

**Rede von
Herrn Dr. Udo Helmbrecht
Präsident des Bundesamtes für Sicherheit in der Informationstechnik**

anlässlich

**der Eröffnung des 8. Deutschen IT-Sicherheitskongresses
am 13. Mai 2003 in Bonn**

(es gilt das gesprochene Wort)

Sehr geehrter Herr Staatssekretär,
meine sehr verehrten Damen und Herren,
liebe Kolleginnen und Kollegen,

ich freue mich sehr, Sie auf dem 8. Deutschen IT-Sicherheitskongress des BSI begrüßen zu können.

Anrede

(Namentliche Begrüßung der Gäste)

Informationstechnik ist für die meisten Menschen in Deutschland längst zur Selbstverständlichkeit geworden. Durch den täglichen Umgang mit IT-Systemen haben wir uns an ihre Funktionsweisen und die ständig erweiterten Möglichkeiten gewöhnt. Im Zuge des Fortschritts verdrängen neue Technologien bereits bestehende Systeme und es treten inkompatible Standards um die Marktführung in Konkurrenz. Angetrieben durch Wettbewerbsdruck und Erfindungsgeist wächst mit der Vielfalt natürlich auch die Komplexität der IT-Landschaft. Heute sind wir schließlich an einem Punkt angelangt, an dem die Informationstechnik von niemanden mehr in allen Details erfasst werden kann.

Für einen Laien vermittelt das Zusammenspiel aus unterschiedlicher Hard- und Software, permanenten Veränderungen und verwirrender Anzahl von Technologien sogar schnell einen chaotischen Eindruck. Hieraus leitet sich auch das Motto "IT-Sicherheit im verteilten Chaos" des diesjährigen Kongresses ab. Damit soll der Fokus auf die erschlagende Vielfalt in der Informationstechnik gesetzt werden, die schließlich auch Experten in besonderer Weise herausfordert.

Das scheinbare Durcheinander lichtet sich zwar bei näherer Betrachtung zu sehr wohl durchdachten und geordneten Teilbereichen, die aber alle wieder auf unterschiedliche Weise miteinander verwoben sind. Obwohl es

für IT-Fachleute nicht notwendig ist, in jedem dieser Teilaspekte ein Experte zu sein, so muss doch ein Grundverständnis des ganzen Systems vorhanden sein. Hierzu gehört natürlich auch die Berücksichtigung aktueller Ereignisse und Abschätzung von Trends um ständig auf dem Laufenden zu sein. Dies erfordert permanentes Lernen und den Austausch von Wissen, gerade auch mit Beteiligten aus angrenzenden und weiter entfernten IT-Bereichen.

Das ist nicht nur wichtig, um in kritischen Situationen schnell und kompetent reagieren zu können. Es ist für die Schaffung und Weiterentwicklung von Sicherheitssystemen eine notwendige Bedingung: Denn eine umfassende und zugleich robuste IT-Sicherheit ist nicht durch isolierte Lösungen zu erreichen.

Vor diesem Hintergrund freue ich mich deshalb ganz besonders darüber, dass ich heute unter Ihnen Vertreter aus den unterschiedlichsten Bereichen der IT begrüßen darf. Sie erwartet in den nächsten Tagen ein umfangreiches und sehr vielfältiges Programm. Die Breite des Kongress-Programms ist mir gerade deshalb so wichtig, weil bei der Diskussion von Fachfragen allzu leicht der übergeordnete Kontext vergessen wird, gerade auch bei IT-Sicherheitsfragen.

Meiner Überzeugung nach steht die IT-Sicherheit anderen - klassischen - Sicherheitsfragen in nichts nach. Zwar ist die physische Fühlbarkeit von Schadensereignissen natürlich eine andere als etwa bei Verkehrsunfällen, aber gerade die gesamtwirtschaftliche Bedeutung der Informationstechnik macht ihren zuverlässigen Schutz so wichtig.

Die möglichen direkten IT-Schäden brauche ich Ihnen an dieser Stelle sicher nicht vor Augen führen. Sie kennen alle die Meldungen verschiedener Angriffe und Sicherheitslücken, wie sie zum Beispiel auch unser CERT-Bund ausgibt. Weil die tatsächlich entstandenen Schäden oft nur schwer zu beziffern sind oder einfach auch nicht bekannt werden, darf die IT-Sicherheit nicht unterschätzt werden.

Noch viel schwieriger, als die Beeinträchtigungen durch den Ausfall oder die Manipulation von IT-Systemen, sind die nicht ausgeschöpften Potenziale zu messen, die uns die Informationstechnik bietet. Wertschöpfungsgewinne, die nicht realisiert werden, weil kein Vertrauen in E-Commerce oder E-Government-Anwendungen besteht, sind verspielte Chancen, deren Ausmaß nur schwer zu beziffern ist.

Anrede,

meine sehr geehrten Damen und Herren,
für ein technologisch und gesellschaftlich führendes Land wie Deutschland stellt die Informationstechnik eine geradezu existenzielle Infrastruktur dar, um deren Schutz wir uns tagtäglich bemühen müssen.

Das BSI nimmt hierbei eine zentrale Stellung in Deutschland ein und arbeitet eng mit internationalen Partnerorganisationen zusammen. Eine erfolgreiche Förderung der IT-Sicherheit setzt aber nicht nur den Austausch von Informationen auf der Verwaltungsebene voraus: Wirtschaft, Wissenschaft und die Bürger müssen bei der Umsetzung natürlich einbezogen werden. Sicherheit lässt sich deshalb nicht verordnen, sondern setzt aktives Handeln voraus.

Das BSI muss sein Handeln nicht zuletzt auch an den Bedürfnissen des Marktes messen lassen. Es kann nicht am IT-Sicherheitsbedarf vorbei entwickeln oder planen. Der konkrete Bedarf „draußen“ ist Basis für die erfolgreiche Dienstleistung und den Erfolg aller Entwicklungen.

Allerdings hat das BSI auch die Aufgabe, die Nachfrage nach IT-Schutzsystemen kritisch zu beobachten und konstruktiv zu fördern. Es darf nicht sein, dass das reale Bedrohungspotenzial in der öffentlichen Wahrnehmung falsch eingeschätzt wird und daraus ein – ich nenne es einmal " falscher Bedarf " - hergeleitet wird. Weder Panikmache noch Untertreibung sind angesagt. Wir müssen durch gezielte Information und

Sensibilisierung möglichen Verunsicherungen vorbeugen und sie auf ein Mindestmaß reduzieren.

Wichtig für eine positive Entwicklung des Marktes ist auch Transparenz über die Leistungsfähigkeit und Zuverlässigkeit der Produkte. Die Anschaffung von IT-Schutz ist eine Vertrauensfrage. Deshalb müssen die verantwortlichen Entscheider und Anwender eine Möglichkeit haben, schnell und einfach die Verlässlichkeit der Produkte und Serviceleistungen einzuschätzen.

Das BSI bietet dazu die Zertifizierung nach internationalen Kriterien an. Damit wird die Sicherheit eines Produkts bestätigt. Für die Hersteller ist dies ein handfester Vorteil und natürlich auch ein wichtiges Verkaufsargument. Derzeit arbeiten wir an einer Erweiterung des Zertifizierungsangebots, um für die verschiedenen Bereiche ein passendes Angebot bereithalten zu können.

Darüber hinaus ermöglicht es zum Beispiel das Grundschutz-Zertifikat die IT-Sicherheitsmaßnahmen, die ein Unternehmen insgesamt durchgeführt hat, auch nach außen glaubhaft zu dokumentieren. Der gewissenhafte und vertrauenswürdigen Umgang mit Informationen wird so bestätigt.

Solche Maßnahmen sind für die Schaffung einer höheren Transparenz für Kunden oder Geschäftspartnern wichtig. Denn insbesondere die Entfaltung von E-Commerce oder E-Government ist vertrauensabhängig.

Zentraler Aspekt ist natürlich die Glaubwürdigkeit dessen, der das Zertifikat herausgibt: Das BSI. Diese Glaubwürdigkeit muss ständig aufs neue unter Beweis gestellt werden. Das ist eine große Herausforderung, wenn Sie nur die Schnelligkeit, die Breite und Tiefe des Gebietes betrachten.

Hier schließt sich der Kreis wieder und ich möchte an dieser Stelle noch einmal das Motto des diesjährigen Kongresses aufgreifen: "IT-Sicherheit im verteilten Chaos": Das BSI muss bei all den zügigen und

vielschichtigen Entwicklungen stets den Überblick bewahren und zuverlässige Informationen anbieten können. Fehlritte gibt es nicht und darf es nicht geben.

Vorschnelle Aussagen, die sich im Nachhinein als falsch erweisen, kann sich das BSI nicht erlauben. Gleichzeitig muss das BSI eine schnelle Einschätzung der Lage bereitstellen. Bei aktuellen Diskussionen, z. B. um TCG - Trusted Computing Group - wird dieser Spagat deutlich.

Ruhe und die zügige Beschaffung von Informationen - das sind die wichtigsten Zutaten für kompetentes und glaubwürdiges Handeln. Die eigens dafür eingesetzte Projektgruppe beim BSI prüft und analysiert die aktuellen Entwicklungen genau. Aussagen auf Grund von Spekulationen oder Vermutungen trifft das BSI nicht. Unser erstes Anliegen ist es, verlässliche Informationen bereitzustellen. Fundierte Informationen erhalten Sie in dieser Tradition natürlich auch in den nächsten drei Tagen auf dem Kongress.

Anrede,
meine sehr geehrten Damen und Herren,
ich wünsche Ihnen eine interessante und angenehme Zeit und bedanke mich für Ihre Aufmerksamkeit. Ich freue mich, nun das Wort weitergeben zu können an Herrn Staatssekretär Dr. Wewer.