Rede des Bundesministers des Innern, Dr. Wolfgang Schäuble, anlässlich der Eröffnung des Public Sector Parc auf der CeBIT am 4. März in Hannover

Dr. Wolfgang Schäuble, Bundesminister des Innern.

Zum dritten Mal in Folge habe ich die Ehre, Schirmherr des Public Sector Parc zu sein. Rund 250 Aussteller sind in diesem Jahr angemeldet, unter ihnen viele Unternehmen sowie öffentliche Institutionen von Bund und Ländern. Ihre technischen Lösungen sorgen für mehr Bürgerfreundlichkeit, senken die Energiekosten, verbessern den Datentransfer über Organisationsgrenzen hinweg und erleichtern die Geschäftsprozesse öffentlicher Verwaltungen. Ich denke, es lohnt sich auch in diesem Jahr, den Messeständen und Vorträgen in Halle 9 viel Aufmerksamkeit zu schenken, zeigen sie doch, in welch großem Umfang die Informationstechnik hilft, Verwaltung zu modernisieren.

Die Gelegenheit, hier am Eröffnungstag der CeBIT zu sprechen, möchte ich nutzen, um zwei mit der Informationstechnik verbundene Entwicklungen anzusprechen, die für einen Innenminister eine große Herausforderung bedeuten. Die eine Herausforderung ist die Modernisierung der Verwaltung. Wir müssen uns bemühen, die Informationstechnik auch in der öffentlichen Verwaltung optimal zu nutzen und ihren Einsatz noch besser zu steuern. Das gilt auch und gerade im Verhältnis zwischen Bund und Ländern. Die andere große Herausforderung ist die wachsende Internetkriminalität, die wir so gut wie möglich zurückdrängen und unterbinden müssen. Mit jedem Fortschritt geht leider einher, dass diejenigen Menschen, die sich auf Kosten anderer bereichern oder in anderer Weise anderen Schaden zufügen wollen, sich an die Entwicklung anpassen und sie für ihre Zwecke einsetzen. Mit dem zunehmenden Einzug neuer Informationstechnologien in unseren Alltag gehört es daher zu den wichtigen Zielen und Aufgaben eines Innenministers, die Sicherheit auch mit Blick auf die Möglichkeiten der Informationstechnologien und des Internet zu gewährleisten.

Lassen Sie mich an dieser Stelle eine Bemerkung zum jüngsten Urteil des Bundesverfassungsgerichts zur Online-Durchsuchung machen: Wir sollten hier sehr sorgfältig in unserer Prüfung sein und nicht vorschnell urteilen, wie einige dies leider in den letzten Tagen erkennen ließen.

In den letzten Jahren hat sich das Internet zum entscheidenden Kommunikationssystem für die Machenschaften von Terroristen entwickelt. Das Internet dient als Informationsbörse, Kommunikationsplattform und Bibliothek. Islamisten verlagern auch ihre Propagandaoffensiven verstärkt ins Internet. Dabei verwenden sie immer häufiger die englische und französische, aber auch die deutsche Sprache. Die zunehmend deutschen Texte und Untertitel erhärten die Einschätzung der Sicherheitsbehörden, dass auch Deutschland im Visier islamistischer Terroristen ist.

Heute werden sogar künftige Attentäter in virtuellen Terrorcamps ausgebildet. Anfang Januar 2008 fand das Gemeinsame Internetzentrum der deutschen Sicherheitsbehörden einen Lehrfilm zum Bau von Bomben. Wissenschaftler haben im Auftrag des Internetzentrums die Mixtur der Chemikalien geprüft und die Bombe nachgebaut. Das alarmierende Ergebnis war, dass eine nach den Vorgaben des Lehrfilms gebaute Bombe funktionsfähig ist. Die Chemikalien sind in Deutschland frei erhältlich. Auch der virtuelle Unterricht im Bombenbau zeigt, dass es in Deutschland eine reale Bedrohung durch den Terrorismus gibt.

Ein weiteres Problem im Zusammenhang mit neuen Informationstechniken ist die damit verbundene Verletzlichkeit unserer Infrastruktur. Die umfassende Nutzung des Internet für Informationsaustausch, Handel und Dienstleistung und die Vernetzung der IT-Systeme machen unsere Gesellschaften in einer neuen Weise angreifbar. Denken Sie nur an den massiven Angriff auf die IT-Systeme von Regierung und Wirtschaft der Republik Estland. Zwischen dem 27. April und dem 18. Mai 2007 waren Internetseiten von Regierungsinstitutionen und Online-Dienste von Banken nicht mehr erreichbar. Zeitweise musste der Internetverkehr nach Estland vollständig unterbunden werden. Der Angriff hat einen erheblichen Schaden bei den betroffenen Unternehmen verursacht und die Handlungsfähigkeit der Regierung vorübergehend eingeschränkt.

Viren, Trojaner und andere IT-Schädlinge richten allein in Deutschland einen volkswirtschaftlichen Schaden von circa 3,5 Milliarden Euro pro Jahr an. Die Fachleute sprechen von einer zunehmenden Professionalisierung der Täter. Diebstahl und Missbrauch persönlicher Daten nehmen zu. Dieses Ausspähen ist ein einträgliches Geschäft mit recht geringem Entdeckungsrisiko. Die Täter verkaufen die Kontozugangsdaten und Transaktionsnummern von Online-Banking-Kunden an andere Kriminelle. Sie haben laut BITKOM 2006 auf die-

se Weise rund 13 Millionen Euro erbeutet, 2007 dürfte die Summe noch größer sein. Und es kommen neue Opfergruppen hinzu: Mit den persönlichen Daten der Besucher von Spiele-Portalen verdienen Kriminelle heute bereits mehr als mit gestohlenen Kreditkarten-Nummern.

Die unterschiedlichen Beispiele – terroristische Aktivitäten, flächendeckende Cyber-Angriffe wie auch vor allem die Zunahme der Alltagskriminalität im Internet, etwa in Form von Datenklau – zeigen, dass mit dem Fortschritt der Technologie ein Wandel der Kriminalität und krimineller Vorgangsweisen einhergeht, auf die wir reagieren müssen, wenn wir uns dagegen schützen wollen.

IT-Sicherheit ist eine gemeinschaftliche Aufgabe. Es ist wichtig, dass die Bürgerinnen und Bürger um die Risiken der neuen Kommunikationstechnologien wissen und sich individuell schützen. Wir dürfen die privaten Nutzer aber auch nicht mit dieser Aufgabe alleine lassen und ihnen die gesamte Verantwortung für die IT-Sicherheit aufbürden. Auch die Hersteller von Hard- und Software müssen ihre Verantwortung besser wahrnehmen. Sie bringen noch viel zu häufig fehlerhafte Produkte auf den Markt, deren Schwachstellen dann von Cyber-Kriminellen ausgenutzt werden.

Und natürlich befasst sich auch die Politik mit dieser Herausforderung. Es ist die Pflicht des Staates, auch in der virtuellen Gesellschaft für das notwendige Maß an Sicherheit, Verbindlichkeit und Vertraulichkeit zu sorgen. Dazu gehört der aktive Schutz von Informations- und Kommunikationssystemen. Hundertprozentige Sicherheit gibt es nicht, aber wir müssen alles tun, um so viel Sicherheit wie möglich zu gewährleisten. IT-Sicherheit ist deshalb ein fester Bestandteil unserer nationalen Sicherheitspolitik.

Die Bundesregierung hat im Jahr 2005 den Nationale Plan zum Schutz der Informationsinfrastrukturen verabschiedet. Seine Umsetzung koordiniert das Bundesamt für Sicherheit in der Informationstechnik, das längst nicht mehr nur eine beratende Funktion hat. Es soll nach innen ebenso wie nach außen als einzige staatliche IT-Sicherheitsbehörde agieren. Aus diesem Grund wird das BSI-Gesetz zurzeit überarbeitet.

Auch der Verein Deutschland sicher im Netz befasst sich mit dem Schutz der Informationsinfrastrukturen. Hier engagieren sich Unternehmen, Branchenverbände, Wissenschaftler und Vereine, indem sie Informationsangebote für Verbraucher und Unternehmen bereitstellen. Als Schirmherr des Vereins möchte ich allen Akteuren für dieses Engagement herzlich danken. Ihre Arbeit ist angesichts der sich immer wieder ändernden Bedrohungen unverzichtbar.

Ein wichtiges Thema der IT-Sicherheit ist die überschaubare, vertrauenswürdige und verlässliche Identifizierung, damit im Internet das Recht auf informationelle Selbstbestimmung gewahrt bleibt und die „digitale Identität" von Bürgerinnen und Bürgern geschützt wird.

Sie sollten sich einfach und sicher im Internet ausweisen können – genauso einfach wie heute mit Ihrem Personalausweis. Und Sie sollten online auch einfach und rechtsverbindlich Ihre Unterschrift leisten können. Deshalb entwickeln wir den elektronischen Personalausweis. Er bringt mehr Sicherheit für die digitale Identität des Ausweisinhabers. Mehr Sicherheit für die Kommunikation im Internet ist auch das Ziel der Bürgerportale, das sind im Kern datenschutz- und verbraucherfreundliche E-Mail-Dienste und elektronische Postfächer. Für das Bundesministerium des Innern bilden diese beiden IT-Projekte einen wichtigen Schwerpunkt auf dieser CeBIT. Der Planungsstand erlaubt es in beiden Fällen, jetzt Kooperationen für die Umsetzungsphase zu suchen. Ich lade daher die Diensteanbieter aus Wirtschaft und Verwaltung ausdrücklich ein, sich aktiv in die Projekte einzubringen.

Wir müssen die Informationsinfrastrukturen schützen. Wir müssen Technologien zum Schutz der Nutzer entwickeln. Wir müssen darüber hinaus aber noch mehr tun, um die Garantiefunktion für die Informationsinfrastrukturen verlässlich zu erfüllen. Wir brauchen klare, eindeutige und beständige Regelungen für die IT-Steuerung, um die Informationsinfrastrukturen zu schützen. Damit komme ich zum zweiten Thema, über das ich zu Ihnen sprechen will, der Neuregelung der IT-Steuerung im Rahmen der Föderalismusreform.

Im Bund haben wir seit Dezember 2007 das Konzept „IT-Steuerung Bund". Es etabliert neue Steuerungsstrukturen in der Bundesverwaltung. Hochrangige IT-Beauftragte in den Ressorts bilden gemeinsam den Rat der IT-Beauftragten für die ressortübergreifende IT-Steuerung. Der Rat der IT-Beauftragten beschließt die Strategien, Architekturen und Standards der Bundesverwaltung und ist somit für das IT-Fundament des Bundes verantwortlich.

Zusätzlich zu dem Rat gibt es die IT-Steuerungsgruppe. Das Bundsministerium des Innern, das Bundesministerium der Finanzen und das Bundeskanzleramt sorgen hier für eine stärkere Verzahnung von IT-Steuerung, politischer Steuerung und haushalterischer Umsetzung. So können wir Einigungsprozesse deutlich beschleunigen.

Die Arbeit der beiden Gremien wird durch den Beauftragten der Bundesregierung für Informationstechnik komplettiert. Zu seinen wichtigsten Aufgaben zählen nun die Erarbeitung der IT-Strategie des Bundes und die Steuerung der zentralen IT-Infrastrukturen. Ich bin sicher, dass Herr Staatssekretär Dr. Beus, der diese Funktion am 1. Januar 2008 übernommen hat, Ihnen heute Mittag an gleicher Stelle einen programmatischen Einblick in seine Pläne für die kommenden Jahre geben wird. Den Vertretern der Länder und Kommunen ebenso wie der Wirtschaft kann ich versichern, dass Sie mit Herrn Beus einen kompetenten Ansprechpartner für die Zusammenarbeit mit der Bundesregierung haben.

Die Steuerung ebenenübergreifender IT-Vorhaben ist weniger klar geregelt. In den letzten Jahren wurden verschiedene

Wege der Kooperation beschritten. Aufgrund dieser Erfahrungen hat der Bund die Verbesserung der IT-Steuerung im föderalen System seit März 2007 regelmäßig auf die Tagesordnung der Föderalismuskommission II gesetzt. Wir sind der festen Überzeugung, dass die Steuerung der Informationstechnik durch Bund, Länder und Kommunen verbessert werden muss.

Vor allem in den Gemeinschaftsprojekten benötigt die fach- und ebenübergreifende Umsetzung von IT-Projekten häufig zuviel Zeit, das einzuführende IT-System wird gelegentlich – wie beispielsweise beim BOS Digitalfunk – von der Innovationsgeschwindigkeit der Technik überholt. Wenn alle Beteiligten es endlich eingeführt haben, ist es schon veraltet. Eine Lösung sind querschnittliche Einrichtungen innerhalb der Kommunen, innerhalb der Länder und im Bund – doch nur solang es sich nicht um ebenenübergreifende Projekte handelt.

Wir sind nach sieben Jahren E-Government in Deutschland an einem Punkt angekommen, an dem die IT-basierte Neugestaltung von Verwaltungsprozessen nicht mehr durch einzelne Behörden oder eine staatliche Ebene allein realisiert werden kann. Die wichtigen IT-Projekte, das sind heute stets ressort- und ebenenübergreifende Vorhaben. Denken Sie an die Umsetzung der EU-Dienstleistungsrichtlinie oder die Einführung der einheitlichen Behördenrufnummer D115. Bisher basiert die ressort- und ebenenübergreifende Zusammenarbeit auf dem freiwilligen Zusammenwirken der Behörden und auf dem Konsens-Prinzip. Entscheidungen werden nur getroffen, wenn alle Beteiligten sich einigen können. Leider kommt es dadurch immer wieder zu erheblichen Projektverzögerungen und zum Neuaufsetzen von Projekten.

Das Recht ist das klarste, eindeutigste und beständigste Steuerungsinstrument für die Verwaltung – das sage ich jetzt nicht als Jurist, sondern aufgrund von vier Jahrzehnten Verwaltungserfahrung. Ich denke, es wäre daher sinnvoll, einen angemessenen Rechtsrahmen für die Bund-Länder-übergreifende IT-Steuerung zu schaffen. Die Föderalismusreform II bietet hierzu eine gute Chance. Das Zusammenwirken der Behörden bei der IT muss zu einer generellen Pflicht von Bund, Ländern und Kommunen werden.

Wir brauchen eine zeitgemäße und beständige Steuerung der Informationstechnik, eine IT-Governance. Die IT-Governance hat drei entscheidende Vorzüge: sie stärkt die Handlungsfähigkeit und die Sicherheit des Gesamtstaates, sie erspart allen staatlichen Ebenen Kosten und sie fördert die Wettbewerbsfähigkeit Deutschlands.

Mit ihr würde es zum Beispiel möglich, eine bundesweite sichere IT-Netzinfrastruktur der deutschen Verwaltung aufzubauen. Ein vom Bund betriebenes IT-Koppelnetz für alle Gebietskörperschaften Deutschlands, über das alle IT-Verfahren auch im Krisenfall sicher abgewickelt werden können. Diese IT-Infrastruktur würde gemeinsam geplant – ähnlich der Verkehrswege- oder der gemeinsamen Finanzplanung. Sie würde mit gemeinsam verantworteten IT-Sicherheitsrichtlinien betrieben, die den Anforderungen des Bundes, der Länder und der Kommunalebene an Verfügbarkeit und Sicherheit gerecht würden. Das ist ein großes Vorhaben. Ohne fest umrissenen Rechtsrahmen werden wir das nicht schaffen. Ich bin deshalb der Auffassung, dass die heute lebenswichtige IT-Infrastruktur einen Platz im Grundgesetz benötigt – neben Basis-Infrastrukturen wie Luftverkehr, Eisenbahnen, Autobahnen und Wasserstraßen. Das werden wir mit den Ländern im Rahmen der Föderalismusreform weiter diskutieren.

Ein zweites Beispiel für das Potenzial der IT-Governance sind Interoperabilitätsstandards. Werden die Anforderungen an die Interoperabilität verbindlich festgelegt, vereinfacht das die elektronische Kommunikation zwischen Verwaltungen ebenso wie zwischen Verwaltung und Wirtschaft bzw. Bürgern. In diesem Fall böte das Recht die beständige Grundlage für ein Verfahren, das die Ziele Verabredung, Durchsetzung und Fortentwicklung der Standards verbindlich kanalisiert.

Ein drittes Beispiel ist die Etablierung einer neuen Art der Verwaltungszusammenarbeit. Durch die Bündelung von IT-Leistungen in Shared Service Centern sind – wie wir bereits wissen – hohe Effizienzgewinne zu erreichen. Sie können standardisierbare Prozesse und Verwaltungshilfsdienste zusammenfassen und effizienter erbringen. Die Verankerung einer entsprechenden Rechtsfigur im Grundgesetz würde die die Kooperation von Verwaltungen bei der IT rechtlich absichern.

Als Innenminister ist es meine Aufgabe, für Sicherheit und Verlässlichkeit zu sorgen – sofern es Deutschland betrifft, auch im virtuellen Raum. Angesichts sich verändernder Chancen und Gefahren müssen die Parameter von Sicherheit und Freiheit in der modernen Informationsgesellschaft immer wieder neu ausgelotet werden. Das sollten wir nicht gegeneinander tun, sondern miteinander.

Bei der Modernisierung der Verwaltung ist es mein Ansatz, die IT-Steuerung den neuen Anforderungen der Informationstechnik so anzupassen, dass sie ihnen gewachsen ist. Dabei geht es nicht um Zentralisierung, sondern um verbindliche Regeln, die schnelles und sicheres Handeln erlauben. Das ist im Kern die Idee der IT-Governance.

Die öffentliche Verwaltung hat in den letzten 15 Jahren große Fortschritte beim Einsatz der Informationstechnik gemacht. Dennoch gibt es natürlich noch viele Verbesserungsmöglichkeiten. Das ist keine Aufgabe, die im Alleingang bewältigt werden kann. Wir brauchen den Austausch der Fachleute über Ziele und Lösungswege. In diesem Sinne eröffne ich den Public Sector Parc der CeBIT 2008 und wünsche anregende Diskussionen.