



Sperrfrist 27.11.07 13.30 Uhr  
Es gilt das gesprochene Wort

---

## **IT-Sicherheit verlangt Durchhaltevermögen**

Eröffnungsrede von Bundesrat Hans-Rudolf Merz; 10. Tagung für Informationssicherheit - Sicherheit im Wandel der Zeit: Sein versus Schein;

**Bern, 27. November 2007**

Dank den phänomenalen Möglichkeiten und Effizienzgewinnen hat die Internet-Revolution einen Vertrauensvorschuss zugunsten ihrer Branche bewirkt. Die Sicherheitsrisiken nehmen jedoch rapide zu. Das fundamentale Recht, in Ruhe gelassen zu werden, wird zunehmend ausgehebelt. Die Vernetzung digitaler Identitäten erlaubt präzise Profile von Individuen. Dabei entzieht sich das Vorgehen häufig einer politischen Kontrolle. Auch der Staat muss kritisch begleitet werden. Stimmen sagen, die grösste Gefahr im Internet gehe von den Regierungen aus. Nur mit Transparenz über den Gebrauch der Informationen und dem Hochhalten der Privatheit wird das Vertrauen der Nutzer gewahrt.

Im Jahr 1999 habe ich mich anlässlich der 2. Berner Tagung für Informationssicherheit zum Thema 'Gefährdung durch Öffnung' geäußert. Wesentliche Gedankenanstöße entnahm ich Reg Whitakers Kultbuch 'Das Ende der Privatheit'. Die Chancen, aber auch das Gefahrenbewusstsein offener Netze, waren damals bekannt. Das Dilemma zwischen Fortschritt und Freiheit bestand ebenfalls. Ich begann den Vortrag daher mit folgendem Computerwitz: Irgendwann werden alle Computer unserer Galaxie parallel geschaltet sein. Wenn man diesem Super-Computer dann die Frage stellt: Gibt es einen Gott? - dann werden sich der Himmel verfinstern und Donner grollen und die Antwort wird lauten: Ja, JETZT gibt es einen!

Darauf wies ich auf die Gefährdungen für das Individuum, also für uns einfache Menschen im gewöhnlichen Alltag hin; sodann machte ich auf die Gefährdungen für den Staat, also für uns als Männer und Frauen in der Gesellschaft hin; weiter sprach ich die Gefährdung unserer Wirtschaft durch Viren, Pannen, Hacker, Cybercrime an. Und am Ende war die Rede von dem, was passieren kann, wenn ganze Datenbanken quasi zum Gefahrenverbund zusammengeschlossen werden.

Seit 1999 hat sich in all dem nichts Grundlegendes verändert, somit gelten die meisten Kernaussagen aus jener Zeit auch heute noch. - Damit könnte ich meine Ausführungen hier bereits wieder schliessen.

Es ging mir als einem liberalen Politiker damals wie heute aber vor allem darum, für die Werte und Würde des Menschen einzustehen, zwischen Fortschritt und Gefahr zu unterscheiden. Ich wollte, dass wir die Rolle der Technik, der Forschung und jene des Staates klären. Und diese Forderung muss uns noch heute das zentrale Anliegen sein.

Ich gehe aus vom fundamentalen Bürgerrecht, in Ruhe gelassen zu werden. Der Berufsmensch braucht einen privaten Raum, um seinen Passionen nachzugehen und sein

Eigentum zu geniessen. Aber man braucht das Private nicht einfach als Freiraum zur Entlastung von den täglichen Zwängen. Privatheit ist auch deshalb lebensnotwendig, weil man nur in der Privatheit lernt, Bürger in der Öffentlichkeit zu sein. Bürgerliche Privatheit heisst also nicht nur Hegung des Eigenen, Selbstgenuss in der Familie und ihrem Eigentum, sondern Privatheit heisst auch Pflege der sozialen Funktionen.

Dieses fundamentale Recht, in Ruhe gelassen zu werden, wird durch die Informatik und Technik zunehmend ausgehebelt. An Begründungen fehlt es nicht: Crime Watch, Identifizierungen, Gläserne Welt. Sie kennen die zahllosen Motive für Überwachungen, GPS, Biometrik ja bestens.

Freilich haben wir das Datenschutzgesetz und viele Normen und Schranken im Umgang mit Menschen, mit Rechtsgütern, mit Wirtschaftstatbeständen. Und natürlich haben Ethik und Moral an Gewicht gewonnen, wenn es um Good Governance und wenn es um Codes of Conduct geht. Aber die technischen Entwicklungen gehen meist den ersten Schritt und sogar den zweiten voraus, ehe sich die Politik hinterher auch bewegen kann. Es ist eine Binsenwahrheit, dass an der Strassenkreuzung vorerst Unfälle passieren müssen, ehe der Verkehr geregelt und genormt wird.

Seit 1999 sind die Netze noch offener geworden und die Chancen und Einsatzmöglichkeiten dementsprechend grösser; die Abhängigkeiten und Sicherheitsrisiken damit eben auch.

Viele Neuerungen sind durchaus als Chancen wahrgenommen worden. Sie haben zu dem geführt, was wir heute als "Web 2.0" bezeichnen: Das Internet als multimediale und soziale Begegnungsplattform. Die virtuelle Welt hat Form angenommen, Stichworte sind "Second Life", "facebook", mySpace und andere. Auch was früher in intimen Tagebüchern geschrieben wurde, geht heute online.

Daran ist - um keine Missverständnisse aufkommen zu lassen - nicht alles schlecht. Ich glaube zum Beispiel, dass es kaum noch einen National- oder Ständerat ohne eigene Homepage gibt. Der grosse Gewinn liegt in der Authentizität der Botschaft. Mit Internet wird die Kontrolle über die eigene Aussage behalten. Wir sind nicht mehr nur auf die Medien als Überträger von Informationen angewiesen.

Aber mit neuen Technologien sind auch neue Risiken verbunden, und zum Teil bedrohen diese das Vertrauen in den elektronischen Geschäfts- oder Behördenverkehr. Man denke hier etwa an die neuen Angriffsformen im Internet Banking, wie z.B. "Phishing", "Pharming", "Man-in-the-middle" oder "Browser Poisoning". Mit solchen Angriffen muss man in Zukunft auch in anderen Wirtschaftszweigen und beim E-Government rechnen. Neben klassischen Hacking-Angriffen auf Server-Systeme ist auch der Client, d.h. das Gerät beim Nutzer in den Mittelpunkt der Betrachtung gerückt. Die Bedrohungslage ist hier äusserst vielfältig. Die entsprechenden Lösungsansätze sind komplex und zwangsläufig interdisziplinär.

Die Vernetzung verschiedener digitaler Identitäten erlaubt recht präzise Profile. Dabei entzieht sich das Vorgehen häufig einer politischen Kontrolle und stellt eine der grossen gesellschaftspolitischen Herausforderungen für die kommenden Jahre dar. Privatheit muss auch in einer von Technik dominierten Welt noch möglich sein. Darum ist der öffentliche Diskurs nötig. Darum müssen wir uns mit allen Vor- und Nachteilen dieses Themenkomplexes befassen.

Aber auch der Staat muss kritisch begleitet werden. Wenn der Internet-Guru und Gründermitleid des Hamburger Chaos Computer Club, Andy Müller-Maguhn, sagt, "Die grösste Gefahr im Internet geht von den Regierungen aus", muss dies ernst genommen werden. Das gilt beispielsweise, wenn der Staat Schutzmassnahmen für die Bürger unterbindet, weil er im Namen der Terrorismusbekämpfung alles sehen will. Hier sind schwierige Abwägungen der Interessen vorzunehmen.

Verschärft hat sich in den letzten 10 Jahren gerade das Bewusstsein für die Gefahr terroristischer Aktivitäten gegen oder mit Hilfe der IKT. Viele Infrastrukturen sind heute in viel stärkerem Masse gefährdet. Diese Bedrohung wird in den entsprechenden IKT-Lösungen noch nicht genügend reflektiert. Der Schutz kritischer Infrastrukturen ist eine andere grosse Herausforderung, die über die IKT hinausgeht. Die Bundesverwaltung hat im Rahmen der Melde- und Analysestelle Informationssicherung MELANI hier die Initiative ergriffen und auf eine auch im Ausland viel beachtete Art und Weise die Kugel ins Rollen gebracht. Das Kooperationsmodell von MELANI zwischen Verwaltung und Wirtschaft ist ein gutes Beispiel der Zusammenarbeit.

Eine absolute Sicherheit kann und wird es nie geben. Diese Weisheit gilt auch im Bereich der Informations- und Kommunikationstechnologien. In der Bundesverwaltung laufen derzeit viele Aktivitäten mit dem Ziel, die Informatiksicherheit so weit zu verbessern, dass die verbleibenden Restrisiken bekannt sind und auch getragen werden können. Das gilt namentlich auch für Projekte im E-Government.

Die Schweiz geniesst heute in Bezug auf Sicherheit, Verfügbarkeit und Stabilität international einen sehr guten Ruf. Als Fachleute sind Sie aufgerufen, mitzuwirken, dass dieser Ruf auch für die IKT gefestigt wird. Zum Teil ist das bereits gelungen. Mit Interesse habe ich vernommen, dass die SWIFT (Society for Worldwide Interbank Financial Telecommunication) kürzlich angekündigt hat, in der Schweiz ein Rechenzentrum als IKT-Hub für den internationalen Finanzbereich aufzubauen. Andere Marktgrössen haben in der Schweiz bereits Standbeine ihrer Forschungs- und Entwicklungstätigkeit aufgebaut.

Ich komme zum Schluss:

Dank den phänomenalen neuen Möglichkeiten und dank den Effizienzgewinnen hat die Internet-Revolution einen Vertrauensvorschuss zugunsten der IKT-Branche bewirkt. Sie

als Fachleute müssen nun damit richtig umgehen. Wenn Sie erstens transparent machen, was Sie mit den Informationen über die Bürger anstellen und was Sie unterlassen, und wenn Sie zweitens die Privatheit hochhalten, werden Sie auch in Zukunft das Vertrauen der Nutzer haben.

Die Verantwortliche für IT-Sicherheit in einer Schweizer Grossbank sagte kürzlich: "IT-Sicherheit verlangt Durchhaltevermögen".