Rede des Herrn Willi Berchtold anlässlich
Deutscher IT-Sicherheitskongress des BSI am 13.05.03 in Bonn-Bad Godesberg:
„Neue Technologien für einen modernen Staat“

Es gilt das gesprochene Wort.

Meine sehr geehrten Damen und Herren,

ich freue mich, dass ich heute zu Ihnen sprechen darf. Diesen Umstand habe ich in erster Linie meiner Funktion als Vizepräsident des BITKOM zu verdanken.

BITKOM ist der führende Branchenverband der Informationswirtschaft, der Telekommunikation und der neuen Medien in Deutschland. Hinsichtlich unserer Größe sind wir in Europa vergleichsweise einmalig. BITKOM vertritt 1.300 Unternehmen, davon gut 700 als Direktmitglieder, mit cirka 120 Milliarden Euro Umsatz und über 700.000 Beschäftigten. Hierzu zählen Produzenten von Endgeräten und Infrastruktursystemen sowie Anbieter von Software, Dienstleistungen, neuen Medien und Content.

Mein Thema ist: „Neue Technologien für einen modernen Staat“. Ein weites Themenfeld, das ich unter dem primären Aspekt „Sicherheit“ abhandeln möchte.

Aber auch dann bleibt das Feld noch sehr groß. Zum einen, weil unser Staat ja als Summe unseres Gemeinwesens alle privaten, wirtschaftlichen, gesellschaftlichen und politischen Aktivitäten umfasst. Zum anderen, da der Begriff Sicherheit vielfältige Ausprägungen und Aspekte unserer hoch entwickelten Gesellschaft tangiert.

Ein chinesisches Sprichwort sagt: „Die am sichersten verschlossene Tür ist die, die offen gelassen werden kann“.

Leider können wir in unserer heutigen Welt nicht alle Türen beruhigt offen lassen, sondern wir müssen Vorkehrungen treffen und Möglichkeiten schaffen, schutzwürdige Informationen zu sichern.

Denn funktionierende und sichere Prozesse sind Grundlage für alle Geschäftstätigkeiten. Das gleiche gilt für den Staat. Auch der kann nur funktionieren, wenn die Prozesse zuverlässig und sicher sind.

Das war eigentlich schon immer so – nicht erst in Zeiten der Informationsgesellschaft. Aber noch nie haben wir uns so sehr auf die Funktionsfähigkeit der Informations-Infrastruktur verlassen wie heute.

In allen Bereichen unseres Gemeinwesens wie z.B. Verwaltung, Gesundheit, Kultur, Geisteswissenschaft oder Forschung.

Das Internet spielt dabei eine ganz entscheidende Rolle!

Heute und noch viel mehr in der Zukunft!

Die Zahl der weltweiten Internet-Nutzer stieg um gut 100 Millionen im vergangenen Jahr. Inzwischen nutzen weltweit mehr als 600 Millionen Menschen das Web.

54 Millionen Internet-Zugänge laufen bereits über Breitband-Anschlüsse.

Und, dieses Wachstumstempo wird sich im Jahr 2003 nicht verlangsamen, sondern auf hohem Niveau fortsetzen.

Das Internet hat sich durchgesetzt, völlig gegenläufig zum neuen Markt, mit dem es irrtümlicherweise oft als Synonym verbunden wurde.

Auch in Deutschland ist Wachstum zu verzeichnen.

Im Jahr 2002 wurden bei uns zusätzlich 1,5 Millionen PCs installiert. Insgesamt sind 29 Millionen Geräte im Einsatz.

36 Millionen Deutsche nutzten im Jahr 2002 das Internet.

5 Millionen Deutsche sind im vergangen Jahr erstmals online gegangen.

Jeder zweite Haushalt ist heute mit einem Rechner ausgestattet.

In diesem Jahr wird in der Internet-Nutzung ein wichtiger Meilenstein erreicht: Jeder zweite Deutsche wird regelmäßig im Internet unterwegs sein.

Und bis 2005 sollen jährlich weitere 4 bis 5 Millionen hinzu kommen. Die deutsche Internetgemeinde wird bis dahin auf ca. 50 Millionen Mitglieder anwachsen.

Relativ gesehen liegen wir damit zwar im internationalen Mittelfeld. In absoluten Zahlen aber stellt Deutschland nach den USA und nur knapp hinter Japan weltweit den drittgrößten Internetmarkt.

Und dies alles ohne Sicherheit?

Natürlich nicht. Wir müssen lernen, der Sicherheit in diesem veränderten Umfeld eine neue Bedeutung zu geben.

Meine Damen und Herren,

die neue digitale Welt ruht auf drei Säulen:

1. Technik, also Servern, Netzen und Endgeräten,
2. Inhalten, also neuen, digitalen Angeboten und
3. Sicherheitslösungen und Rechtemanagement-Systemen.

In allen drei Bereichen werden zurzeit Durchbrüche erzielt. Auf die Verbreitung der Netze und Endgeräte bin ich schon kurz eingegangen.

Aber die digitale Welt lebt nicht nur von hochleistungsfähigen Netzen und Endgeräten.

Sie bezieht ihre Attraktivität vor allem aus neuen, digitalen Angeboten. Auch in dieser Beziehung wurden zuletzt große Schritte nach vorn gemacht.

Der Kostenlos-Kultur des Internet wird eine Kultur kostenpflichtiger Premium-Inhalte zur Seite gestellt. Zeitschriften- und Musikverlage haben in den Jahren 2001 und 2002 das Internet als ergänzenden Vertriebsweg für ihre Produkte entdeckt.

Filmstudios, Rundfunk- und Fernsehsender sowie Buchverlage ziehen nach.

Sicherheit ist neben Technik und Inhalten das dritte erfolgskritische Element der digitalen Welt.

Unternehmen, öffentliche Verwaltung, Wissenschaftler, Künstler, Privatpersonen und nicht zuletzt Sie als Bürger werden das Internet nur dann in vollem Umfang nutzen, wenn sie darüber sicher und vertraulich Informationen austauschen können.

Wenn sie rechtsverbindlich Verträge abschließen können.

Ihre Geschäftspartner und Kunden müssen also eindeutig identifizierbar sein. Verbraucher müssen wissen, dass ihre Privatsphäre im Internet geschützt ist.

In den kommenden Jahren werden die Visionen der 90er Wirklichkeit:

- Video-on-demand,
- riesige und dennoch wohl geordnete Internet-Bibliotheken,
- abrufbare Musik- und Filmarchive,
- elektronische Marktplätze für alles und jeden,
- Online-Services von Bund, Ländern und Gemeinden,
- Anwendungen in Privathaushalten,
- durchgängig digitalisierte Wertschöpfungsketten von Unternehmen, Tele-Medizin, Tele-Arbeit und Tele-Learning.

Damit durchdringen neue Informations- und Kommunikationstechniken zunehmend alle Lebensbereiche. Es entstehen nicht nur für den Einzelnen, sondern auch für Staat, Wirtschaft und Gesellschaft völlig neuartige Situationen.

Sichtbar übrigens aktuell auch durch den Irak-Krieg.

Diese weltpolitische Aktion führte, laut erstem Quartalsbericht 2003 des „Internet Security System“ (ISS), zu einem Anstieg der Zahl bestätigter Attacken und außergewöhnlicher Vorkommnisse im Internet.

Im vierten Quartal des Vorjahres stiegen demnach die Attacken um 84 Prozent an. Nicht mehr die Geschäftsideen und Produkte sind das eigentliche Herzstück der Wirtschaft, sondern vor allem die Technologien, mit denen sie ermöglicht und verbreitet werden.

Die informationstechnologischen Schnittstellen sind ein begehrtes Angriffsziel geworden. Auch „europemedia.net“ berichtet, dass mit Beginn des Irak-Krieges die Hacker-Angriffe auf Webseiten zugenommen haben, darunter sowohl „Denial of Service“ (DNS) als auch „Defacement“-Angriffe.

Dabei standen nicht nur Regierungsseiten im Fokus der Angreifer, auch eine Vielzahl von Unternehmensseiten wurde attackiert.

Herkömmliche Unterscheidungen, wie die zwischen Krieg und Nichtkrieg, zwischen öffentlichen und privaten Interessen, zwischen kriegerischen und kriminellen Handlungen oder politischen und geographischen Grenzen verschwimmen im Cyberwar**.**

Insbesondere ist es im Informations- und Kommunikationsbereich kaum mehr möglich, zwischen innerstaatlichen und ausländischen Bedrohungspotenzialen oder zwischen innerer und äußerer Sicherheit eines Staates oder eines Unternehmens zu unterscheiden.

Risiken bei Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit in allen Infrastrukturbranchen sind zahlreich vorhanden: Sie beginnen mit dem allseits bekannten Einbringen von Viren, Trojanischen Pferden, logischen Bomben oder Netzwürmern in IT-Systemen.

Und die werden von unzureichend gesicherten Fernwartungszugängen unterstützt und setzen sich in der Manipulation, Schädigung und Zerstörung von Betriebssystemen oder Applikationssoftware fort.

Bitte vergessen wir nicht: Der Schaden kann sowohl durch Innen- als auch durch Außentäter erfolgen.

Obwohl bereits heute die Hälfte der Firmen in Deutschland schon einmal Opfer eines Angriffs durch Computerviren geworden ist, werden zu wenig unternehmensweite Sicherheitsvorkehrungen eingeführt.

Bislang verfügt lediglich ein Drittel aller Unternehmen über ein systematisches Regelwerk für die IT-Sicherheit.

Eine sträfliche Vernachlässigung - zumal der Grad der Vernetzung unseres Wirtschaftssystems mit der Weiterentwicklung neuer Technologien noch wachsen wird.

Insbesondere kleine und mittelständische Unternehmen hinken am meisten hinter her und stellen ein hohes Risiko dar. Sie sind die Achillesferse eines hoch vernetzten Wirtschaftssystems. Denn das Netz kann nur so sicher sein, wie sein schwächstes Glied.

Den zuständigen Managern muss bewusst sein, dass IT-Sicherheit kein notwendiges Übel, sondern eine sinnvolle und notwendige Maßnahme in der Unternehmensstrategie ist.

Meine Damen und Herren,

in einem modernen Staat nutzen Wirtschaft, Behörden und Bürger gleichermaßen die Vorteile der Informations- und Kommunikationstechniken.

Dementsprechend ist der Schutz der IT-Systeme und Netze vor unbefugtem Zugriff, Missbrauch und Schädigung sowie neuartigen Bedrohungen existenziell geworden.

Ohne sichere IT-Infrastruktur können heute grundlegende Funktionsabläufe gar nicht mehr gewährleistet werden.

Die besten Beispiele sind der Luftverkehr oder die Energieversorgung.

Neue Technologien bieten Chancen und Risiken für die Gesellschaft, die Wirtschaft und für jeden Einzelnen. Es wäre jedoch falsch, die Risiken in den Vordergrund zu stellen. Vielmehr müssen wir die Rahmenbedingungen beachten und umsichtig gestalten:

Fakt ist: dass aufgrund seiner gewollt offenen Architektur ein Computer nach heutigem Stand keine Basis für ein wirklich vertrauenswürdiges System bietet. Daher wurde 1999 die „Trusted Computing Platform Alliance“ – kurz TCPA – gegründet. Ihr Ziel ist, gemeinsame Standards für Sicherheitshardware zu definieren.

Bis heute sind der Initiative weltweit etwa 200 Firmen beigetreten.

Eine andere – Ihnen wohl vertraute Technologie – ist die elektronische Unterschrift. Das Verfahren brauche ich in diesem Umfeld nicht mehr erläutern. Mit dem Signaturbündnis im April ist ein Grundstein für die deutschlandweite Einführung von Chipkarten mit elektronischen Signaturen gelegt worden.

Eine Bürgerkarte oder intelligente Gesundheitskarte sind denkbar geworden.

Eine Bürgerkarte wäre auch die ideale Plattform, die elektronische Signatur zu integrieren. Wenn die digitale Unterschrift flächendeckend eingeführt würde, könnte sie effizient die E-Government-Bestrebungen der Bundesregierung unterstützen.

Auch Länder und Kommunen erhielten dadurch ihrerseits einen höheren Anreiz, E-Government-Projekte zügiger anzugehen und umzusetzen.

Ein großer Teil der Investitionen für eine Bürgerkarte ließe sich so durch das vorhandene Sparpotenzial im E-Government kompensieren.

Was bringt der digitale Ausweis noch?

Mit ihm würde sich die Innere Sicherheit erhöhen.

Personen können schnell und sicher verifiziert werden, die Verarbeitungsgeschwindigkeit ist hoch, und auch die Möglichkeit der „Offline-Verifikation“ und die dezentrale Speicherung persönlicher Daten sprechen für eine solche Lösung.

Eine chip-basierte Lösung bedeutet einen Technologiesprung in der Sicherheit, den kein anderes Verfahren bieten kann.

Darüber hinaus bietet ein digitaler Ausweis zusammen mit biometrischen Merkmalen auch die Möglichkeit, hochsensible Bereiche wie z.B. Kernkraftwerke abzusichern.

Wir haben übrigens bei G&D unseren Zugang zum Rechenzentrum durch Chipkarten mit biometrischen Merkmalen - Fingerabdruck und Iriserkennung - abgesichert.

Neue Möglichkeiten bietet auch die Gesundheits- oder Patientenkarte. Bislang wurden zahlreiche regional, sektoral und technologisch begrenzte IT-Lösungen im Gesundheitswesen implementiert. Das ist ineffektiv, kostet Zeit und Geld.

Sinnvoll hingegen ist ein von vornherein flächendeckend angelegtes, umfassendes Modellprojekt, wie es nun durchgeführt werden soll.

Die Bundesregierung hat die Absicht, die Gesundheitskarte mit einer umfassenden Telematik-Architektur bis 2006 einzuführen und hierzu termingerecht alle notwendigen Richtlinien vorzugeben.

Diese Einführung kann jedoch nur erfolgreich sein, wenn sie zugleich einen verbindlichen Informations- und Kommunikationstandard beinhaltet und sicherstellt, dass alle Beteiligten die einzelnen Bestandteile der elektronischen Kommunikation beachten.

Beide Formen der Verbindlichkeit müssen durch den Gesetzgeber hergestellt werden.

Dabei ist es unabdingbar, dass die Risiken einer solchen Karte, wie beispielsweise das Ausspähen der Gesundheitsdaten, schon bei der Sicherheitsarchitektur minimiert werden.

Web-Identitäten sind ein weiteres Thema

Eine Internet- oder Web-Identität für Internet-Benutzer kann vergleichbar mit einem Pass sein, der es einem Bürger ermöglicht, sich eindeutig zu identifizieren.

Je nach adressiertem Service ist die Web-Identität wichtiger Bestandteil von Servicemodellen und Geschäftsvorfällen, wie zum Beispiel bei der Kontoeröffnung oder bei E-Commerce und E-Government. Sie ist auch optionaler Bestandteil von Diensten, wie E-Mail, Spielen oder Chats.

Die Sicherheitsanforderungen für die Bereitstellung einer eindeutigen Identität spielen hierbei eine große Rolle.

Meine Damen und Herren,

Deutschland war eines der ersten Länder der Welt, das die elektronische Unterschrift der eigenhändigen Unterschrift gleichgestellt hat. Damit waren wir Vorreiter auf juristischer Ebene.

Aber leider nicht in der Praxis. Noch sind Online-Geschäfte und Online-Behördengänge mit elektronischer Signatur die Ausnahme, nicht die Regel.

Entscheidend für die Akzeptanz von Signaturen ist neben dem bereits angesprochenen Vertrauen die vielseitige Verwendbarkeit von Chipkarten. Niemand kauft eine spezielle Chipkarte, um sich damit komfortabel umzumelden, wenn er alle paar Jahre mal umzieht. Das hat auch die Bundesregierung erkannt.

Deswegen ist das Signaturbündnis eine wichtige und richtige Initiative.

Der Bürger kann mit einer Chipkarte seiner Wahl eine Vielzahl von Anwendungen nutzen.

Und zwar Anwendungen aus dem öffentlichen Bereich wie aus dem privatwirtschaftlichen Bereich.

Zahlreiche Beispiele sind hier denkbar: Beispielsweise kann ich mit der Bankkarte gleichzeitig auch die Steuererklärung signieren und elektronisch übermitteln.

Oder einfach nur E-Mails signieren und verschlüsseln. Dieser Mehrwert - die Kombination von Anwendungen des öffentlichen und des privaten Sektors - machen das Signaturbündnis für die Bürger, den Staat und die Wirtschaft interessant.

Aber auch andere Einsatzmöglichkeiten der elektronischen Unterschrift sind nur als integrierte Lösung möglich. Beispielsweise das Verfahren der Massenrechnungsstellung.

Die Rechtslage ist derzeit so, dass Rechnungen, die in elektronischer Form versandt worden sind, mit einer qualifizierten elektronischen Signatur versehen werden müssen, um steuerlich anerkannt zu werden.

Nach meinem Kenntnisstand wird die elektronische Signatur jedoch im Rechnungsverkehr so gut wie gar nicht genutzt. Die Unternehmen scheuen den hohen technischen und organisatorischen Aufwand, der mit der Einrichtung von Signaturstellen für die qualifizierte elektronische Signatur verbunden ist.

Hier sind nun die Anbieter von ERP Systemen gefordert die eine elektronische Unterschrift als integrierte Lösung mit anbieten müssen.

Ein weiteres Themenfeld ist Diebstahl von geistigem Eigentum.

Dadurch entstehen schwere wirtschaftliche Schäden für die Rechteinhaber quer durch sämtliche Arten urheberrechtlich geschützter Werke.

Laut der Software-Pirateriestatistik der „Business Software Alliance“, einer weltweit operierenden Organisation von Software Herstellern zur Förderung einer sicheren und gesetzesmäßigen Online-Welt, entstanden allein in Westeuropa in 2002 rund 3 Milliarden Euro Umsatzverluste durch Software-Raubkopien.

Der Anteil illegaler Kopien bei gewerblich eingesetzten Programmen liegt nach dieser Statistik weltweit bei 40 Prozent.

Eine von IDC und der Business Software Alliance im April diesen Jahres veröffentlichte Studie zu den gesamtwirtschaftlichen Folgen der Softwarepiraterie kommt zu dem Ergebnis, dass durch eine zehnprozentige Senkung der Piraterierate von derzeit 34 Prozent auf 24 Prozent bis zum Jahr 2006 allein in Deutschland 40.000 zusätzliche Arbeitsplätze geschaffen werden könnten.

Die Musikindustrie vermeldet ebenfalls hohe Verluste durch Raubkopien, speziell durch illegal gebrannte CDs aus dem Internet.

In ihrem Piraterie-Bericht 2002 bezifferte die International Federation of the Phonographic Industry den Schaden, der im Jahr 2001 weltweit durch Raubkopien im Musikbereich entstand, mit 3,4 Milliarden US-Dollar.

Spätestens der Napster-Fall in der Audio-Industrie – Napster war die bedeutendste Tauschbörse für kostenlose Musik im Internet – hat gezeigt, dass sich die Industrie hier an die eigene Nase fassen muss.

Die großen Audio-Labels hatten es versäumt, rechtzeitig eigene Geschäftsmodelle für den Absatz ihrer Produkte über das Internet zu schaffen.

Das trieb die Nutzer und die Anbieter von Songs geradezu in die Hände von Napster: Die Nutzer erhielten hierdurch erstmalig die Möglichkeit, aus einer riesigen Vielfalt nur die einzelnen Songs ihrer Wahl zu erhalten, nicht mehr – wie im CD-Bereich – gekoppelt mit unzähligen anderen Titeln.

Und für die vielen kleinen Autoren ergab sich hiermit erstmalig die Möglichkeit, am Verbreitungsmonopol der großen Labels vorbei ihre Titel zum Endkunden zu vertreiben.

Es bleibt zu hoffen, dass die Videoindustrie ihre Lehren aus Napster gezogen hat. Mit der zunehmenden Breitbandigkeit des Internets wird sie die nächste Industrie sein, die sich intensiv mit dem Internet als Vertriebsweg für ihre Produkte – nämlich Filme – befassen muss.

Doch nicht nur der Musik- und Softwarebereich leidet unter Einbußen. Auch die Fernseh- und Medienindustrie hat mit Urheberrechtsverletzungen und daraus folgenden Umsatzverlusten zu kämpfen.

Die kanadische Fernsehindustrie schätzt beispielsweise, dass sie ungefähr 325 Millionen US-Dollar Einnahmen pro Jahr verliert, weil mehr und mehr Zuschauer illegal Satelliten-TV-Signale empfangen.

Leider ist uns das Problem auch in Deutschland nicht fremd. Der größte deutsche PayTV-Anbieter „Premiere“, der seine Programme digital verbreitet, hat mindestens nach Expertenmeinung halb so viele Schwarzseher wie zahlende Kunden.

Sie verfügen über gehackte Smart Cards, mit denen sie Zugang zum Programmangebot erhalten.

Die hieraus resultierenden Umsatzeinbußen sind beträchtlich und haben mit dazu beigetragen, dass die Kirch-Gruppe im letzten Jahr Insolvenz anmelden musste.

Besonders delikat ist, dass in verschiedenen Publikumszeitschriften und auch auf Websites kontinuierlich Anleitungen zur Herstellung und Umgehung der Premiere-Verschlüsselungstechnologie oder Kopierschutzvorrichtungen publiziert und beworben werden.

Hier zumindest schafft das neue Gesetz zum Urheberrecht in der Informationsgesellschaft, welches im April vom Bundestag verabschiedet wurde, Abhilfe.

Zukünftig soll die Veröffentlichung solcher Anleitungen sowie die Werbung für derartige Umgehungstechnologien verboten und strafbar sein.

Glücklicherweise helfen die neuen Technologien auch, neue und sichere Vergütungssysteme für Urheber zu schaffen. Digital Rights Management-Systeme, kurz DRM, kann zusammen mit Verschlüsselung und digitalen Wasserzeichen benutzt werden, um den individuellen Gebrauch von Werken zu regulieren und kontrollieren.

Sie helfen im Kampf gegen Piraterie, indem sie verhindern, dass Werke ohne Zustimmung des Urhebers vervielfältigt werden.

Der Autor kann so entscheiden, zu welchen Bedingungen sein Werk genutzt werden kann und er wird genau die Vergütung dafür bekommen, die er für jeden Gebrauch festlegt.

Der Nutzer seinerseits muss nur für das bezahlen, was er tatsächlich haben möchte. Er muss nicht mehr für die bloße Möglichkeit, Vervielfältigungen anfertigen zu können, bezahlen.

Daher ermöglichen es uns DRM-Technologien ein Vergütungssystem zu schaffen, welches gerechter ist als das System der Pauschalabgaben.

Das Grundprinzip des Urheberrechts ist es, jeden Urheber für jede erlaubte Nutzung seines Werkes zu vergüten. Wo das möglich ist, bleibt kein Raum mehr für Pauschalabgaben.

Vor diesem Hintergrund setzt sich BITKOM nachhaltig dafür ein, das antiquierte System der gerätebezogenen Urheberrechtsabgabe im digitalen Bereich durch ein modernes nutzungsbezogenes System zu ersetzen.

Meine Damen und Herren,

Technik und Geschäftsmodelle alleine reichen nicht aus, das Problem des Urheberrechtsschutz zu lösen. Die europäischen Länder müssen einen rechtlichen Rahmen schaffen, der den erfolgreichen Einsatz technischer Schutzmaßnahmen ermöglicht.

Die EU-Richtlinie zur Harmonisierung einiger Aspekte des Urheberrechts und verwandter Schutzrechte war ein erster Schritt - der Vorschlag für eine Richtlinie über Maßnahmen und Verfahren zum Schutz der Rechte an geistigem Eigentum ein weiterer.

Nun müssen die Einzelstaaten die Umsetzung des EU-Rechts als Chance begreifen und nutzen, um das nationale Urheberrecht an die Bedürfnisse der Informationsgesellschaft anzupassen.

Wie bereits erwähnt, hat Deutschland sichergestellt, dass technische Schutzmaßnahmen nicht umgangen werden dürfen. Das ist ausdrücklich zu begrüßen und ist Grundvoraussetzung für neue Vertriebs- und Vergütungsmodelle.

Ein weiterer Punkt ist in diesem Zusammenhang wichtig:

– das öffentliche Bewusstsein.

Genau genommen sind wir ein Volk von Hackern und Piraten. Das „Rippen“ des Kopierschutzes von CDs und das unerlaubte Herunterladen von Software und Inhalten ist wie ein Volkssport.

Unsere Kinder wissen, dass sie im Supermarkt um die Ecke nichts stehlen dürfen. Aber im Internet fehlt offensichtlich solches Unrechtsbewusstsein.

Hier müssen wir ansetzen und bewusst machen, dass geistiges Eigentum wichtig und notwendig ist, um kulturelle Vielfalt zu garantieren.

Respekt vor den digitalen Gütern muss entwickelt werden und darf nicht hinter dem Respekt vor materiellen Gütern zurückbleiben.

Dies ist nicht allein mit repressiven Maßnahmen bei der Ausführung von Gesetzen möglich, sondern hat mit der Entwicklung einer Werteordnung für die digitale Welt zu tun.

Wir im BITKOM haben uns bereits in der Vergangenheit durch Gespräche mit der Politik, Stellungnahmen zu Gesetzgebungsvorhaben und Vorführungen von DRM-Systemen bemüht, zur Weiterentwicklung des Urheberrechts beizutragen. Auch in Zukunft und gerade im Hinblick auf geplante weitere gesetzgeberische Maßnahmen werden wir diese Bemühungen fortsetzen.

Der BITKOM vereint sowohl Rechteinhaber, also Inhalteanbieter und Softwareproduzenten, als auch Hardware- und Technologieanbieter unter einem Dach.

Deswegen ist der Verband eine ideale Plattform, um sich auszutauschen und gemeinsam Systeme für die digitale Welt zu entwickeln.

Verehrte Gäste,

laut einer OECD-Studie haben Investitionen in den 90er Jahren in die Informations- und Kommunikationstechnik zu einer Steigerung des Wirtschaftswachstums in den weltweit führenden Industrieländern geführt.

Am stärksten war dieser Effekt mit 0,9 Prozent in den USA zu beobachten, aber auch in Australien und Finnland gingen mehr als 0,6 Prozentpunkte des Wirtschaftswachstums auf das Konto der ITK-Investitionen.

In Deutschland lag der Beitrag zum Wirtschaftswachstum mit weniger als 0,4 Prozentpunkten nicht einmal halb so hoch wie in den USA.

Die international unterschiedliche Entwicklung zeigt zweierlei: Die Wachstumspotenziale der modernen Informations- und Kommunikationstechnologien werden in Deutschland noch längst nicht ausgeschöpft. Dies möchte ich Ihnen an zwei Beispielen verdeutlichen.

- 87 Prozent des elektronischen Geschäftsverkehrs spielt sich zwischen Unternehmen ab. Die deutsche Wirtschaft hat hier eine Vorreiterrolle übernommen. 28 Prozent des gesamten E-Commerce in Westeuropa findet in Deutschland statt. Damit ist Deutschland im Internet-Handel stärker vertreten als im traditionellen Geschäftsverkehr.

- Im Jahr 2002 wurden weltweit mehr als 200 Millionen zusätzliche Kommunikationsanschlüsse geschaltet, analoge Festnetzanschlüsse nicht mitgerechnet. Die Zahl der Mobilfunkteilnehmer überschritt erstmals die Marke von einer Milliarde. Aus unserer Sicht besonders erfreulich ist, dass mehr als 70 Prozent auf den in Europa und Deutschland entwickelten GSM-Standard zurückgreifen.

Das World Economic Forum sieht die deutsche Wirtschaft international auf Rang 1, was die Nutzung leistungsfähiger Informations- und Kommunikationssysteme angeht.

Wir sollten und wir müssen diese Basis nutzen!

Diese Chance ergreifen!

Im Mittelpunkt aller Anstrengungen muss nun jedoch der Roll-Out neuer, elektronischer Sicherheitstechnologien in Deutschland stehen.

Sicherheitssysteme gehören zu den wenigen verbliebenen Marktsegmenten, in denen deutsche Unternehmen zu Recht die Technologieführerschaft im Weltmarkt für sich beanspruchen dürfen.

So erfreulich es ist, dass deutsche Unternehmen reihenweise Ausschreibungen in Malaysia, Singapur oder Taiwan und sogar in den USA gewinnen – wir müssen nun auch dafür sorgen, dass der Inlandsmarkt zum Laufen kommt.

Die Sicherheitstechnologie ist ein wichtiger Standort- und Wachstumsfaktor für Deutschland. Deshalb muss in Kooperation zwischen Wirtschaft und Politik alles getan werden, diese Schlüsseltechnologie weiter voranzubringen.

Dafür sind solche Projekte, wie Mcert, die in Public Private Partnership realisiert werden, sehr gut.

Aber wir müssen auch an der Forschungsförderung von Seiten des Staates ansetzen: Statt Basistechnologien mit Millionen zu fördern, sollte der Staat besser ein volkswirtschaftlich strategisches Ziel definieren, das gemeinsam von Wirtschaft und Staat erreicht werden kann. Bestes Beispiel dafür ist das Ziel der Amerikaner gewesen, den ersten Menschen auf dem Mond landen zu lassen, was bekanntlich einen wahren Innovationsboom auslöste.

Unser gemeinschaftliches Ziel könnte lauten:
„Wir wollen das sicherste Internet schaffen“. Das würde private und staatliche Investitionen ergebnisorientiert bündeln und dazu beitragen, dass vielfältige, neue, vermarktungsfähige Technologien und Produkte entstehen. Es würde einen volkswirtschaftlichen Schub auslösen, den Deutschland zur Zeit mehr denn je gebrauchen kann.

Meine Damen und Herren,

lassen Sie mich meinen Vortrag in fünf Thesen zusammenfassen:

These 1: Die Digitalisierung ist für jede Branche, jede Firma, jeden Bürger – einfach jeden – unverzichtbar.

These 2: Neue ITK-Technologien bieten Chancen und Risiken. Die Chancen müssen wir nutzen, die Risiken beherrschen.

These 3: Sicherheit ist integraler Bestandteil von Lösungen und kein Stand Alone-Produkt.

These 4: Sicherheit ist eine relative und dynamische Größe. Neue Technologien erfordern neue Sicherheitslösungen.

These 5: Sicherheit „Made in Germany“ kann Spitze und Hoffnungsträger für den High-Tech-Standort Deutschland sein.

Meine Damen und Herren, Sicherheit erreicht man nicht, indem man Zäune errichtet, Sicherheit gewinnt man, indem man Türen öffnet. Es ist die Aufgabe von uns allen hier, daran mitzuwirken, die richtigen Türen zu öffnen.
Dabei wünsche ich uns allen viel Erfolg und Ihnen einen interessanten und lebendigen Kongress.

Vielen Dank für Ihre Aufmerksamkeit.