Das Potential der IT-Sicherheit ist längst nicht erschöpft.

Rede
von Bundesminister
Dr. Wolfgang Schäuble
beim 2. Gipfel zur Sicherheit in der Informationsgesellschaft der Initiative
„Deutschland sicher im Netz“
am 25. April 2006 in Berlin

Wo es um die Sicherheit unserer Informationstechnologie geht, da ist der Bundesminister des Innern gerne. Ohne IT geht es heute nicht, ohne Sicherheit aber auch nicht.

Als die Initiative „Deutschland sicher im Netz“ vor rund einem Jahr mit einem 1. Gipfel startete, wurde schon mit dem Namen ein äußerst ehrgeiziges Ziel formuliert. Gleichwohl haben sich die Partner der immensen Herausforderung, Deutschland sicher ins Netz zu bringen, selbstbewusst und siegesgewiss gestellt. Um die Erfolge messbar zu machen, wurden acht konkrete Vorhaben benannt.

Nach mehr als einjähriger Arbeit gilt es nun, Bilanz zu ziehen. Wir wollen uns fragen, welche Aufgaben erfüllt werden konnten und wo es noch Defizite gibt, – um in der Folge realistisch einordnen zu können, wo Deutschland im Hinblick auf die IT-Sicherheit heute tatsächlich steht. Daraus wiederum ergeben sich die Anforderungen für unsere zukünftigen Anstrengungen auf diesem Gebiet.

Wie Sie wissen, sind es neben den immer wieder beeindruckenden technologischen Innovationen vor allem Sicherheitsfragen, die das Vertrauen, die Akzeptanz und somit die Nutzung des Mediums Internet bestimmen.

Zahllose Studien belegen, dass die Sicherheitslage auf dem Gebiet der Informationstechnologie durchaus prekär ist. Nicht nur die Zahl der Schadprogramme und Hackerangriffe nimmt ständig zu, auch die Techniken der Angreifer werden immer komplexer und raffinierter.

Der Hacker von gestern drang meist im Rahmen seiner Freizeitgestaltung in fremde Systeme ein, um sich zu profilieren. Der Hacker von heute ist oft von kriminellen Motiven geleitet und agiert professionell.

Die Angriffe zielen immer mehr auf finanzielle Gewinne oder dienen Spionagezwecken – die zwar ein wenig

phantastisch klingen, aber keineswegs harmlose Spielereien sind. Um ihr Ziel zu erreichen und nicht die Aufmerksamkeit des Nutzers auf sich zu ziehen, agieren die Angreifer in aller Regel verdeckt.

Im Bericht des Bundesamtes für Sicherheit in der Informationstechnik zur Lage der IT-Sicherheit in Deutschland ist nachzulesen, dass allein im zweiten Halbjahr 2004 mehr als 1.400 neue IT-Schwachstellen entdeckt worden sind. Das bedeutet – verglichen allein mit der ersten Jahreshälfte – einen Anstieg von 13 %. Mehr als 7.300 neue Wurm- und Viren-Varianten wurden im gleichen Zeitraum registriert, was einem Anstieg von sage und schreibe 64 % entspricht.

Ein relativ neues Phänomen, das die IT-Sicherheit gefährdet, ist das so genannte Phishing. Und die Bedrohung durch Phishing nimmt kontinuierlich zu.

Das Sicherheitsunternehmen Symantec hat allein im zweiten Halbjahr des vergangenen Jahres täglich knapp 8 Mio. Phishingversuche verzeichnet. Im gesamten Jahr 2005 hat sich die Anzahl der gemeldeten Phishing-Vorfälle um dramatische 300 % gegenüber dem Vorjahr erhöht. Besonders erschreckend ist, dass Phishing-

Betrüger nach internationalen Schätzungen bei bis zu 5 % der E-Mail-Empfänger erfolgreich sind.

Der finanzielle Schaden, den das Phishing verursacht, ist schwer zu beziffern. Die Schätzungen sind hier sehr unterschiedlich. Sicher aber ist, dass Phishing-Angriffe durch Verunsicherung und Vertrauensverlust unschätzbaren Schaden nach sich ziehen.

Alle diese Zahlen sprechen eine eindeutige, besorgniserregende Sprache. Und sie zeigen uns deutlich, dass in der Zukunft noch eine Menge zu tun ist.

Ein grundlegendes Problem ist, dass die Bürgerinnen und Bürger in unserem Land der IT-Sicherheit einen recht geringen Stellenwert einräumen, während sie zugleich zunehmend von der Informationstechnik abhängig sind.

Eine repräsentative Studie, die das Bundesamt für Sicherheit in der Informationstechnik bei TNS Emnid in Auftrag gegeben hat, ergab, dass jeder Vierte Deutsche ohne Virenschutz im Internet unterwegs ist. Und mehr als die Hälfte der befragten Nutzer hat auch keine Firewall.

Die Studie deckt zudem eine paradoxe Situation auf: Das ***Wissen*** über Angriffsmöglichkeiten durch das Internet ist

in der Bevölkerung durchaus vorhanden. Trotzdem werden vielfach nicht die erforderlichen ***Schutzmaßnahmen*** ergriffen.

Und so trägt jeder einzelne Computernutzer, der ohne Absicherung im Netz agiert, eine Mitverantwortung für Hackerangriffe und die Verbreitung von Schadprogrammen und Spam im Internet. Denn schlecht abgesicherte Computer sind die Ursache dafür, dass Viren so erfolgreich sind.

Auch die Bundesregierung sieht sich in der Pflicht, hier Abhilfe zu schaffen. Der Koalitionsvertrag enthält einen weit reichenden Gestaltungsauftrag zum Schutz der Informationsinfrastrukturen in unserem Land.

Wir sind gerade dabei, unseren Nationalen Plan zum Schutz der Informationsinfrastrukturen umzusetzen. Der Nationale Plan bietet der Öffentlichkeit, der Verwaltung wie auch der Wirtschaft eine umfassende IT-Sicherheitsstrategie.

Der in meinem Haus erarbeitete Nationale Plan verfolgt drei strategische Ziele:

- Wir wollen den Schutz der Informationsinfrastrukturen durch präventive Maßnahmen deutlich erhöhen.
- Wir wollen auf sicherheitsrelevante Vorfälle schnell und effektiv reagieren.
- Und wir wollen einen nachhaltigen Schutz ermöglichen, indem wir die Kompetenz unseres Landes auf dem Gebiet der IT-Sicherheit stärken und selbst international Maßstäbe setzen.

Einen wirkungsvollen Schutz unserer IT-Systeme können wir aber nur durch vereinte Anstrengungen erreichen. Keine gesellschaftliche Gruppe darf sich hier aus der Verantwortung stehlen.

Deshalb bezieht unser Nationaler Plan die Verantwortlichen in Verwaltung und Wirtschaft genauso ein wie die Bürgerinnen und Bürger. Er benennt Ziele und erste Maßnahmen für eine langfristige Sicherung der Informationsinfrastrukturen in unserem Land.

Neben der Verantwortung des Staates und der Verantwortung der Nutzerinnen und Nutzer dürfen wir die Verantwortung der IT-Wirtschaft nicht aus den Augen verlieren.

Denn je sicherer Hard- und Software sind, desto weniger Angriffspunkte bieten sie. Die großen Erfolge von Schadprogrammen verdanken sich zu einem großen Teil Sicherheitslücken, die von Angreifern schamlos ausgenutzt werden. Darum muss die IT-Wirtschaft ihre Anstrengungen vermehrt auf die Entwicklung und Bereitstellung sicherer Produkte richten.

Die Produktsicherheit muss höchste Priorität besitzen. Denn ohne die Übernahme der Verantwortung für die Sicherheit ausgelieferter Produkte laufen die Bemühungen zur Sensibilisierung und Aufklärung der Verbraucher ins Leere.

Die Initiative „Deutschland sicher im Netz“ hat einen wertvollen Beitrag zur Sensibilisierung und Aufklärung geleistet. Sie hat Fragen rund um die IT-Sicherheit in den Fokus des öffentlichen Interesses gerückt. Dafür möchte ich allen Beteiligten herzlich danken.

Sie sind mit konkreten und messbaren Handlungsversprechen angetreten und haben es nicht bei hohlen Phrasen belassen. Darin unterscheiden Sie sich – zu Ihrem Vorteil – von anderen Projekten ähnlicher Art.

Die Palette Ihrer mutigen Versprechen reichte von der Vermittlung von Medienkompetenz an Kinder und Jugendliche bis zu einem IT-Sicherheitspaket für den Mittelstand. Sie hatten von Anbeginn eine Vielfalt der Zielgruppen im Auge.

Sie haben recht beachtliche Erfolge erzielt. Leider blieben einige Ergebnisse aber auch hinter den Erwartungen zurück.

Besonders gut haben mir Ihre Bemühungen um eine höhere Medienkompetenz bei Kindern und Jugendlichen gefallen. Ihr Portal für Kinder, das über die Chancen und Risiken der Neuen Medien informiert, halte ich für beispielhaft. Und auch der für Pädagogen entwickelte Medienkoffer mit Lehrmaterial zu Themen wie Chat, Raubkopien, Handys ist sehr zu begrüßen.

Gleichwohl muss sich die Initiative an ihren eigenen ambitionierten Zielen messen lassen. Und Handlungsversprechen, die Absichten wie „Entwicklung sicherer Software“ oder „Sicherer Online-Handel“ formulieren, wecken natürlich sehr weit gehende Erwartungen.

Um aber die Nutzerinnen und Nutzer vor den im Internet bestehenden Gefahren tatsächlich wirksam zu schützen,

bedarf es Maßnahmen, die umfangreicher sind und die tiefer gehen als die bislang von der Initiative unternommenen Schritte.

Denn Deutschland ist noch lange nicht sicher im Netz. Deswegen müssen wir den eingeschlagenen Weg fortsetzen und noch deutlich weiter gehen. Das Potential der IT-Sicherheit ist längst nicht erschöpft.

Wir müssen in Zukunft neben Sensibilisierung und Aufklärung noch viel stärker auf verbindliche Maßnahmen wie die Übernahme von Produktverantwortung und den Aufbau tragfähiger Sicherheitsstrukturen setzen. Ebenso wichtig erscheint mir eine ausgewogene Beteiligung verschiedenster IT-Anbieter – etwa auch aus dem Open Source-Bereich.

Damit die Nutzerinnen und Nutzer die wunderbaren Möglichkeiten des Internets angstfrei und in großer Zahl frequentieren, müssen wir alle – der Staat, die Hersteller, die Betreiber wie auch die Nutzer selbst – eng und vertrauensvoll kooperieren.

Mit der Initiative „Deutschland sicher im Netz“ haben Sie etwas Wichtiges angestoßen. Nun gilt es, den Schwung

aufzunehmen und das Tempo zu erhöhen. Dabei möchte ich Sie gerne nach Kräften unterstützen.

Die Gewährleistung von Sicherheit in unseren Informationsinfrastrukturen ist eine Aufgabe, die immerwährend ist und folglich nie als abgeschlossen betrachtet werden kann. Sie mögen jetzt vielleicht zu Recht an Sisyphos denken und an seinen rollenden Felsen. Aber lesen Sie Camus. Der wusste: „Wir müssen uns Sisyphos als einen glücklichen Menschen vorstellen."

Und weil die Aufgabe unendlich ist, müssen wir die Zusammenarbeit von Staat und Wirtschaft bei der IT-Sicherheit über einzelne Initiativen und Partnerschaften hinaus kontinuieren und ihr langfristig eine institutionelle Struktur verleihen.

Mein Ziel ist eine breite, herstellerübergreifende und produktneutrale Plattform, die möglichst alle Beteiligten einbezieht.

Auf dieser Basis wird sich das Bundesministerium des Innern und werde ich mich selbst engagieren – und dann auch gegebenenfalls die freundlicherweise von Ihnen an mich herangetragene Schirmherrschaft übernehmen.

Ich danke Ihnen nochmals für Ihr bisheriges Engagement und freue mich auf die weitere Zusammenarbeit im Interesse der IT-Sicherheit unseres Landes.