Rede von

Herrn Dr. Udo Helmbrecht

Präsident des

Bundesamtes für Sicherheit in der Informationstechnik

auf dem 9. Deutschen IT-Sicherheitskongress

des BSI

am 10. Mai 2005

in Bonn

(Es gilt das gesprochene Wort!)

Sehr geehrter Herr Minister,

meine sehr geehrten Damen und Herren,

liebe Kolleginnen und Kollegen,

willkommen auf dem 9. Deutschen IT-Sicherheitskongress des BSI!

1905, im Annus Mirabilis[1], revolutioniert der bedeutendste deutsche Naturwissenschaftler aller Zeiten, Albert Einstein, in atemberaubendem Tempo die klassischen Vorstellungen der Physik. Mit fünf bahnbrechenden Aufsätzen verändert Einstein unser Verständnis von der Welt.

Und auch 100 Jahre später wird mehr denn je deutlich, welch bedeutsamen Einfluss er auf die Technologie unserer modernen Welt genommen hat. Einsteins Experimente mit einzelnen Quantensystemen haben zu neuen Ideen der Informationsverarbeitung und -übertragung geführt und damit das Tor zu einer neuen Technologie eröffnet. Davon hat weder Einstein noch ein anderer Wissenschaftler geträumt. Wir können nur erahnen, welche neuen Technologien auf uns warten und was wir mit ihrer Hilfe werden leisten können.

Zum Beispiel die Quantenkryptographie: Inzwischen existieren Systeme, mit denen ein Schlüsselaustausch über mehrere Kilometer möglich ist. Einer Gruppe von Physikern ist es im vergangenen Jahr sogar gelungen, eine quantenmechanisch verschlüsselte Banküberweisung vom Wiener Rathaus zu einer Bankfiliale zu schicken.

Meine Damen und Herren,

die naturwissenschaftliche Forschung und die technische Realisierung der Ergebnisse sind treibende Kräfte für die Fortentwicklung unserer Gesellschaft. Neue Technologien bieten ungeahnte Chancen, bergen jedoch Risiken in sich. Daher stellt sich die Frage nach der Verantwortung. Wer übernimmt die Verantwortung für die Entwicklung all der Technologien, die wir tagtäglich nutzen?

---

[1] Wunderjahr

Grundsätzlich ist der Mensch selbst verantwortlich für das, was er tut. Die nahezu vollständige Durchdringung der Gesellschaft mit Informationstechnologie und die damit verbundene Abhängigkeit überfordern heute den Einzelnen. Manche Dinge kann er nicht allein verstehen und bewältigen. Kommt es beispielsweise in vernetzten IT-Infrastrukturen zu Störungen, können diese massive Folgeschäden anrichten. Diese Schäden betreffen dann aber nicht nur den einzelnen Menschen, sondern unter Umständen gleich den ganzen Staat.

IT-Sicherheit ist heute ein integraler Bestandteil der inneren Sicherheit! Die Erwartung an den Staat, hierfür etwas zu tun, erfüllt das Bundesamt für Sicherheit in der Informationstechnik. In der Begründung des Gesetzentwurfs für die Errichtung des BSI hieß es vor ziemlich genau 15 Jahren[2]:

> *„Die Informationstechnik ist eine der Schlüsseltechniken, von denen erhebliche Veränderungen in Gesellschaft und Wirtschaft ausgehen. (...) Mit dem zunehmenden Einsatz der Informationstechnik steigen auch die Gefahren durch unrichtige, unbefugt gesteuerte, fehlende oder rechtsgutgefährdende Informationen. (...) Den bestehenden Gefahren muß – auch zur Wahrung der Akzeptanz der Informationstechnik – angemessen begegnet werden. (...).“*

Konnte man schon damals – zur Gründung des BSI – ahnen, welchen informationstechnischen Herausforderungen wir uns heute stellen? Definitiv nicht. Technologische Entwicklungen sind nur schwer vorhersagbar.

Es gibt zwar Konstanten wie das von Gordon Moore formulierte Gesetz, wonach sich ca. alle 18 Monate die Geschwindigkeit von Computerprozessoren verdoppelt. Dieses Gesetz hat auch nach 40 Jahren nichts von seiner Gültigkeit verloren. Doch das ist wohl eher die Ausnahme.

Zur Gründungszeit des BSI haben wir uns eingehend mit den Themen Kryptographie, Zertifizierung und Computerviren beschäftigt. Das tun wir noch immer. Die Tatsache, dass 14 Jahre später fast jeder Deutsche ein Handy besitzt und die mit einem Betriebsystem ausgestatteten Mobiltelefone immer häufiger Opfer

von Virenangriffen werden, hätte damals aber wohl kaum jemand für möglich gehalten. Hätte man Ihnen zu Beginn der Neunzigerjahre – als sich Computerviren noch vorrangig über Disketten verbreitet haben – gesagt, dass das BSI sich eines Tages mit Handy-Viren beschäftigen würde, hätten Sie wahrscheinlich nur ungläubig die Stirn in Falten gelegt.

Diese Entwicklung zeigt, mit welcher ungeheuren Dynamik Veränderungen heute geschehen – gerade in der Informationstechnik. Um hier Schritt halten zu können, darf das BSI nicht in alten Denkweisen und Strukturen verharren. Die Aufgaben, die sich uns stellen, sie sind von besonderer Qualität und sie erfordern flexibles, schnelles und effizientes Handeln.

Denken Sie nur an die so genannten Zero-Day-Exploits. Schwachstellen sind kaum bekannt, da stehen schon die entsprechenden Programme zu Verfügung, um genau diese Schwachstellen auszunutzen.

Oder denken Sie an den Wurm Sober.O, der in der vergangenen Woche – punktgenau zur Ticketvergabe der FIFA – gefälschte Ticket-E-Mails mit Wurm-Anhang in Umlauf brachte. Seit dem ersten Auftreten von Sober mussten wir übrigens bereits Warnmeldungen zu 15 verschiedenen Varianten von Sober verschicken.

Und noch eine Meldung erreichte mich vor wenigen Tagen: Inzwischen besteht die Möglichkeit in IT-Geräte mit Bluetooth von einer Entfernung von 1,6 km einzudringen. Vor gut zwei Jahren gab es diese Problematik nur bei großen Menschenmassen – auf Flughäfen oder Bahnhöfen beispielsweise. Der Angreifer musste sich seinerzeit mindestens 10 Meter im Umkreis des Opfers befinden. Jetzt überlegen Sie, mit welchen Angriffs-Distanzen wir in 5 Jahren rechnen dürfen, wenn sich diese Entwicklung fortsetzen sollte. Das BSI steht in der Pflicht auf diese Trends zu reagieren. Und genau das tun wir.

---

[2] 27. April 1990

Meine sehr geehrten Damen und Herren,

14 Jahre nach seiner Gründung ist und bleibt das BSI der zentrale IT-Sicherheitsdienstleister des Bundes. Neben dem Bundesamt für Verfassungsschutz, dem Bundesgrenzschutz und dem Bundeskriminalamt bildet das BSI damit die vierte Säule der inneren Sicherheit. „Sichere Informationstechnik für unsere Gesellschaft“ – so haben wir es nicht nur in unser Leitbild geschrieben, sondern so verstehen wir unsere Arbeit. Dabei richten wir uns alle – von der öffentlichen Verwaltung über die Wirtschaft bis hin zum Privatanwender.

Drei Ziele beschreiben die strategische Neupositionierung des BSI und markieren den Weg zu mehr Sicherheit in der Informationstechnik:

1. Prävention: Wir müssen die Informationsinfrastrukturen angemessen schützen.
2. Reaktion: Wir müssen bei IT-Sicherheitsvorfällen wirkungsvoll handeln.
3. Nachhaltigkeit: Wir müssen die deutsche IT-Sicherheitsindustrie national wie international stärken.

Diese strategischen Ziele haben wir immer vor Augen. Wir wollen und müssen sie umsetzen. Denn nur dann sorgen wir auch in Zukunft dafür, dass wir uns kritisch mit den Risiken der IT auseinandersetzen und Ihnen – unseren Kunden – sichere Lösungen anbieten. Um dieses Ziel zu verwirklichen, hat sich das Selbstverständnis des BSI in den vergangenen Jahren gewandelt und wandelt sich stetig weiter. Woran können Sie das konkret erkennen?

Meine Damen und Herren,

das BSI ist für IT-Sicherheit in Deutschland verantwortlich! Wir sind

- operativ für den Bund
- kooperativ für die Wirtschaft
- informativ für den Bürger

tätig.

Das bedeutet konkret: Im Bereich der Verwaltung ist das BSI ist auf dem Weg operativer zu werden und Verantwortung zu übernehmen. Wir erstellen heute mehr

als nur Gutachten und Berichte. Wir machen schlüssige Aussagen und geben konkrete Empfehlungen zu aktuellen Themen ab – ohne Konjunktiv.

Wir orientieren uns an den politischen Zielen und stellen entsprechende Produkte und Dienstleistungen zur Verfügung. In den nächsten Monaten werden wir den von Herrn Minister Schily angesprochenen und von ihm unterstützten „Nationalen Plan zum Schutz der Informationsinfrastrukturen in Deutschland“ weiter auf den Weg bringen.

An dieser Stelle möchte ich Ihnen, Herr Minister Schily, für Ihr Engagement bei den Stellen- und Haushaltsverhandlungen danken. Wir wissen im BSI, dass es angesichts der angespannten Haushaltslage nicht selbstverständlich ist, mehr Personal und zusätzliche Haushaltsmittel zu erhalten. Mit diesen Ressourcen werden wir u. a. auch das notwendige IT-Krisenreaktionszentrum des Bundes im BSI aufbauen.

Zusätzlich werden wir unser Augenmerk in Zukunft noch stärker auf die Wirtschaft legen. In den vergangenen Jahren ist das BSI enge Kooperationen mit Unternehmen der IT-Sicherheitsindustrie eingegangen – ganz im Sinne des Public Private Partnership-Gedankens. Erwähnen möchte ich Sicherheitspartnerschaften mit SIT und secunet. Gemeinsam mit anderen, insbesondere den großen Technologieunternehmen wie Infineon, Philips, G&D, die Bundesdruckerei, Siemens und T-Systems bilden sie die Basis der nationalen IT-Sicherheitsindustrie, welche die Umsetzung einer nationalen IT-Sicherheitspolitik überhaupt erst ermöglichen. Der Erfolg einer nationalen IT-Sicherheitsindustrie hängt nicht zuletzt davon ab, dass ihre Produkte auch im eigenen Land Verwendung finden und im Exportgeschäft als Referenzlösungen mit dem Markenzeichen "IT-Security made in Germany" vermarktet werden können.

Die qualitative Bedeutung dieser Marke leitet sich in hohem Maße aus den technischen Sicherheitsprüfvorschriften des BSI ab: „IT-Security approved in Germany“. Hierbei zertifiziert das BSI IT-Sicherheitsprodukte nach den Common Criteria. Maßgeblich wird unser Anteil bei der Umsetzung der Chipkartenstrategie der Bundesregierung sein, die im März diesen Jahres im Bundeskabinett beschlossen wurde. Mit diesen sicherheitstechnischen Prüfvorschriften, die z.B. bei

Beschaffungsvorhaben innerhalb von Großprojekten Verwendung finden, kommt dem BSI hierbei eine Schlüsselrolle zu: Auf diese Weise werden nationale IT-Sicherheitsstandards im Markt umgesetzt und die Marktposition deutscher Unternehmen im internationalen Wettbewerb gestärkt.

Das Selbstverständnis des BSI schließt natürlich auch den Privatanwender ein. Insgesamt wird das BSI immer stärker in der Öffentlichkeit wahrgenommen und öffnet sich entsprechend. Die meisten IT-Anwender wünschen sich noch immer, das Thema Sicherheit an andere zu delegieren. Doch so leicht ist es leider nicht. Jeder Anwender muss sich selbst um ein Mindestmaß an „sicherer IT-Versorgung“ kümmern. Das BSI bietet den Privatanwendern mit zahlreichen Informationen Hilfe zur Selbsthilfe an.

Und auch unsere internen Prozesse entwickeln wir stetig weiter: Das BSI ist unternehmerischer geworden. Wir haben beispielsweise begonnen, die Balanced Score Card als kennzahlenorientiertes Steuerungsinstrumentarium zu nutzen.

Meine Damen und Herren,

Sie sehen, das BSI verändert sich. Dennoch möchten wir manch alte – liebgewonnene – Tradition pflegen. Dazu zählt mit Sicherheit dieser Kongress.

Ich freue mich, dass Sie den Weg nach Bonn gefunden haben. Sicherlich haben Sie bemerkt, dass wir in diesem Jahr hinter unser Kongressmotto „IT-Sicherheit geht alle an!“ ein Ausrufungszeichen gesetzt haben. Nicht umsonst. Denn inzwischen ist die Informationstechnik bis in unsere Wohnzimmer vorgedrungen. Und es gibt kein Zurück. Deshalb sollten alle Menschen etwas über IT-Sicherheit wissen und entsprechend handeln. IT-Sicherheit muss umsetzbar sein, sie muss „lebbar“ sein. Für alle.

Wie in den vergangenen Jahren setzen wir uns in den kommenden drei Tagen mit ganz unterschiedlichen Sicherheitsfragen auseinander: Es geht – wie immer – um die Technik, aber auch um die gesellschaftliche Bedeutung von IT-Sicherheit. Wir werden IT-Sicherheitsaspekte aus den unterschiedlichsten Bereichen diskutieren.

Dazu zählen technische Entwicklungen wie zum Beispiel biometrische Verfahren, der technische Schutz digitalisierten Eigentums oder die Entwicklungen im Umfeld des Sicherheitsmanagements und auf dem Gebiet der Sicherheitsarchitektur. Auf dem Programm stehen aber auch Konzepte, wie wir ein individuelles Sicherheitsbewusstsein entwickeln können. Die Breite des Kongress-Programms ist deshalb so wichtig, weil bei der Diskussion von Fachfragen allzu leicht der übergeordnete, der gesamtheitliche Kontext vergessen wird. Gerade auch bei IT-Sicherheitsfragen kommt es auf den Zusammenhang an.

Meine Damen und Herren,

noch einmal kurz zurück zu Einstein. Er selbst meinte, es sei das Mysterium des Nichtverstehens, das die Menschen an seinen Theorien anziehe. Er sprach von Dingen, von denen die Menschen schon seit Jahrtausenden träumen:

weit entfernten Sternen und dem ganzen Universum. Er dachte über so schwer verständliche Sachen nach wie vier Dimensionen, die nur als Einheit zu verstehen sind; über Sterne, die nicht dort stehen, wo sie zu stehen scheinen; über Uhren, die bei Lichtgeschwindigkeit langsamer werden; über Energie als Masse.[3] Er sprach und nur wenige konnten ihm folgen.

Das Mysterium des Nichtverstehens – genau das meine Damen und Herren, wollen wir nicht. Wir wollen es nicht, wenn wir über das Thema IT-Sicherheit sprechen. IT-Sicherheit geht alle an! – das diesjährige Kongressmotto spiegelt sich in Alltagstechnologien wieder: dem Reisepass, der Gesundheitskarte und der Mobilkommunikation. Nur, wenn es gelingt, den hohen Anforderungen an die IT-Sicherheit Rechnung zu tragen, werden die Bürgerinnen und Bürger die neuen elektronischen Dienstleistungen akzeptieren. Akzeptanz erreichen wir aber nur über Wissen. Deshalb können wir uns das Nichtwissen und Nichtverstehen nicht leisten.

Unser Ziel muss es also sein, Wissen über die Informationstechnik – und damit einhergehend über das Thema Sicherheit – in verständlicher Form zu vermitteln. Wir wollen die Menschen für neue Technologien begeistern.

---

[3] Quelle: www.einsteinjahr.de

Meine sehr geehrten Damen und Herren,

„Wichtig ist, dass man nicht aufhört, zu fragen“, so begründete Einstein die Begeisterung, mit der er sich seiner Forschung widmete. Er suchte nach Antworten – Antworten, die unsere Welt verändert haben.

Deshalb bitte ich Sie, liebe Kongressteilnehmer, in den kommenden drei Tagen viele Fragen zu stellen und erkläre den 9. Deutschen IT-Sicherheitskongress hiermit für eröffnet!