Quelle: http://www.bmi.bund.de/cln_183/SharedDocs/Reden/DE/2010/10/bm_isse.html?nn=10 (2010-07-10)

"Das Internet als Chance und integrativen Bestandteil unseres Lebens verstehen"

Anlass: Europäische Sicherheitskonferenz ISSE
Datum: 05.10.2010
Ort: Berlin
Redner: Dr. Thomas de Maizière, Bundesminister des Innern

Es gilt das gesprochene Wort.

Stellen Sie sich vor, es gäbe kein Internet.

Stellen Sie sich vor, es gäbe keine Email-Kommunikation.

Stellen Sie sich vor, es gäbe keine Mobil-Telefonie.

Manche von den hier Anwesenden, meine Person eingeschlossen, würden sich dann in 1980er Jahre zurückversetzt fühlen. Wir hätten keine Viren- und Trojaner-Attacken, unsere Netze würden nicht durch Spam-Mails verstopft und im Restaurant würde ein schöner Abend mit Freunden nicht durch ständiges Mobiltelefon-Gebimmel unterbrochen werden.

Andererseits gäbe es aber auch keine boomende Internet-Industrie, keine schnellen und unkomplizierten Kommunikationswege und auch der Abend mit den Freunden wäre vielleicht so spontan nicht zusammengekommen, weil eben diese nicht erreichbar gewesen wären.

Wenn Sie sich nochmal zurückerinnern, war das Internet vor einigen Jahren hauptsächlich eine Informationsplattform, anfangs nur wenigen bekannt und zugänglich. Heute ist das Netz integrativer Bestandteil unseres Lebens. Diese Entwicklung hat viele neue Möglichkeiten geschaffen, wirtschaftlich, gesellschaftlich, sozial. Denken Sie nur an die neuen Geschäftsmodelle rund um das Netz. Denken Sie an die Fortschritte für Meinungsfreiheit in der Welt. Oder denken Sie an Eltern und Großeltern, die per Internet einfach Kontakt zu weit entfernten Kindern und Enkeln halten.

So positiv und chancenreich die zunehmende Vernetzung aller Lebens-, Wirtschafts- und Verwaltungsbereiche über das Internet ist, sie hat auch ihre Schattenseiten. Die Verfügbarkeit unserer Computernetze wird zunehmend von einer stark international tätigen organisierten Kriminalität missbraucht. Mittels ausgeklügelter Schadaktivitäten versuchen Cyber-Kriminelle wirtschaftliche Vorteile zu erzielen. Ganz neue Wertschöpfungskreisläufe haben sich um diese Schattenwirtschaft gebildet. Wir erleben eine deutliche Zunahme von Spionage- und Sabotageaktivitäten.

Aktuell ist Anfang Juli ein neues mächtiges Schadprogramm entdeckt, welches auf den Namen Stuxnet getauft wurde. Dieses greift erstmalig sogenannte SCADA-Systeme (SCADA: Supervisory Control and Data Aquisition) an, die in vielen wichtigen Infrastrukturbereichen eingesetzt werden. Für Erstinfektion reicht schon das Einstecken eines USB-Sticks an einen Computer, es muss nicht einmal ein Programm aufgerufen werden, mit dem sich der Schädling tarnt.

Dieser Vorfall bedeutet eine Zeitenwende im IT-Sicherheitsmanagement. Selbst Prozessleitsteuerungssysteme, die bisher in isolierten Umgebungen eingesetzt wurden, können zukünftig von IT-Angriffen wie Stuxnet beeinträchtigt werden. Denn anscheinend hat es eine schleichende Entwicklung gegeben, diese Systeme mit dem Internet zu verbinden, außerdem werden immer mehr Standard-PC-Systeme eingesetzt, was zu einem höheres Angriffsrisiko führt. Diese Entwicklung ist mit Sorge zu betrachten, denn sie eröffnet neue Möglichkeiten kriminellen Handelns, wenngleich der Aufwand für solche Angriffe extrem hoch ist.

Auch der Schutz vor missbräuchlicher Verwendung sog. Botnetze, also das illegale Kapern und Zusammenschalten von Rechnern ohne Wissen der eigentlichen Besitzer, ist eine der Herausforderungen des modernen Computer-Zeitalters. Dabei gilt es, Millionen von Computern, die alle zu jeder Zeit online sind, effektiv gegen Schadcodeinfektion und Missbrauch zu schützen.

Das beständig laufende Wettrennen zwischen den Sicherheitsverantwortlichen und den Angreifern können wir nur dann bestehen, wenn Wirtschaft, Forschung und Verwaltung gemeinsam in einen Dialog treten und auf nationaler und internationaler Ebene partnerschaftlich und vertrauensvoll zusammenarbeiten. Wir müssen weiterhin und verstärkt sensibilisieren und dem Thema IT-Sicherheit eine hohe politische Bedeutung beimessen.

Bei all unserem Handeln dürfen wir nicht vergessen, dass nicht die Informations- und Kommunikationstechnologien oder das Internet, sondern der selbstbestimmte Mensch im Mittelpunkt unseres Schutzes und unseres Handelns steht. Die rasante technische Entwicklung und vor allem das Internet mit seinen scheinbar grenzenlosen Chancen aber auch seinen Risiken verlangen, dass wir die Menschen auf dem Weg in das "Cyber-Zeitalter" mitnehmen und schützen.

Dazu müssen wir

1. aufklären,

2. Transparenz schaffen

3. und unsere Verantwortung ernst nehmen.

Zu meinem ersten Punkt: Jeder "User" des Internets darf eines nicht vergessen: Wer im Netz unterwegs ist, braucht Grundkenntnisse und einen Gutteil gesunden Menschenverstand: Warum soll ich intime Details meines Lebens ins Internet stellen, die ich sonst nur mit wenigen Freunden teilen würde? Wie muss ein zuverlässiges und sicheres Passwort aussehen? Welche Grundeinstellungen muss ich vornehmen, um mich vor Viren und Schadprogrammen zu schützen? Auf welche Sicherheitsgefahren muss ich achten, wenn ich im Internet unterwegs bin? Wie gestalte ich eigene Angebote so, dass andere keinen Schaden nehmen können? Mein Ministerium unterstützt deshalb bereits Initiativen wie "Deutschland sicher im Netz", die einen wichtigen Beitrag zur Aufklärung leisten. Das wollen wir auch weiterhin tun.

Zu meinem zweiten Punkt: Bei der Transparenz geht es vor allem um die Nachvollziehbarkeit der Datenverarbeitung. Auch hier ist viel zu tun.

Unternehmen können und müssen im Internet ungleich einfacher, rascher und vollständiger als bisher in allgemein verständlicher Weise darüber informieren, welche Daten sie erheben, zu welchem Zweck sie sie verarbeiten und an wen sie weitergeleitet werden. Die Anbieter sind gut beraten, hierzu gemeinsam rechtlich bindende Vereinbarungen zu verabreden.

Und zu meinem dritten Punkt: Viele Neuerungen der Informations- und Kommunikationstechnologien und des Internets sind durch das bestehende Recht bereits zufriedenstellend geregelt. Und: Wir sollten stets versuchen, zunächst eine Analogie zur „Offline-Welt“ zu bilden.

Nur wo das geltende Recht Lücken offenbart, muss der Staat prüfen, ob und wie er diese Lücken schließt. Er sollte aber bei jeder einzelnen neuen gesetzlichen Regelung genau prüfen, ob es nicht ausreicht, die Selbstregulierungskräfte von Gesellschaft und Wirtschaft zu nutzen und - wo notwendig - einfordern. Erst wo dies nicht zu gesellschaftsverträglichen Lösungen führt oder starke Partikularinteressen das Gemeinwohl überlagern, muss und wird der Staat selbst aktiv werden.

An anderer Stelle hingegen müssen wir uns intensiver über den möglichen gesetzgeberischen Handlungsbedarf Gedanken machen. Wie können wir es zum Beispiel schaffen, dass der Einzelne auch im digitalen Zeitalter die Kontrolle über sensible Informationen und personenbezogene Daten behält?

Zur Beantwortung dieser Frage müssen wir unser geltendes Datenschutzrecht, das ganz überwiegend aus dem analogen Zeitalter stammt, auf den Prüfstand stellen. Dabei wird insbesondere zu beachten sein, dass Datenschutz und Datensicherheit immer eine rechtliche, eine technische und eine internationale Komponente aufweisen - beide müssen im Einklang miteinander weiterentwickelt werden wenn man zu guten Lösungen gelangen will.

Als gutes Beispiel hierfür möchte ich auf die Notwendigkeit der vertrauenswürdigen Online-Identifizierung und der sicheren Übermittlung von Identitätsinformationen verweisen. Mit „De-Mail“ und dem neuen Personalausweis bieten wir für beides technische Möglichkeiten an.

Ebenso könnten internetbasierte - also technische - Datenschutz-Applikationen, sogenannte "Privacy-Apps" bestehende Auskunfts- oder Widerspruchsrechte "per Mausklick" einfach und ökonomisch umsetzen. Vielleicht entstehen erste Ideen für solche "Apps" im Rahmen dieser Konferenz.

Auch wenn es um die Kontrollmöglichkeiten des einzelnen Bürgers geht, müssen rechtliche und technische Lösungsansätze „Hand in Hand“ verfolgt werden. Als Beispiel mag insoweit das digitale Verfallsdatum dienen, mit dessen Hilfe jeder Nutzer bestimmen kann, wie lange die von ihm ins Netz gestellten Informationen abrufbar bleiben sollen. Erfreulicherweise beschäftigen sich bereits Lösungsanbieter und Forschungseinrichtungen mit der Realisierung solcher Ansätze. Unbestritten sind dabei noch einige technische Probleme zu lösen.

Das Internet ermöglicht uns eine global vernetzte Informationsverarbeitung und -speicherung. Beim sog. "Cloud-Computing" etwa befinden sich die Daten innerhalb einer „virtuellen Wolke“ außerhalb der eigenen Infrastruktur. Das hat zum einen den Vorteil, dass ich fast überall und jederzeit auf meine Daten zugreifen kann. Zum anderen kann ich allerdings dabei nur schwer nachvollziehen, wo und von wem genau meine Daten gespeichert und verarbeitet werden. Damit einher geht die Unsicherheit, welches Recht Anwendung findet.

Die Kontrolle über sensible Informationen und personenbezogene Daten zu behalten, ist daher eine Herausforderung für die Zukunft. Bei der Ausgestaltung der Daten- und Informationssicherheit, für das „Identitäts-, Berechtigungs- und Zugriffsmanagement“ werden wir vertrauenswürdige und international interoperable Systeme und Applikationen benötigen.

Wenn wir über rechtliche Rahmenbedingungen für "Clouds" sprechen, die Datensicherheit und Datenschutz garantieren, so müssen wir europäisch und global denken. Die Entwicklung nationaler, supranationaler und internationaler Regelungen muss Hand in Hand gehen.

Auf nationaler Ebene können und werden wir eigene Konzepte für den Umgang mit dem Internet entwickeln und diese in die internationale Willensbildung einbringen.

25 Jahre, nachdem die E-Mail ihren Siegeszug angetreten hat, werden heute immer noch weniger als 5 Prozent der E-Mails in Deutschland verschlüsselt versendet. Der bei weitem überwiegende Teil aller E-Mails kann samt der Anhänge auf seinem Weg durch das Internet abgefangen, wie Postkarten mitgelesen und inhaltlich verändert werden. Absender und Empfänger können deshalb nie vollständig sicher sein, mit wem sie gerade kommunizieren und ob der Inhalt der E-Mail verändert wurde. Daneben gibt es das Problem der fehlenden Nachweisbarkeit: sie können nie sicher sagen, ob eine E-Mail tatsächlich beim Empfänger angekommen ist.

Mit der "De-Mail" schaffen wir gemeinsam mit Vertretern der IT-Industrie ein höheres Vertrauensniveau zwischen den Kommunikationspartnern. Abgesicherte Anmeldeverfahren und Verbindungen zwischen den Anbietern verhindern ein Mitlesen oder Verändern der Nachricht. Außerdem ist der Zeitpunkt der Zustellung der Nachricht verbindlich nachweisbar.

Bei der Konzeption von "De-Mail" haben wir darauf Wert gelegt, dass die Technologie so vertraut zu nutzen ist wie die heutige E-Mail. Dadurch versprechen wir uns, das Sicherheitsniveau beim Austausch elektronischer Nachrichten schnell auf ein höheres Niveau zu heben und "De-Mail" in den Alltag zu integrieren.

Eine schnelle Integration in den Online-Alltag wünsche ich mir auch für den neuen Personalausweis, den man ab dem 1. November beantragen kann.

Mit dem neuen Dokument wird das Identifizieren auch in der Online-Welt möglich – so einfach, komfortabel und zuverlässig, wie man dies schon vom herkömmlichen Ausweis im Alltag kennt.

Die so genannte Online-Ausweisfunktion ist für Anbieter und Nutzer freiwillig. Sie ist ein Angebot. Ein Angebot der gegenseitigen eindeutigen Authentifizierung.

Wird diese Funktion genutzt, macht der neue Ausweis es für die Bürgerinnen und Bürger leichter, ihre Daten zu kontrollieren. Und wenn doch Daten offengelegt werden müssen, dann kann dies bewusster und zielgerichteter getan werden.

Viele Vorkehrungen sorgen dafür, dass Daten und Informationen nicht zusammengeführt werden können. Niemand muss befürchten, zu einem "gläsernen Bürger" zu werden.

Bei der Konzeption haben wir daher ein besonders hohes Schutzniveau für die Daten der Bürger in den Mittelpunkt gestellt, ohne dass die Nutzung deswegen kompliziert wird. Dies beinhaltet, dass nur die Daten aus dem Ausweis ausgelesen werden können, die in der jeweiligen Situation auch tatsächlich benötigt werden.

Wenn Sie beispielsweise bei einem Online-Shop ein Buch kaufen wollen, wird dieser zwar meine Adresse lesen, auf mein Geburtsdatum dagegen nicht zugreifen können.

Welche Daten offenbart werden, entscheidet am Ende in jedem Fall der Nutzer selbst. Dabei erfolgt das "Online-Ausweisen" wechselseitig: der Online-Shop, der meinen Ausweis sehen will, muss sich ebenfalls ausweisen. Dafür vergibt der Staat Berechtigungszertifikate, die an strenge datenschutzrechtliche Auflagen geknüpft sind. Hier fungiert der Staat als ein hoheitlicher Vertrauensstifter, ohne sich jedoch in die Kommunikation zwischen Nutzern und Anbietern einzuschalten.

Den neuen Personalausweis haben wir gemeinsam mit Experten entwickelt und prüfen lassen. Dadurch konnten wir sowohl, was die physikalische Dokumentensicherheit, als auch die Sicherheit der elektronisch abgelegten Daten anbetrifft, eine moderne und sichere Identitätskarte entwickeln. Alle Übertragungen sind mit Sicherheitsmechanismen geschützt, so dass niemand Daten mitlesen, kopieren oder verändern kann, dem es nicht ausdrücklich gestattet ist. Ohne aktives Zutun des Ausweisinhabers können keine Daten ausgelesen bzw. ausgetauscht werden. Auch hier gilt: Der "User" bleibt aufgefordert, seinen Rechner auf dem sicherheitstechnisch aktuellen Stand zu halten, um Missbrauch zu verhindern.

Der Bund hat mit den Strukturen des neuen Personalausweises eine leistungsfähige Grundlage für die Nutzung geschaffen. Technische Aspekte sind dabei genauso berücksichtigt wie rechtliche und organisatorische. Nun ist es an den Dienstleistern im Internet, dies zu nutzen. Dieser Appell richtet sich einerseits an die Unternehmen, die ihre personalisierten Dienstleistungen im Internet anbieten, aber auch an die Länder und Kommunen, die es mit dem neuen Ausweis einfacher haben, ihre Behördendienstleistungen komfortabler zu machen. Bürgerinnen und Bürgern kann so mancher persönliche Besuch auf dem Amt erspart werden.

Auch innerhalb der Bundesverwaltung besitzt die Informationstechnik herausragende Bedeutung für die Handlungs- und Arbeitsfähigkeit. In Wirtschaft und Verwaltung ist mobiles Telefonieren und Versenden von Kurznachrichten fester Bestandteil des beruflichen Alltags.

Mittlerweile ist aber allgemein bekannt, dass GSM-Mobilfunknetze mit relativ geringem Aufwand abhörbar sind. Konkret bedeutet dies, dass Telefonate und SMS-Nachrichten durch zusätzliche Verschlüsselung in Mobiltelefonen geschützt werden müssen.

Das Bundesamt für Sicherheit in der Informationstechnik entwickelte daher einen Standard für das verschlüsselte Telefonieren und den verschlüsselten SMS-Versand, mit dem Namen "Sichere Netzübergreifende Sprachkommunikation", kurz SNS.

Dank dieses neu definierten Standards sind verschlüsselte Telefongespräche und SMS-Versand zwischen Mobiltelefonen unterschiedlicher Hersteller möglich. Der neue Standard sieht außerdem auch verschlüsselte Verbindungen zu TETRA-Funkgeräten von Polizei, Feuerwehr und anderen Sicherheitsorganisationen vor. Der SNS-Standard ist offen und ermöglicht interessierten Herstellern, entsprechende Produkte zu entwickeln und auf dem Markt anzubieten.

Diese und weitere Produkte nach SNS-Standard sichern zukünftig die mobile Kommunikation der Bundesverwaltung ab.

Wir wollen grundsätzlich unsere Möglichkeiten nutzen und bereits in der Designphase neuer Infrastrukturen die Rahmenbedingungen für IT-Sicherheit verbessern. "Security-by-Design" muss die in der Vergangenheit häufig praktizierte Vorgehensweise "Security-bolted-on" perspektivisch völlig ablösen.

Wir können es uns weder volkswirtschaftlich noch sicherheitspolitisch leisten, abzuwarten, um lange nachdem die Funktionalität einer Infrastruktur aufgebaut ist, die IT-Sicherheit mit größtem Aufwand nach zu entwickeln. Dem Bundesamt für Sicherheit in der Informationstechnik (BSI) kommt daher eine wichtige Rolle zu. Das BSI begleitet frühzeitig den Aufbau von Infrastrukturen und neuen IT-basierten Applikationen.

Durch Technische Richtlinien des BSI zur IT-Sicherheit von konkreten Applikationen und Infrastrukturen, Zertifizierungen von Produkten nach festgelegten Schutzprofilen und den IT-Sicherheitsstandards des BSI werden die Weichen für eine deutlich sichere IT-Welt gestellt.

Auf diese Weise wird ein verlässlicher Rahmen für langfristige Investitionssicherheit in immer komplexer werdenden Strukturen geschaffen. Gleichzeitig wirkt der Bund durch das Setzen von Standards als Richtungsgeber und Förderer für zukünftige Innovationen in der Informationstechnik.

IT-Sicherheit ist längst kein nationales Thema mehr. Durch den hohen Grad an weltweiter Vernetzung unserer Informationssysteme haben Vorfälle in anderen Ländern zunehmend Auswirkungen auch auf die IT-Sicherheit in unserem Land. Die Grenzen zwischen innerer und äußerer Sicherheit verschwimmen immer mehr.

Die Bundesregierung setzt sich daher nicht nur national, sondern auch international für eine Stärkung der grenzüberschreitenden IT-Sicherheit ein.

Auf europäischer Ebene muss unser mittelfristiges Ziel sein, europaweit Sicherheitsthemen für die IT zu etablieren und so ein harmonisiertes IT-Sicherheitsniveau in der EU zu schaffen, auf das sich alle Beteiligten verlassen können. Wichtige Dienste auf dem Weg dorthin leistet die seit 2004 bestehende Europäische Agentur für Netz- und Informationssicherheit "ENISA".

Das Mandat für ENISA wird aktuell gerade neu verhandelt. Mein Wunsch ist es, ENISA zukünftig stärker in politische Entscheidungsprozesse der Europäischen Union und deren Umsetzung in den Mitgliedstaaten einzubinden.

Außerhalb der EU engagieren wir uns für IT-Sicherheit in staatenübergreifenden Initiativen und Organisationen, wie etwa der OECD, der Nato oder der G8. Hier wird das nächste Etappenziel sein, auf eine Bündelung der mittlerweile in einer Vielzahl von Einzelinitiativen zersplitterten internationalen Aktivitäten hinzuwirken. Bestehenden Sicherheitsstandards müssen wir zu größerer Akzeptanz verhelfen.

Ob national oder international, mit Konferenzen wie dieser tragen Sie dazu bei, dass unsere Ideen und unser Handeln transparent werden. Der Austausch über die Herausforderungen, die uns das Internet in Zukunft bringt, hilft uns allen ein Stück weit neue, innovative Lösungen zu schaffen und nicht gleich weitere rechtliche Regularien zu fordern.

Diese ISSE-Konferenz stellt sich genau diesem Anspruch, neuen innovativen Lösungen in Europa eine Bühne zu geben. Daher ist mein Apell an Sie, lassen Sie uns weiterhin mit großer Kreativität gemeinsam, Privatwirtschaft und Regierungen, die Potentiale heben, die in den modernen Informations- und Kommunikations-Technologien (IKT) stecken und interessante, vielseitige aber insbesondere vertrauenswürdige IT-Lösungen für die Gesellschaft schaffen.

Stellen Sie sich also eine Welt vor, in der es ein jederzeit sicheres Internet gibt.

Stellen Sie sich eine Welt vor, in der mobile Kommunikation für jeden Nutzer einfach, sicher und zuverlässig ist.

Stellen Sie sich eine Welt vor, in der jeder "Hoheit" über seine Daten hat.

Das mag uns im Augenblick vielleicht noch 20 Jahre in die Zukunft versetzen, aber wir müssen schon heute die Chancen nutzen, Visionen Realität werden zu lassen, damit die Segnungen des digitalen Zeitalters nicht zur Last werden.

Dafür wünsche ich Ihnen für die nächsten drei Tage dieser Konferenz ein gutes Gelingen und einen regen Austausch.