

Rede von
Herrn Staatssekretär Dr. Wewer
anlässlich der Eröffnung des 8. IT-Sicherheitskongresses
des BSI
am 13. Mai 2003 in Bonn

(Es gilt das gesprochene Wort.)

Anrede,

10 Jahre ist es erst her, dass Marc Andreessen sein Browserprogramm MOSAIC vorstellte, mit dem erstmals HTML-Daten - die Basis des World Wide Web - komfortabel verarbeitet werden konnten. Kaum länger her ist die Erfindung des WWW selbst, dessen erstes Konzept Ende der 80er Jahre durch Tim Berners-Lee am Schweizerischen Kernforschungszentrums CERN entwickelt wurde.

So jung dieses neue Medium auch ist, wegzudenken aus dem täglichen Leben ist es nicht mehr. Längst ist die Informationstechnik integraler Bestandteil des täglichen Lebens geworden. Handy, PC und Internet sind zu alltäglichen Gebrauchsgegenständen geworden und beeinflussen zunehmend unsere Lebensgewohnheiten. Nach einer Studie des Statistischen Bundesamtes waren im Jahr 2002 mit 55 % bereits mehr als die Hälfte der bundesdeutschen Haushalte mit einem PC ausgestattet und 44 % der Haushalte verfügen zwischenzeitlich über einen Internetanschluss.

Durch Informationstechnologie lassen sich auch Geschäftsprozesse neu definieren und strukturieren. Deutschland ist mit einem Umsatz von 47,9 Milliarden US\$ für das Jahr 2002 europaweit führend im Bereich des eCommerce. E-Business wird in der deutschen Industrie als wichtig erachtet. Nach einer aktuellen Studie von Cap Gemini Ernst & Young messen 76 % der Unternehmen eBusiness eine hohe Bedeutung zu. Eine explizite E-Business-Strategie hat fast die Hälfte der deutschen Unternehmen.

Auch die Bundesregierung setzt auf das Potential, das in der IT-gestützten Abwicklung von Geschäftsprozessen steckt. Mit der eGovernment-Initiative BundOnline 2005 werden bis zum Jahr 2005 fast 400 Dienstleistungen des Bundes per Internet verfügbar sein. Damit können Bürgerinnen und Bürger, aber auch Wirtschaftsunternehmen die Dienstleistungen der Bundesverwaltung künftig schneller, einfacher und kostengünstiger nutzen. Darüber hinaus wird sich bei der vollständig funktionieren

den Umsetzung von eGovernment für den Bund ein jährliches Einsparpotential von 400 Millionen € ergeben. Schon jetzt sind 190 BundOnline-Dienstleistungen online verfügbar. Dazu einige Beispiele:

- Über 14.000 meldepflichtige Unternehmen nutzen inzwischen das Angebot des Statistischen Bundesamtes, ihre Meldungen zur innereuropäischen Handelsstatistik über das Internet zu übermitteln. Damit werden die Unternehmen von bürokratischem Aufwand entlastet.
- Mit dem Internet-Service "DEPATISnet" stellt das Deutsche Patent- und Markenamt erstmals sein gesamtes Archiv seit 1977 über das Internet der Öffentlichkeit zur Verfügung. Das sind mehr als 25 Millionen Patentdokumente. Jährlich kommen rund eine Million neue hinzu. Das kostenlose Recherchesystem verzeichnet monatlich rund 50.000 Zugriffe. Als nächster Schritt wird ein elektronisches Patent-Erteilungsverfahren eingeführt, das jeden Schritt von der Anmeldung bis zur Veröffentlichung online ermöglicht.
- Ein anderes Beispiel ist ELSTER. Gemeinsam mit den Ländern arbeitet der Bund mit Nachdruck daran, Steuererklärungen internetfähig zu machen. Bei 35 Millionen Lohnsteuerkarten jährlich wird dies zu einer erheblichen Verbesserung für die Arbeitnehmer, die Arbeitgeber und die Verwaltung führen. Im Rahmen des Projekts ELSTER wurden bisher knapp 1,4 Millionen Einkommenssteuererklärungen und über 15 Millionen Steueranmeldungen elektronisch übermittelt, mit steigender Tendenz.

Die Beispiele zeigen, dass eGovernment und BundOnline der richtige Weg sind zum Abbau von Bürokratie. Voraussetzung für eine breite Nutzung von eGovernment und auch eCommerce ist das Vertrauen der Anwender in die Sicherheit und Zuverlässigkeit der Technik. Je komplexer und undurchschaubarer technische Vorgänge sind, desto schwieriger ist es, beim Anwender Vertrauen in die Sicherheit zu erzeugen.

Vertrauen zu schaffen ist schwer, weil die heutigen IT-Strukturen für den Anwender nur schwer zu durchschauen sind.

Gerade das Internet ist ein gutes Beispiel für ein scheinbar undurchschaubares, selbständig gewachsenes Informationsnetz, dessen Aufbau auf den ersten Blick unstrukturiert und chaotisch wirkt. So ist es praktisch nicht vorhersehbar, welchen Weg Datenpakete innerhalb des Internet einschlagen werden. Je nach Verfügbarkeit und Auslastung von Verbindungsleitungen und Knotenpunkten können Datenpakete aus einer Quelle ganz verschiedene Wege zum Ziel nehmen. Der Weg ist nicht vorgeschrieben und auch nicht vorhersehbar, was zählt ist einzig und allein die vollständige und richtige Übertragung aller Daten von der Quelle zum Ziel.

Gerade diese scheinbare Unordnung in bezug auf den Weg der Daten ist gewollt und wurde von den damaligen Entwicklern des Internet als Mittel zur Erhöhung der Sicherheit und Zuverlässigkeit eingesetzt. Durch diese Netzwerkstruktur ist es möglich, jene Ausfallsicherheit des Internet zu erzielen, für die es einst konzipiert wurde. Durch weitgehende Selbstorganisation aller Teile des Netzwerkes wird Redundanz geschaffen, die das Internet vor einem Ausfall schützt.

An diesem Beispiel wird auch deutlich, dass Chaos und Sicherheit keine Gegensätze sein müssen. In diesem Fall wäre eine hierarchische Ordnung sogar kontraproduktiv, weil damit angreifbare Zentralsysteme geschaffen würden.

Das Motto dieses Kongresses „IT-Sicherheit im verteilten Chaos“ trifft daher auf die Infrastruktur des Internets ganz besonders zu. Wichtig ist in diesem Zusammenhang jedoch, dass die Zuverlässigkeit und Sicherheit transparent gemacht wird. Ohne Transparenz entsteht kein Vertrauen in die Dienstleistungen, die mit Hilfe des Internet realisiert werden.

Anrede,

Vertrauen schaffen ist auch deshalb eine nicht einfache, aber wichtige Aufgabe, weil regelmäßig Berichte über Sicherheitsvorfälle die Öffentlichkeit verunsichern. Die Berichte über neue Computerviren, Denial-of-Service-Attacken und Sicherheitslücken in Betriebssystemen und Internetapplikationen gehen nicht zurück. Im Gegenteil, die aktuellen Fallzahlen zeigen, dass hoher Handlungsbedarf besteht. Zahlen aus verschiedenen Quellen machen das deutlich:

- Nach einem Bericht des Internet Fraud Complaint Center (IFCC) haben sich Meldungen über kriminelle Aktivitäten im Internet, die zu Ermittlungen führten, im Jahr 2002 gegenüber dem Vorjahr verdreifacht.
- Nach einer Erhebung von Mummert Consulting, wurden bereits fast 60 % der Unternehmen in Deutschland Opfer von Hackern oder Saboteuren.
- Der weltweite Schaden durch Computerviren belief sich nach einer Studie von Computer Economics im Jahr 2001 auf 14,96 Milliarden Euro.
- Der Symantec Internet Security Threat Report meldet für das vergangene Jahr eine Steigerung der dokumentierten Schwachstellen in der Software von 81,5 % gegenüber dem Vorjahr.

Diese Zahlen verpflichten uns zum Handeln, die Wirtschaft ebenso wie den Staat.

Anrede,

die Bundesregierung hat im Bereich der Informationstechnik bereits in der Vergangenheit ganz konkrete Maßnahmen zur Steigerung der Sicherheit umgesetzt und wird diese auch weiterhin ausbauen. Ich möchte dies hier exemplarisch an drei Aktionsfeldern veranschaulichen:

1. Wir fördern sichere Technik.
2. Wir sichern die Infrastrukturen.
3. Wir bringen IT-Sicherheit ins öffentliche Bewusstsein

1. Bereich: Wir fördern sichere Technik

Ein Baustein für eine gesunde und sichere IT-Landschaft ist das verträgliche Miteinander unterschiedlicher Software. Genau wie z.B. in der Landwirtschaft Monokulturen von Schädlingen besonders bedroht werden, sind auch Softwaremonokulturen von Computerviren besonders bedroht; ein Zustand der mit der zunehmenden Bedeutung der Informationstechnik für alle Bereiche unseres Lebens nicht akzeptabel ist. Wir haben es uns daher zur Aufgabe gemacht, diesem Trend aktiv entgegen zu wirken, wo wir realistische Möglichkeiten dazu sehen. Das Engagement zur Förderung von offener Software ist dabei ein zentraler Baustein. Durch die verstärkte Nutzung von Open-Source-Produkten kann nicht nur Monokulturen entgegengewirkt werden, sondern auch die Position von kleineren und mittelständischen Unternehmen der Softwarebranche gestärkt werden. Konkret möchte ich hier unser Engagement zur Nutzung von LINUX als alternatives Betriebssystem nennen, dessen Einsatz wir durch den Abschluss entsprechender Rahmenverträge unterstützen. Den Endanwender unterstützen wir ebenfalls in seinen Bemühungen um ein alternatives Betriebssystem. Im Rahmen des LINUX-Tages hat das BSI daher die sog. KNOPPIX-CD in einer einmaligen Aktion an interessierte Bürgerinnen und Bürger verteilt. Diese „LINUX-CD für Jedermann“ ist auf ein äußerst positives Echo gestoßen und hat viele Endanwender von den Qualitäten dieses freien Betriebssystems überzeugt. Im Interesse der IT-Sicherheit hoffe ich, dass unsere Initiativen auch bei Ihnen Zustimmung finden und dass wir in Zukunft anfällige Monokulturen vermeiden können.

Gerade im schnelllebigen IT-Bereich kann Zukunft aber bereits Morgen heißen. Umso wichtiger ist es, sich abzeichnende Trends bereits frühzeitig zu verfolgen, um im Interesse von Wirtschaft und Verbrauchern frühzeitig steuernd eingreifen zu können. Dabei stellt sich oft die Frage, wie Sicherheit im Hinblick auf neue Technologien zu bewerten ist. Hier möchte ich als Beispiel nur die Initiativen TCPA (Trusted Computing Platform Alliance) und Palladium nennen, mittlerweile umbenannt in TCG (Trusted Computing Group) und NGSCB (Next Genera

tion Secure Computing Base). Einerseits sollen damit Mechanismen eingeführt werden, die IT-Systeme besser als bisher vor Schadsoftware und Missbrauch schützen, andererseits besteht die Gefahr, dass diese Technologien den Nutzer in seiner Freiheit beschneiden und dem Nutzer unbemerkt die Kontrolle über seine persönlichen Daten entgleitet. Soll der Anwender dieser neuen Technologie vertrauen ? Unter welchen Umständen ? Diese Fragen harren nach der Beantwortung. Das BSI hat dazu eine Projektgruppe eingesetzt.

Wir werden diese und andere neue Technologien intensiv beobachten, analysieren und durch Gespräche mit den Initiatoren darauf hinwirken, dass nur Sicherheitsfunktionen umgesetzt werden, die für den Nutzer transparent sind und deren Aktivierung nicht die informelle Selbstbestimmung des Anwenders gefährdet.

In dieses Spannungsfeld zwischen Sicherheit, Datenschutz und die Wahrung der Persönlichkeitsrechte fällt auch eine weitere neue Technologie, die Biometrie. Biometrische Verfahren haben ein erhebliches Potential, die Sicherheit zu erhöhen. Dieses Potential wollen wir nutzen. Der Erfolg der Bemühungen und die Akzeptanz der Systeme wird aber auch davon abhängen, dass sie IT-Sicherheits- und Datenschutzbelange berücksichtigen. Diese Fragen werden auch hier auf dem Kongress diskutiert werden - durch eine eigene Sektion zur Biometrie.

Ein eher klassischer Bereich der Sicherheitstechnik ist die Kryptographie. Beim Einsatz der Kryptographie bleiben wir auch weiterhin den bisherigen Eckpunkten unserer Kryptopolitik treu, die den Einsatz der Kryptographie fördert und jeglicher Kryptoregulierung eine klare Absage erteilt. Kryptographie ist für uns die Basis für einen sicheren elektronischen Geschäftsverkehr.

2. Bereich:

Wir sichern die Infrastrukturen

Von staatlicher Seite wird zu recht erwartet, dass für ein sicheres, stabiles Umfeld Sorge getragen wird. Heutzu

tage heißt das auch, dass wir uns um sichere Informationsinfrastrukturen kümmern müssen. Wir haben deshalb ein umfangreiches Programm initiiert, das das Problem nicht nur punktuell aufgreift, sondern im Sinne einer umfassenden Sicherheitsinfrastruktur ganzheitlich betrachtet.

Dabei geht es um folgende Maßnahmen:

ERSTENS

Wir werden die bestehende CERT Landschaft in Deutschland zu einer flächendeckenden Infrastruktur ausbauen. Der Begriff Computer Emergency Response Team (CERT) subsumiert verschiedene Ansätze und Bestrebungen die Sicherheit von Systemen der Informationstechnik zu gewährleisten. Diese Notfallteams sind heutzutage sozusagen die Feuerwehr im IT-Bereich. Ihre Arbeit ist anerkannt und nicht mehr weg zu denken. Wir können heute in Deutschland bereits auf eine funktionierende Infrastruktur dieser CERTs aufbauen. Insgesamt gibt es in Deutschland derzeit etwa 15 CERTs in Wirtschaft, Forschung und Verwaltung. Das „CERT-Bund“ im Bundesamt für Sicherheit in der Informationstechnik verfügt u.a. über einen Warn- und Informationsdienst und betreibt ein Rund-um-die-Uhr erreichbares Lagezentrum.

ZWEITENS

werden wir weitere Sicherheitskooperationen zwischen Bundesregierung und Infrastrukturunternehmen schließen, in denen die gemeinsamen Handlungsstränge festgehalten sind. Nach dem 11. September 2001 hat Bundesinnenminister Otto Schily selbst mit allen für kritische Infrastrukturen verantwortlichen Wirtschaftszweigen intensive Gespräche geführt. Daraus sind inzwischen immer mehr unmittelbare Sicherheitskooperationen mit Unternehmen entstanden, die auch erste praktische Erfolge zeigen. Ich nenne nur die CERT Kooperation mit der Deutschen Telekom und den Kooperationsvertrag mit IBM zur Förderung sicherer offener Software in der öffentlichen Verwaltung.

DRITTENS

Wir untersuchen das Sicherheitsniveau in den Gefährdungsbereichen im Detail. Die IT-Abhängigkeit der kritischen Infrastrukturbereiche steht dabei im Vordergrund. Die ersten Studienergebnisse werden derzeit ausgewertet. Anschließend werden Sie mit den Vertretern der Infrastrukturen diskutiert, um gemeinsam die nächsten Schritte zu erörtern, denn hier trägt nicht der Staat allein Verantwortung.

VIERTENS

Wir werden aber auch selbst mit gutem Beispiel vorangehen und die kritischen IT-Systeme der Bundesverwaltung identifizieren und - soweit noch nicht geschehen - entsprechend schützen. Denn auch in staatlichen IT-Systemen finden sich kritischen Infrastrukturen für unsere Gesellschaft.

FÜNFTENS

bauen wir die Kompetenz des BSI weiter aus, um die Angreifbarkeit von IT-Systemen unter realen Bedingungen feststellen zu können. So haben wir im BSI sogenannte Tiger- bzw. Penetrationsteams eingerichtet, die die zuvor identifizierten kritischen IT-Systeme in der Bundesverwaltung und deren IT-Sicherheitsmaßnahmen praktisch auf den Prüfstand stellen.

SECHSTENS

ist die Entwicklung eines Hochsicherheitskompendiums vorgesehen, in dem für typische Kommunikationsanbindungen Hochsicherheitskonzepte als Sicherheitsprofil vorgegeben sind. Dieses Kompendium ergänzt das erfolgreiche IT-Grundschutzhandbuch des BSI um Maßnahmenbündel für den Hochschutzbedarf.

3. Bereich:

Wir bringen IT-Sicherheit ins öffentliche Bewusstsein

In diesem Bereich haben wir ganz konkrete Maßnahmen ergriffen, um für das Thema Sicherheit im Internet zu sensibilisieren. Ich gehe zwar davon aus, dass unter den Zuhörern dieses Sicherheitskongresses viele Experten sind die nicht mehr sensibilisiert werden müssen, aber es zeigt sich, dass immer noch ein Großteil der Anwender nur rudimentäre Kenntnisse im IT-Bereich besitzen. Speziell für diese Zielgruppe wurde durch das BSI eine Sicherheits-CD entwickelt. Ziel der CD-ROM war es dabei, Bürgerinnen und Bürger für das Thema "IT-Sicherheit" zu sensibilisieren. Die Inhalte der CD richten sich daher an Anfänger bzw. eher unerfahrene Anwender. Die Kernaussage lautet: Sicherheit im Internet beginnt zu Hause. Denn das Verhalten der Anwender am eigenen Computer hat große Auswirkungen auf die Abwehr von Risiken aus dem Internet. Die überaus positive Resonanz auf diese CD hat uns dazu bewogen auf der diesjährigen CeBit eine überarbeitete Version zu präsentieren. Die Rückmeldungen zu dieser Aktion bestärken uns darin auf diesem Weg fortzufahren. Ein weiterer Meilenstein auf diesem Weg war die Platzierung der Webseite www.bsi-fuer-buerger.de. Dort können die jeweils aktuellen Inhalte der Sicherheits-CD online abgerufen werden, so dass dem Nutzer jeweils die aktuelle Version zur Verfügung steht.

Sicherheit in das öffentliche Bewusstsein zu bringen, schafft Erwartungshaltungen: „was sollen wir tun“ wird gefragt. Auch diesem Anliegen müssen wir gerecht werden. So ist die Bürger-CD für den einfachen Internetnutzer mit einer Tool-Box versehen und vielen praktischen Hinweisen. – Und für die Anwender im Bereich von Behörden und Industrieunternehmen gibt das BSI konkrete Handlungsempfehlungen: das e-Government Handbuch für die öffentliche Verwaltung und das IT-Grundschutzhandbuch – inzwischen geradezu ein Klassiker in diesem Bereich – für Partner im Wirtschafts- und Industriebereich. Durch ein zusammen mit Wirtschaftspartnern vom BSI erarbeitetes Zertifizierungsschema für den IT-Grundschutz und Kooperation mit vom BSI lizenzierten

Grundschutzauditoren konnten wir dies Programm noch effektiver in die Fläche bringen.

Der Bedarf für fundierte Sicherheitsinformationen und Nutzungshinweise ist – so wissen wir alle hier – auch ganz praktisch da. Deshalb überlegen wir derzeit, wie wir unsere Maßnahmen im Bereich IT-Sicherheit noch exakter auf die jeweilige Zielgruppe zuzuschneiden können.

Anrede,

diese Aufzählung hat verdeutlicht dass wir IT-Sicherheit sehr ernst nehmen und hier auf vielen Ebenen tätig sind. Auch in Zukunft werden wir bewährte Maßnahmen zur Steigerung der IT-Sicherheit, wie die Förderung von offener Software oder die Förschreibung unserer liberalen Kryptopolitik weiterführen und neue, vielversprechende Bereiche wie die Biometrie aktiv vorantreiben.

Wie bereits am Anfang erwähnt, müssen wir für komplexe Techniken, die nicht auf den ersten Blick zu verstehen sind, Vertrauen schaffen. Umfassende Aufklärung, Transparenz und Verständnis sind daher Grundvoraussetzungen für allseits akzeptierte Sicherheitslösungen. Ich bin sicher die Vorträge und Diskussionen im Rahmen dieses Kongresses werden dazu beitragen.

Ich bedanke mich für Ihre Aufmerksamkeit und wünsche Ihnen während der drei Kongresstage interessante Vorträge, spannende Diskussionen und einen angenehmen Aufenthalt hier in Bonn.