemunterbrüche – in erster Linie die (privaten) Infrastrukturbetreiber selbst um einen adäquaten Schutz bemüht sein müssen. Wie auch in anderen Staaten liegt der Fokus in der Schweiz auf der Eigenverantwortung der einzelnen Unternehmen. Der Staat reguliert nur im Notfall und muss die richtige Balance zwischen Sicherheitsstandards und Wirtschaftlichkeit finden. Handelt es sich hingegen um Gefahren in der Grössenordnung von terroristischen Angriffen oder Naturkatastrophen, wird ein Agieren seitens des Staates erwartet, da es sich um ein sicherheitspolitisches Problem handelt.

Partnerschaft von Staat und Privatwirtschaft

Informationssicherung stellt einen Prozess dar, in welchem der ständige Austausch von Erfahrungen eine zentrale Rolle spielt. Der systematische Ausbau eines übergreifenden Informations-, Krisenmanagement- und Schutzsystems für die Informationsinfrastrukturen, wie es beim Vier-Säulen-Modell vorgesehen ist, kann aber nur in enger Partnerschaft von Staat und Privatwirtschaft realisiert werden. Das schweizerische Milizsystem, in dem die Kommunikation zwischen Politik und Wirtschaft seit langem gepflegt wird, ist hier gewiss von Vorteil. ▮