



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



*Fachgruppe Security
(FGSec) der Schweizer
Informatiker-Gesellschaft*

Gefährdung durch Öffnung

Dr. Hans-Rudolf Merz
Ständerat

*Berner Tagung für Informationssicherheit 1999
Schützenswerte Daten in offenen Netzen
9. November 1999, Bern*

Gefährdung durch Oeffnung
Berner Tagung für Informationssicherheit 1999
Referat von Hans-Rudolf Merz, Ständerat, Herisau

Ich möchte mit zwei eher suggestiven Fragenkreisen beginnen: 1. Hatte es einen Sinn, gegen die Atomforschung angesichts der Kernspaltung zu protestieren und was erreicht man mit Widerstand gegen die gentechnologische Forschung mit Blick auf die DNA-Entschlüsselung und Genom-Analyse des Menschen? Wäre es nicht gescheiter gewesen, der Wissenschaft freien Lauf zu lassen? 2. Soll die Politik der Gesellschaft und ihren Trends/Entwicklung vorausseilen oder muss sie ihr hinterherhinken?

Das Dilemma zeigt sich auch hier ganz deutlich. Soll man vor Gefahren warnen, die ohnehin kräftig und durchschlagend sind wie ein riesiger Rinder-Trek, mit welchem die Farmer das amerikanische Land erobert, um nicht zu sagen niedergewalzt haben? Gefahren, die vielleicht im folgenden Computerwitz kulminieren: Irgendwann werden alle Computer unserer Galaxie parallel geschaltet sein. Wenn man diesem Supercomputer 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!

Trotz all dieser Fatalismen möchte ich den Warnfinger heben. Nicht mit dem Ohnmachtsfanal der Witwe Bolte von Wilhelm Busch, sondern mit dem bescheidenen Zeigefinger eines Parlamentariers.

Ich sehe vier Gruppen von Gefährdungen und möchte diese kurz darstellen, nämlich jene für das Individuum, jene für Gesellschaft und Staat sowie jene für Organisationen und die Wirtschaft.

1. Gefährdungen für das Individuum.

Ich gehe aus vom fundamentalen Bürgerrecht, in Ruhe gelassen zu werden. In einer Publikation der Bank Julius Bär findet sich behutsam geschildert: Den privaten Raum braucht der Berufsmensch, 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 durchaus auch deshalb lebensnotwendig, weil man nur in der Privatheit lernen kann, Bürger in der Oeffentlichkeit zu sein. Bürgerliche Privatheit heisst also nicht nur Hegung des Eigenen, Selbstgenuss in der Familie und ihrem Eigentum, sondern auch soziale Funktion.

Aber dieses fundamentale Recht, in Ruhe gelassen zu werden, wird durch die Technik zunehmend ausgehebelt. An Begründungen fehlt es nicht: Crime

Watch, Verkehrsführung, Verbraucheridentifizierung, Umwandlung von Information in Handelsware, Umleitung von Information in Statistiken ohne Zahl, Neugierde, Voyeurismus, Gläserne Welt usw. Sie kennen diese zahllosen Motive bestens.

Und Sie kennen selbstverständlich auch die Techniken: Simple Fotografie, Wanzen, biometrische Erkennungssysteme (Kreditkarten), Videoüberwachung, GPS (global positioning systems), Lasertechnik und dereinst wohl das bionische Gehirn, also die Vernetzung der quantitativen (Computer) mit der qualitativen (Gehirn) Intelligenz.

Freilich haben wir das Datenschutzgesetz als mehr oder weniger griffige Missbrauchsgesetzgebung. Aber wie weit ist der Weg noch vom heutigen Verbot mit Erlaubnisvorbehalt zur Erlaubnis mit blossem Verbotsvorbehalt, die Verwandlung der Privatheit in das Offen-Ungeschützte und in die Celebrity? Das erste psychoanalytische Protokoll von Sigmund Freud war geradezu eine Zeitungsmeldung gegenüber einem Interview von Larry King mit Monica Lewinsky im Internet

Was mir dabei Sorgen macht ist weniger die Rasananz der technischen Entwicklungen, sondern die zunehmende Unempfindlichkeit diesen gegenüber. Der offene Bauch eines Patienten im Live-Mitschnitt der Darmoperation, der nackte Leib von Audrey Hepburn im Internet, die letzten Lebensmomente in der Hoteldrehtüre von Prinzessin Diana sind nur oberflächlichste Hinweise auf diesen Eisberg.

In seinem lesenswerten Buch ‚das Ende der Privatheit‘ beschreibt Reg Whitaker das ursprünglich als Gefängnisbau vorgeschlagene Panopticon. Die Zellen sind rundum voneinander isoliert, der in der Mitte stehende Aufseher kann jedoch alle einsehen. Sinn ist Disziplinierung und Schulung. Da die Gefangenen befürchten, permanent überwacht zu werden und da sie Angst vor Bestrafung haben, verinnerlichen sie die Vorschriften. Wenn man über staatliche Nachrichtenbeschaffung für innere wie äussere Zwecke spricht, ist diese panoptische Ueberwachung in der Tat ein Schlüsselbegriff. Der panoptische Staat mit seinen Fähigkeiten, zu überwachen, kennt die Verteilung von Eigentum und Einkommen der Bürger, beispielsweise um sie zu besteuern. Der moderne Verwaltungsstaat hat häufig Anstoss zur Entwicklung neuer Technologien und Techniken der Ueberwachung gegeben, denken Sie an das Erfassungssystem für die LSVA oder im Strafvollzug an den elektronisch überwachten Hausarrest. Aber umgekehrt droht der Staat ebenso das Opfer zu werden, wenn Zahlungsvorgänge und andere Wirtschaftstransaktionen via Internet am Fiskus vorbei verrechnet werden, doch darüber später.

2. Gefährdung der Gesellschaft

Vielleicht sollten wir zunächst einmal unterscheiden zwischen Gefährdungen im Staat und solchen für den Staat.

Im Staat wächst generell die Bedeutung der Informatik. Die ganze Logistik (Strom, Wasser, öffentlicher Verkehr) und grosse Teile des Verwaltungsapparates werden über Informatik und Datenbanken abgewickelt. Der Mensch hat das Walten (oder glaubt es zu haben) und der Computer hat das Schalten. Am Horizont zeichnet sich hier bereits eine Kombination in Form von Knowbots, nämlich sog. intelligenter Software ab, die im Namen des Benutzers handeln kann. Klammer geschlossen.

Die Gefahren im Staat sind vom Delegierten für das Jahr 2000 und seiner Crew hinreichend aufgezeigt worden.

3. Die Gefährdung des Staates

Die globale Oekonomie des Verbrechens im oder trotz des Rechtsstaates (Geldwäscherei, Mafia) technisiert sich zunehmend, Internet und Handy gehören zur Grundausrüstung der Edelgangster.

Die grösste Gefahr sehe ich allerdings darin, dass offene Netze im Wirtschaftsverkehr keine Intermediatäre mehr brauchen. Steuerbegründende Abwicklungen, fiskalische Transaktionen und statistikrelevante Vorgänge gehen am Staat vorbei. Das Ergebnis wird aus Steuerausfällen und Zahlenverfälschungen bestehen. Darin wird sich die ganze Janusköpfigkeit offener Netze zeigen: mit mehr Möglichkeiten sind mehr Missbräuche verbunden. Faust steht in Mephistos Schatten. Die traditionellen Institutionen des staatlichen Gemeinwesens können mittels Nutzung der globalen und offenen Netzwerkstrukturen durch informelle Gruppen unterlaufen werden. Das kann letztlich zur unmerklichen Herabstufung des Rechtsstaates führen.

A propos Janusköpfigkeit: derzeit wird offenbar in den USA und in Frankreich unter dem Schlagwort ‚Krypto Debatte‘ die Verbindung von Informatik und Netzen diskutiert. Man kann sich einerseits der globalen offenen Netzwerkstrukturen des WWW bedienen, dabei aber ein sog. ‚private virtual network‘ aufbauen. Es erinnert an die Glasfassade moderner Gebäude, bei denen man von aussen nicht hineinsieht, von drinnen aber wohl beste Sicht nach aussen hat. Aus diesem Grund wird unter dem Stichwort ‚Key Recovery‘ die Forderung erhoben, dass die berechtigten Benutzer den Schlüssel-Algorithmus bei einer Zulassungsstelle hinterlegen müssen

Die Gefährdung für den Staat besteht in der Bedrohung im eigentlichen Sicherheitsbereich. Auf die militärischen Bedrohungen durch information warfare möchte ich im Themenkreise nicht eingehen. Vielleicht nur der

Reminder, dass die Erfindung des Internet der amerikanischen Militärtechnologie entsprungen ist. Von der aushebelnden Wirkung mafioser Kräfte wurde ebenfalls gesprochen. Die Bundesanwaltschaft könnte dazu mehr sagen, z.B. dass in unserem Land etwa 300 mafiose Organisationen daran sind, sich in das Normalgeschehen zu infiltrieren. Die Summen, um welche es geht, bewegen sich in den zweistelligen Milliarden. Anlässlich eines Staatsbesuches im Dezember 1998 konnte ich Ex-Ministerpräsident Tschernomyrdin zum Thema aus russischer Sicht befragen: er ist unumwunden der Ansicht, dass mehr als 50 Mia \$ das Land in Richtung Westen verlassen haben und dort gewaschen oder in ‚Legalstrukturen‘ versickert sind.

Eindrücklich war, dass die grossen Kurdendemonstrationen im Frühjahr 1999 in der Schweiz via Handy und Internet aus dem Ausland innert Minuten ausgelöst worden sind, dass aber unser Staatsschutz davon regelrecht überrumpelt war.

4. Gefährdung für die Wirtschaft

Hier ist weniger von Viren und technischen Pannen zu sprechen als vielmehr vom Patentschutz, vom geistigen Eigentum, von Werkspionage, Wirtschaftsnachrichtendienst, von Geheimhaltung im Rahmen der strategischen Verantwortung für ein Unternehmen oder einen Konzern und vielleicht von einigen Rechtsfragen wie der Behandlung von E-Mails, die (noch) vom WWW getrennt aber auf denselben Geräten übermittelt werden.

Nicht wahr, der Transfer von Zeichnungen und Plänen, von patentgeschützten Applikationen ist im globalen Wirtschaftsumfeld und im Lichte moderner Uebertragungstechniken ein kostenminimierender Faktor geworden. Der stetige Zwang zur Einführung neuer Technologien lässt oft Sicherheitsüberlegungen in den Hintergrund treten. Insbesondere Unternehmen, die sich mit Hochtechnologie befassen und davon leben, dass sie einen Innovationsvorsprung besitzen, müssen lernen, dass sie über hochsensibles Wirtschaftsgut verfügen. Der jüngste Fall des Verrats deutscher Rüstungstechnologie aus dem Münchner Dasa-Konzern an Moskau hat diese Dimension wieder einmal deutlich gemacht. In diesem Zusammenhang war übrigens zu erfahren, dass Russland das Personal seiner Geheimdienste wieder aufstockt, um die Wirtschaftsspionage zu intensivieren (NZZ 9.8.99). Man spricht von 10'000 Personen. Die Schäden aus Wirtschaftsspionage durch Cybercrime werden weltweit jährlich auf 40 Mia \$ geschätzt.

Zum Bereich von Wirtschaft und Organisationen gehört endlich auch die Börse, die sich je länger je mehr zum internetzugänglichen, virtuellen und damit standortunabhängigen Markt mausert. Das Börsengeschehen hat sich nicht nur vom wirtschaftlichen Geschehen etwas entfernt, es ist auch für den Teilnehmer und für den Staat (Stempel) immer weniger im wahrsten Sinne fassbar.

5. Gefährdungsverbund

Zum Schluss möchte ich beispielhaft auf einige Schnittstellen hinweisen, die sich als Gefährdungen in der Ueberlappung der Sphären von Individuum, Staat und Wirtschaft ergeben:

- ° im Bereich des Gesundheitswesens, für das wir jährlich bereits fast 40 Mia ausgeben. In diesem Bereich arbeiten gemäss KVG Versicherer (v.a. Krankenkassen) und Leistungserbringer (v.a. Aerzte und Spitäler) für den Leistungsempfänger (Patient) zusammen. Die Versuchung ist nun, Zahlen und Fakten aus dem Patientengut der Aerzte/Spitäler (Segmentation von Krankheiten) mit den Betriebszahlen der Leistungserbringer zwecks Optimierung der Versorgung zu vernetzen. Auf dem Weg über vernetzte Datenbanken entstünde heimlich das staatliche Gesundheitswesen
- ° im Bereich Konsum, wo vor allem das Sammeln, Auswerten und Vermarkten von statistischen Daten und Adressen hilfreich ist
- ° im Bereich der Medien, wo das Internet die traditionellen elektronischen Medien inhaltlich, rechtlich und kommerziell unterlaufen kann.

Nun zurück zur Eingangsfrage: Fatalismus oder nicht? Ich bin klar der Meinung, nein! Der Staat darf weder in der Kernforschung noch in der Gentechnologie noch in der Cyberentwicklung das blosse laissez-faire zulassen. Er muss – und darin besteht eine seiner wesentlichen Aufgaben – Sicherheit ermöglichen. Er muss sich aber auch vor sich selber schützen und verhindern, dass er zum Irrläufer und willenlosen Monstrum wird. Im Bereich Datenschutz ist dies bisher gut gelungen. Im Bereich der Gefährdung durch offene Netze muss er ebenfalls Schutzbedürfnisse befriedigen. Dass er der Entwicklung stets einen Schritt nachhinkt, braucht kein Nachteil zu sein, solange diese nicht entschwindet. Im Gegenteil: mit der Distanz wachsen Tritt- und Spursicherheit. Information Assurance ist deshalb ein Thema geworden.