*Informationsgesellschaft sicher gestalten*

**Rede**
**von Bundesminister**
**Dr. Wolfgang Schäuble**
**beim 10. Deutschen IT-Sicherheitskongress**
**des Bundesamtes für Sicherheit**
**in der Informationstechnik**
**am 22. Mai 2007 in Bonn**

Der IT-Sicherheitskongress des Bundesamtes für Sicherheit in der Informationstechnik findet in diesem Jahr zum zehnten Mal statt: Ein solches Jubiläum ist ein guter Anlass, um zurückzuschauen, Bilanz zu ziehen und sich zu fragen, welche Aufgaben noch vor uns liegen.

Die Kongressreihe des Bundesamtes ist zu einer der wichtigsten Veranstaltungen zum Thema IT-Sicherheit im deutschsprachigen Raum geworden. Das unterstreicht die herausragende Stellung des BSI als dem Kompetenzzentrum für Informationssicherheit in Deutschland – und auch darüber hinaus.

Das BSI geht auf die Zentralstelle für das Chiffrierwesen zurück, die Mitte der 50er Jahre gegründet worden war und sich insbesondere mit kryptographischen Verfahren sowie deren Koordination und Standardisierung im Rahmen der NATO befasste. Die Verschlüsselung von Nachrichten, die Unbefugte am Mitlesen hindern sollte, spielte schon seit Urzeiten in der Geschichte eine wichtige Rolle: Bereits im 6. Jahrhundert wendeten die Spartaner die Technik des Vertauschens von Buchstaben an, um geheime Botschaften zu übermitteln. Wir alle kennen die bekannteste Chiffriermaschine der jüngeren Geschichte ENIGMA, die zunächst als ziviles Chiffriersystem konzipiert worden war und 1918 zum Patent angemeldet wurde. Legendäre und traurige Berühmtheit erlangte sie dann im Zweiten Weltkrieg.

1989 machte die Zentralstelle für das Chiffrierwesen ihre erste Wandlung durch und wurde in Zentralstelle für die Sicherheit in der Informationstechnik umbenannt. Mit der Namensänderung einher ging eine Erweiterung der Aufgaben, zu denen nun auch die Sicherheit in der IT gehörte. Es war übrigens noch diese Zentralstelle, die den ersten IT-Sicherheitskongress durchführte.

Der Rückblick zeigt, dass man schon früh erkannte, wie wichtig es ist, über die Informationstechnik und damit verbundene Gefahren aufzuklären – auch wenn die flächendeckende Verbreitung der Informationstechnologie damals noch nicht absehbar war. Man muss sich an die Technologien Ende der 80er Jahre erinnern: Zeitungen, Radio und Fernsehen sowie Telefon, Fax und Briefsendungen bestimmten die Kommunikation der Menschen untereinander. Auch wenn alles immer etwas farbiger wurde und man das eine oder andere Kabel am Telefon einsparen konnte, so hatte sich an der Art unserer Informationsbeschaffung und -verteilung sowie an der Weise der Kommunikation über Jahrzehnte hinweg wenig geändert.

Anfang der 90er Jahre gab es nahezu revolutionäre technologische Veränderungen: Computer – mit ihnen E-Mail und Internet –, Mobiltelefone und viele andere Formen der Digitalisierung hielten Einzug ins tägliche Leben und die Arbeitswelt. Die Bürgerinnen und Bürger haben heute selbstverständlich nicht nur an ihrem Arbeitsplatz einen Computer stehen und nutzen elektronisch automatisierte Verfahren. Auch aus dem Privatleben ist die neue Informations- und Kommunikationstechnik nicht mehr wegzudenken.

Die Computertechnologie hat uns vielfältige Erleichterungen gebracht. Das Arbeiten an und mit elektronischen Dokumenten ist in vielerlei Hinsicht schneller und unkomplizierter. Man bekommt heute fast alle Informationen im Handumdrehen über das Internet. Bankgeschäfte oder Behördengänge können wir elektronisch erledigen, sogar online einkaufen, ohne das Haus verlassen zu müssen.

Aber jede Medaille hat zwei Seiten. Neben neuen Freiheiten und Bequemlichkeiten sind neue Abhängigkeiten und Gefährdungen entstanden. IT-Systeme sind – egal ob es sich um private Anwenderinnen und Anwender oder ein ganzes Firmennetz handelt – Hackerangriffen und Bedrohungen durch Viren und Würmer ausgesetzt.

Fred Cohen schuf 1983 das erste belegte Computervirus im Rahmen einer Doktorarbeit. Er schrieb ein Programm, das andere Programme veränderte, indem es sich selbst darin einpasste und reproduzierte. Die Folgen seiner Erfindung hat er wahrscheinlich nicht vorhergesehen. Heute soll es zwischen 60.000 und 100.000 verschiedene Arten von Viren geben. Hinzu kommen andere Computerschädlinge wie Trojanische Pferde, Würmer und neuerdings Spionagesoftware. Die steigende Unabhängigkeit moderner Informationstechnologie von mechanischen Speichermedien wie Disketten und die ständig zunehmende Nutzung des Internets beschleunigen die Verbreitung der Schadprogramme.

Neben der zunehmenden Quantität von Schadprogrammen ist aber vor allem ihre neue Qualität besorgniserregend. Schadprogramme sind weniger darauf ausgerichtet, direkten und bemerkbaren Schaden anzurichten, als vielmehr Kontrolle über Rechner zu erlangen und Daten auszuspionieren. In einer Zeit, in der digitale Informationen einen immer höheren Stellenwert haben, ist das vorrangige Ziel der Programmierer dieser Schadprogramme eine anhaltende Präsenz auf dem infizierten Computer. So können möglichst viele Daten über einen langen Zeitraum gesammelt werden, beispielsweise um diese gewinnbringend an andere Kriminelle zu verkaufen.

Statistiken und Erhebungen belegen, dass Schadcodes, die vertrauliche Daten ausspähen sollen, einen immer höheren Anteil an den verbreiteten Schadprogrammen ausmachen: Von den 60 gefährlichsten Schadprogrammen im Jahr 2005 waren mehr als drei Viertel darauf angesetzt, Daten auszuspionieren.[1]

---

[1] Vgl. z. B. den 9. Sicherheitsreport von Symantec (Zeitraum 01.07.2005-31.12.2005).

Auch der Bericht des BSI zur „Lage der IT-Sicherheit in Deutschland“, der heute veröffentlicht wird, hält diese Entwicklung für bedrohlich. Das BSI beschreibt in diesem Bericht auch eine neue Art der Programmierung: Kriminelle bauen Schadprogramme immer modularer auf. Sie hinterlegen mehrere kleine Programme auf Rechnern, die auf Anweisung des Angreifers weitere Schadfunktionen nachladen können. Weil sich die Programme ständig verändern, können herkömmliche Virenschutzprogramme sie nur schwer erkennen.

Also ist sichere Informationstechnik heute eine strukturelle Herausforderung für moderne Industriestaaten. Aufgrund der zunehmenden Durchdringung des gesamten gesellschaftlichen Lebens mit neuen Informations- und Kommunikationstechnologien brauchen wir Lösungen, die die Nutzung dieser Technologien dauerhaft sicher machen.

Dabei geht es nicht allein um Computertechnik. Genauso sind beispielsweise Handhelds oder Mobiltelefone betroffen. 82 Prozent der deutschen Haushalte besaßen im Jahr 2005 ein Handy – die Tendenz ist steigend, und der Trend geht zu mehreren Geräten pro Haushalt.[2] Der Lagebericht des BSI stellt fest, dass die Infektionen von solchen mobilen Endgeräten zunehmen. Im Vergleich mit PCs ist das Risiko zwar noch gering, aber die Zahl bekannter Schadprogramme ist seit dem ersten Auftreten im Jahr 2004 immerhin auf einen dreistelligen Wert gestiegen.

Die Angriffe auf Netzwerke, Computer und mobile Kommunikationsgeräte mehren sich auffallend. IKT-Systeme werden dabei zunehmend zu Spionagezwecken genutzt – sowohl zum Ausspähen der Regierung als auch zur Wirtschafts- und Forschungsspionage. IT-Sicherheit ist daher ebenso wichtig für den Wirtschaftsstandort Deutschland wie für die Innere Sicherheit unseres Landes.

---

[2] Informationstechnologie in Unternehmen und Haushalten 2005, Statistisches Bundesamt, Wiesbaden 2006.

Bürgerinnen und Bürger ebenso wie Unternehmen oder die öffentliche Verwaltung müssen sicher kommunizieren können. Die Sicherheit und Zuverlässigkeit von Computeranwendungen kann sogar lebenswichtig sein: Computertechnik in medizinischen Geräten muss verlässlich funktionieren, am besten auch Anlagen zur Steuerung von Flugzeugen. Korrekt und zuverlässig arbeitende Computerprogramme sind auch eine entscheidende Voraussetzung für komplexe industrielle Produktions- und Steuerungsprozesse. In sicherheitskritischen Anwendungen kann der Ausfall oder schon eine Fehlfunktion technischer Anlagen aufgrund eines Softwarefehlers katastrophale Folgen für Menschen, Sachwerte und Umwelt haben.

Inzwischen sind Hardware- und Software-Lösungen zum Schutz der IT überall im Einsatz. Besonders Internet-bezogene Dienstleistungen wie Firewall, Viren- und Spamschutz sowie deren Aktualisierung sind ein bedeutender Umsatzfaktor der IT-Branche. Marktführer im IT-Sicherheitsmarkt sind die USA; Deutschland belegt immerhin einen guten zweiten Platz – allerdings mit großem Abstand. Der globale Security-Markt hat derzeit ein Volumen von 60-70 Mrd. Euro und wächst um rund 8 Prozent im Jahr. Allein die IT-Sicherheitsindustrie setzt davon rund 15-20 Mrd. Euro um. Deutsche Anbieter haben daran einen Anteil von rund 10 Prozent.

Leistungsfähigkeit und Sicherheit der IT-Infrastruktur können über die Wettbewerbsfähigkeit eines Unternehmens entscheiden. Und sie sind auch ein wesentliches Kriterium im Wettbewerb um Industriestandorte. Eine effiziente Sicherheitsarchitektur ist aus vielen Gründen unverzichtbar. Deswegen muss das Bewusstsein für IT-Sicherheit geschärft und vorbildliche Sicherheit in Unternehmen noch nachhaltiger kommuniziert werden.

Dabei ist IT-Sicherheit natürlich eine dynamische Aufgabe. Die Sicherheitsbehörden müssen sich permanent auf neue Kriminalitätsformen und Gefahren einstellen. Die Forschung leistet dabei wichtige Hilfe. Die Bundesregierung hat daher Anfang des Jahres das erste Nationale Sicherheitsforschungsprogramm beschlossen, mit dem die Entwicklung innovativer Technologien zur Stärkung der zivilen Sicherheit in Deutschland gefördert werden

soll. Die erste Förderperiode ist bis zum Jahr 2010 angelegt, und sie hat einen Umfang von rund 123 Millionen Euro.

Gegenstand der Forschung sind Konzepte und Lösungen, die Schutz vor und bei Terroranschlägen, Kriminalität, Umweltkatastrophen oder auch Zusammenbrüchen von kritischen Infrastrukturen bieten sollen. Verkehrssysteme, Kommunikationsnetze, Versorgungssysteme oder Warenströme sollen weniger anfällig für Katastrophen und damit für Angreifer unattraktiver werden. Gesucht werden auch Lösungen für eine rasche und umfassende Krisenreaktion und Frühwarnsysteme bei Gefährdungen verletzlicher Infrastrukturen.

Das Nationale Sicherheitsforschungsprogramm zielt also auf Lösungen zur Erhöhung der Sicherheit der Menschen und zum Schutz lebenswichtiger Infrastrukturen. Folgende Szenarien stehen dabei im Vordergrund: Schutz und Rettung von Menschen, Schutz von Versorgungs- und Verkehrsinfrastrukturen sowie Sicherung der Warenketten. Fragen der IT-Sicherheit werden dabei einen großen Raum einnehmen.

Seit der Gründung des BSI hat es sowohl enorme politische Veränderungen als auch gewaltige technologische Entwicklungen gegeben. Politisch betrachtet gab es bis Anfang der 90er Jahre zwei unterschiedliche Gefährdungen für die Sicherheit unseres Landes: Bedrohungen der inneren und äußeren Sicherheit waren für jedermann als zwei unterschiedliche Gefährdungsszenarien erkennbar. Diese klassische Trennung in äußere Sicherheit – also die Verteidigung gegen militärische Angriffe von außen – und innere Sicherheit – die Bekämpfung von Kriminalität und Terrorismus im Inland – lässt sich heute nicht mehr aufrechterhalten. Die Grenzen verschwimmen.

Parallel zu diesen politischen Veränderungen erleben wir in gleichem Maße seit Anfang der 90er Jahre technologische Veränderungen grundsätzlicher Art: Der unaufhaltsame Siegeszug der Informations- und Kommunikationstechnologien begann und setzt sich bis heute ungemindert fort.

Auch wenn es kaum möglich ist, genau zu sagen, in welchem Umfang politische Veränderungen durch die technische Entwicklung verursacht wurden, so ist es doch gewiss, dass die neuen Technologien einen ganz entscheidenden Anteil daran hatten.

Die globale Vernetzung bietet neue Chancen und vielen Menschen, Völkern und Staaten die Möglichkeit, am weltweiten Informationsfluss teilzuhaben. Die Erfolgsgeschichte des Internet hat allerdings die Kehrseite, dass sie die Spaltung der Welt und ihre Bedrohungspotentiale unmittelbar erlebbar macht. Das sind die zwei Seiten der Medaille.

Die Möglichkeiten des *world wide web* werden in vielfältiger Art und Weise auch von Straftätern genutzt. Neuartige Delikte wie Phishing oder E-Bay-Betrug gehören ebenso dazu wie eine Nutzung des Internet für die Vorbereitung von Terroranschlägen. Weil kriminelle und terroristische Gruppierungen zunehmend über PC und Internet kommunizieren, gibt es für die Sicherheitsbehörden immer weniger Ermittlungsansätze in der „realen“ Welt. Also müssen Polizei und Verfassungsschutz in der virtuellen Welt ermitteln, wenn sie solchen Tätern das Handwerk legen wollen.

Deshalb setze ich mich für die Einführung von Online-Durchsuchungen ein. Ich bin der festen Überzeugung, dass die Sicherheitsbehörden die Möglichkeit haben müssen, auch zukünftig ihren Aufgaben schnell und sachgerecht nachzugehen. Das bedeutet, dass die Sicherheitsbehörden dort ermitteln können müssen, wo relevante Informationen liegen und ausgetauscht werden. Denn wir müssen Kriminellen auf Augenhöhe begegnen, um Gefahren von unserem Gemeinwesen in unser aller Interesse so gut wie möglich abzuwenden.

Das ist nicht das Thema, um das es heute und morgen auf diesem Kongress geht. Dennoch möchte ich es ansprechen, weil ich weiß, dass es Sie beschäftigt. Mir ist bewusst, dass der zwingend notwendige staatliche Zugriff auf IT-Systeme Diskussionen über die Auswirkungen auf die IT-Sicherheit ausgelöst hat. Die dabei gestellten Fragen sind leider durchaus berechtigt.

So muss beispielsweise größte Sorgfalt darauf verwendet werden, dass die für Online-Durchsuchungen einzusetzende Software keine Sicherheitslücken produziert oder durch Dritte verwendet werden kann. Diese und weitere Sicherheitsfragen gilt es mit den Bedürfnissen der Sicherheitsbehörden in Einklang zu bringen.

Ich werde bei der Umsetzung der nötigen rechtlichen Regelungen auf diesen Ausgleich achten. So wie ich das Bundeskriminalamt und das Bundesamt für Verfassungsschutz mit den notwendigen Befugnissen für ihre Arbeit ausstatten muss, so werde ich auch das Bundesamt für Sicherheit in der Informationstechnik bei seiner Arbeit zur Sicherung der IT unterstützen. Beides sind grundlegende staatliche Aufgaben. Und beide Bereiche werden wir im Übrigen sorgfältig voneinander getrennt halten.

Heute wird unsere Sicherheit immer stärker von nichtstaatlichen Akteuren bedroht. Hierunter fassen wir den internationalen islamistischen Terrorismus, die organisierte Kriminalität. Und auch im Bereich der Informationssicherheit haben asymmetrische Bedrohungen massiv zugenommen. Es geht zwar auch heute noch darum, die Spionage fremder staatlicher Nachrichtendienste abzuwehren. Aber wir müssen darüber hinaus eine Flut von Angriffen nichtstaatlicher Akteure in den Griff bekommen, die aus den unterschiedlichsten Motiven heraus handeln.

Folgen eines solchen Angriffs können von isolierten Ausfällen von Kommunikation und Produktion bis zum Stillstand des gesamten gesellschaftlichen Lebens reichen. Diese veränderte Bedrohungslage macht es erforderlich, dass wir die Informations- und Kommunikationstechnologien neu bewerten: Sie sind heute Voraussetzung für das Funktionieren des Gemeinwesens, und sie stellen ein Bindeglied verschiedener Infrastrukturen untereinander dar.

Wir haben es mit unterschiedlichen Problemen zu tun: IT-Strukturen, die unabhängig voneinander aufgebaut und weiter entwickelt wurden, werden miteinander vernetzt. Die Folge ist eine heterogene IT-Landschaft. Diese birgt die Gefahr, dass Schwachstellen an einer Stelle es ermöglichen, in die IT-

Systeme einer Vielzahl von Behörden einzudringen. Dieser Gefahr können wir am ehesten begegnen, indem wir zentral auf Bundesebene – beispielsweise durch das Bundesamt für die Sicherheit in der Informationstechnik – einheitliche und strenge Sicherheitsstandards festlegen.

Mit neuen technischen Entwicklungen entstehen neue Geschäftsmodelle und verändern sich Geschäfts- und Verwaltungsabläufe. Immer häufiger werden IT-Dienstleistungen in öffentlichen Verwaltungen und in der Wirtschaft zentralisiert und ausgelagert, wobei die Auftraggeber bei der Beurteilung der Fachkenntnis und Vertrauenswürdigkeit eines Dienstleisters bisher ziemlich auf sich allein gestellt sind. Die Beauftragung externer Dienstleister birgt aber die Gefahr, sich versteckte Spionageprogramme einzufangen.

Die Gefahr der Industrie- und Wirtschaftsspionage, die sich immer stärker der modernen Technologien bedient, darf nicht unterschätzt werden. Der Bericht des BSI zur Lage der IT-Sicherheit in Deutschland warnt eindrucksvoll vor den Risiken, die der sorglose Austausch von Informationen über das Internet birgt. Hierbei werden immer wieder auf vielfältige Weise Know-how, Informationen und neue Erkenntnisse abgeschöpft.

Diesen neuen Herausforderungen muss auch das IT-Sicherheitsrecht Rechnung tragen. Das BSI-Errichtungsgesetz wurde 1990 beschlossen und trat 1991 in Kraft. Damals hatte ich schon einmal das Amt des Bundesinnenministers inne und das Gesetz selbst unterzeichnet. Seither ist das Gesetz im Wesentlichen unverändert geblieben.

Nach dem BSI-Errichtungsgesetz ist der Zweck des BSI die Förderung der Sicherheit in der Informationstechnik. Das BSI hat heute die Aufgabe zu beraten, zu forschen, zu informieren und Systeme zu gestalten. Es ist verantwortlich für die Untersuchung von Sicherheitsrisiken bei der Anwendung von Informationstechnik und für die Entwicklung von Sicherheitsvorkehrungen. Es informiert über Risiken und Gefahren beim Einsatz der IT und versucht, Gegenmaßnahmen dafür zu finden.

Das BSI prüft und bewertet die Sicherheit von IT-Systemen ebenso wie deren Entwicklung in Zusammenarbeit mit der Industrie. Auch bei sicherheitstechnisch ausgereiften Informations- und Telekommunikationssystemen können Schäden durch unzureichende Administration und Anwendung entstehen. Um dieses Risiko zu minimieren, wendet sich das BSI an verschiedene Zielgruppen: Es berät Hersteller, Vertreiber und Anwender von Informationstechnik. Darüber hinaus analysiert es Entwicklungen und Trends in der Informationstechnik.

Inzwischen arbeiten über 450 Experten im BSI – mit dem Ziel, die IT-Sicherheit in Deutschland zu erhöhen. Damit verfügt Deutschland über eine europaweit einmalige Institution.

Angesichts der rasanten Entwicklung in der Informationstechnologie müssen wir prüfen, ob das BSI zusätzliche Aufgaben übernehmen sollte oder bereits existierende Aufgaben angepasst werden müssen. In jedem Fall möchte ich das BSI als präventive Sicherheitsbehörde weiter stärken.

Schon heute ist eine der wesentlichen Aufgaben des BSI die Vergabe von Sicherheitszertifikaten. Hier sind neben dem IT-Grundschutzzertifikat insbesondere die national wie international hoch anerkannte Zertifizierung nach Common Criteria zu nennen. Zur Erhöhung der allgemeinen IT-Sicherheit ist aber ein viel breiterer Einsatz von vertrauenswürdigen IT-Produkten, möglichst zertifizierten Produkten, sinnvoll**.** Und dazu müssen wir prüfen, mit welchen gesetzgeberischen Anreizen der Einsatz zertifizierter Produkte erhöht werden kann.

Ein anderes wichtiges Feld ist die Akkreditierung von IT-Sicherheitsdienstleistern durch das BSI. Nur geeignete Schutzmaßnahmen können sicherstellen, dass Unbefugte keinen Zugriff auf vertrauliche, sensible und gegebenenfalls personenbezogene Daten bekommen. Deswegen prüft das BSI, private IT-Dienstleister zu akkreditieren, deren Kompetenz und Zuverlässigkeit dann durch das BSI zu begutachten wären. Dies erscheint sinnvoll: In der Regel liegt die Entscheidung, welche Produkte eingesetzt und

wie diese konfiguriert werden, bei dem beauftragten IT-Dienstleister. Unternehmen und zunehmend auch Behörden kaufen Komplettlösungen, die bis zur vollständigen Auslagerung der IT aus dem Unternehmen bzw. der Behörde reichen. Die Prüfung von Kompetenz und Vertrauenswürdigkeit des Dienstleisters könnte hier einen erheblichen Qualitätsschub bewirken und die Gefahr reduzieren, sich verdeckte Spionageprogramme einzufangen.

Auch gegenüber der Bundesverwaltung muss die Rolle des BSI angepasst werden. Die starke IT-Vernetzung der Bundesverwaltung bietet enormes Einsparpotential, ist aber auch angreifbar. Zur Verbesserung der Sicherheit der Netze muss das BSI bei Verdacht auf IT-Vorfälle in der Bundesverwaltung gezielt handeln können. Die Unterstützungsfunktion für andere Behörden ist zwar im derzeitigen Gesetzestext als Aufgabe enthalten, aber sie scheint mir nicht ausführlich genug ausgestaltet zu sein.

Eine Klarstellung im Gesetz ist auch bezüglich der Beratung der Öffentlichkeit durch das BSI zu prüfen. Mit dem Internetangebot www.bsi-fuer-buerger.de und dem integrierten Bürger-CERT nimmt das BSI schon entsprechende Aufgaben wahr. Um eine IT-Sicherheitskultur bei allen IT-Nutzern zu etablieren, müssen diese Angebote ständig erweitert und der aktuellen Situation angepasst werden.

Denn Untersuchungen zeigen, dass private Endanwender immer stärker in den Fokus von kriminellen Hackern geraten. Ich habe das Phänomen Phishing schon erwähnt. Zwischen Januar 2004 und Mai 2006 hat sich die Zahl der gemeldeten Phishing-Fälle verhundertfacht.

Es kommt darauf an, das Vertrauen der Nutzer in die Informations- und Kommunkationstechnik zu erhalten, damit im eCommerce, eHealth und eGovernment das Innovationspotenzial auch ausgeschöpft werden kann. Dabei entwickelt sich die IT-Sicherheit immer mehr zu der entscheidenden Schlüsselfrage einer zukunftsorientierten Sicherheitspolitik. Jeder Nutzer trägt Verantwortung. Wir brauchen eine IT-Sicherheitskultur, in der alle verantwortlich handeln.

Und damit das BSI weiterhin seine Aufgaben verantwortungsbewusst, kompetent und den aktuellen Bedrohungen angemessen wahrnehmen kann, muss das IT-Sicherheitsrecht der veränderten Lage angepasst werden. Das BSI muss künftig als die einzige staatliche IT-Sicherheitsbehörde IT-Sicherheit nach innen wie nach außen gewährleisten können.

Neue Strategien und Produkte können nur dann erfolgreich und wirklich innovativ sein, wenn man regelmäßig untereinander Erfahrungen austauscht und wenn man bereit ist, voneinander zu lernen. Ich freue mich daher sehr über Ihr zahlreiches Erscheinen und über Ihr großes Interesse an diesem Fachkongress des BSI. Mit Blick auf das anspruchsvolle und sehr vielfältige Programm der kommenden Tage wünsche ich Ihnen allen neue und wertvolle Erkenntnisse – und vor allem eine Vernetzung diese Erkenntnisse.