Die Bundesregierung

HPI Hasso Plattner Institut

Nationaler IT-Gipfel

18. Dezember 2006
Hasso-Plattner-Institut Potsdam

Arbeitsgruppe 4
„Sicherheit und Vertrauen in IT und Internet“

1. Bestandsaufnahme
2. Handlungsfelder
3. Lösungsvorschläge

1. Bestandsaufnahme

- Die Nutzung von Informationstechnologien und Diensten der Informationsgesellschaft ist Teil des Alltags sowohl von Unternehmen aller Größen als auch von Privatpersonen geworden. Ihr Einsatz schafft enorme wirtschaftliche wie auch gesellschaftliche Chancen, birgt aber auch immer wieder Risiken missbräuchlicher Nutzung. Diese können das Vertrauen in die Technologien und die darauf basierenden Dienste schwächen und die Rechtssicherheit als eine Grundvoraussetzung des elektronischen Geschäftsverkehrs beeinträchtigen.
- Den Gefahren kann wirksam begegnet werden; Schutzmechanismen stehen bereit und werden fortlaufend weiterentwickelt, um sich neuen Bedrohungspotentialen anzupassen. Ein Erfolg im Bemühen um stetig wachsende Sicherheit in der Nutzung von IT und Internet kann aber nur durch Kooperation aller beteiligten Akteure erreicht werden, von der Wirtschaft über die öffentliche Hand, die Wissenschaft, gesellschaftliche Gruppen bis zum Nutzer selbst. Dieses gemeinsame Engagement voranzutreiben, ist Ziel der Arbeitsgruppe „Sicherheit und Vertrauen in IT und Internet“.
- Mit dem Nationalen Plan zum Schutz der Informationsinfrastrukturen hat sich auch die Bundesregierung ein weit reichendes Programm für die IT-Sicherheit gegeben. Der Plan basiert ebenfalls auf der gemeinsamen Verantwortung von Staat und Verwaltung, Wirtschaft und Industrie, Bürgerinnen und Bürger für IT-Sicherheit. Nur im intensiven Zusammenwirken kann eine erfolgreiche Umsetzung gelingen.

2. Handlungsfelder

- Die Arbeitsgruppe hat die breite Vielfalt von Sicherheitsfragen zu einer Agenda der mit besonderem Augenmerk zu adressierenden Handlungsfelder verdichtet. Dabei wurden folgende Themen identifiziert:
    - **Datensicherheit**: Der Schutz der mit IT verarbeiteten Daten vor Verlust und unbefugtem Zugriff ist die Grundlage und zentrale Voraussetzung für die sichere und vertrauensvolle Nutzung von IT. Besonders in Klein- und Mittelbetrieben wird die Bedeutung von Datensicherheit aber meist unterschätzt und vernachlässigt, obwohl Sie von entscheidender Bedeutung bei der Vermeidung von Wettbewerbsnachteilen ist. Erstes Element der Datensicherheit ist der Schutz der vertraulichen Daten mittels Verschlüsselung vor dem Zugriff unberechtigter Personen. Die Gefährdung entsteht z.B. durch den Verlust von mobilen Geräten (Notebook , Pocket PC) oder auch

durch gezielte Datenspionage, mittels Viren, Würmer, Trojaner oder sonstige Spionageprogramme. Schließlich ist die Zugriffs- und Abhörsicherheit von transportierten Daten etwa im Bereich eMail, Voice-over-IP oder auch bei drahtlosen Internetzugängen wie WLAN sicherzustellen.

- **Identitätsschutz**: Die Feststellung der Identität von Personen durch ihre Identifizierungsdaten (wie z.B. Name, Anschrift, Benutzernamen oder Kennwörter) und die Verwendung von digitalen Identitäten sind vielfach Grundlage von Aktivitäten im Internet. Gerade in der geschäftlichen Nutzung des Internets ist es von zentraler Bedeutung, dass nur berechtigte Personen Zugang zu Informationen und Transaktionsmöglichkeiten haben. Die Identifizierungsdaten von Personen sind aber immer wieder Ziel von Angriffen, um betrügerische Handlungen vorzunehmen oder gar die Herrschaft über fremde Benutzerkonten (z.B. im Bereich des Online-Bankings) zu gewinnen. Dies kann sowohl zu erheblichem wirtschaftlichen Schaden führen als auch das Vertrauen der Nutzer in diese Anwendungen nachhaltig erschüttern. Die Form der Angriffe ist vielfältig. Sie reichen vom Einsatz von Trojanern zum Ausspionieren von Kennwörtern über Phishing und Pharming bis hin zum Diebstahl einer fremden Identität für Internet-Aktivitäten oder die Nutzung gefälschter Absenderangaben bei eMails. Die Attacken setzen somit gleichermaßen an technischen, prozeduralen als auch menschlichen Schwachstellen in der Nutzung des Internets an und erfordern daher Maßnahmen auf verschiedenen Ebenen.
- **Schutz vor Online-Betrugsformen**: Transaktionssicherheit im elektronischen Geschäftsverkehr kann nur erreicht werden, wenn der Nutzer hinreichend vor betrügerischen Aktivitäten geschützt ist. Ein angemessener Identitätsschutz ist dabei nur ein - wenn auch wichtiger – Beitrag unter vielen. Daneben ist immer wieder eine Verlagerung von auch offline bekannten Betrugsmustern (Warenbetrug, Warenkreditbetrug, betrügerische Finanzanlagen, Nigeria-Spam/“Scam“ etc.) in elektronische Medien zu beobachten und muss auch dort wirksam bekämpfbar sein, um das Vertrauen der Nutzer nicht zu gefährden. Gleiches gilt für den betrügerischen Einsatz spezifischer TK- und IT-Technologien, wie zum Beispiel den Missbrauch von Dialern.
- **Jugendmedienschutz / Illegale Inhalte:** Die Bekämpfung illegaler Inhalte wie Kinderpornografie oder rechtsextremer Hasspropaganda muss ein zentrales Element der Bemühungen um ein sicheres Internet sein. Gerade das deutsche Beispiel zeigt, dass hier ein intensives Zusammenwirken von Staat, Unternehmen und gesellschaftlichen Akteuren auch in einem globalen Medium greifbare Ergebnisse erzielen kann. Ein besonderes Augenmerk gilt zudem einem effektiven Jugendmedienschutz. Auch hier haben in Deutschland die etablierten Systeme der Selbstregulierung, teils in Form der Co-Regulierung mit staatlichen Stellen, bereits ein im internationalen

Vergleich sehr gutes Schutzniveau erreicht. Alle diese Maßnahmen müssen schließlich von einer stetigen Fortentwicklung der Medienkompetenz, insb. bei Kindern und Jugendlichen sowie deren Eltern und Lehrern, begleitet werden.

- **Spam**: Der Missbrauch der eMail-Dienste zu Spamming führt zu erheblichen Effizienzeinbußen bei der Nutzung dieser Kommunikationstechnik. Gleiches kann in Zukunft anderen modernen Kommunikationstechnologien wie Mobile oder Instant Messaging drohen. Deshalb ist es notwendig, hier nicht nur mit reaktiven Maßnahmen wie effektiven Spam-Filtern die Beeinträchtigungen gering zu halten, sondern alles zu unternehmen, das Übel auch an der Wurzel zu packen, ohne die legitime Nutzung des Mediums – auch für legale Werbezwecke – zu gefährden.
- **Piraterie / Raubkopien / Urheberrechtsverletzungen:** Als Folge der Digitalisierung verstärkt sich der Grad der Bedrohung geistigen Eigentums durch die Verbreitung und Nutzung unerlaubter Kopien. Der Piraterie von Software, aber auch Medieninhalten wirksam Einhalt zu gebieten, gehört daher ebefalls zu einem sicheren wirtschaftlichen Umfeld für IT-Nutzung und Internet.

3. Lösungsvorschläge

- Die Gewährleistung von Sicherheit und Vertrauen beim Umgang mit IT und Internet ist eine kontinuierliche Aufgabe, um den immer neuen Herausforderungen zu begegnen.
- Erfolg kann dabei nur erzielt werden, wenn nicht nur objektiv gute Sicherheitsbedingungen geschaffen, sondern auch die Existenz und der richtige Einsatz vorhandener Schutzinstrumente den geschäftlichen wie privaten Nutzern vermittelt werden. Die Warnung vor Gefahren sollte stets auch mit dem Aufzeigen von Lösungen für einen wirksamen Schutz und konkreten Hilfestellungen für den Nutzer verbunden werden. Dies wird die tatsächliche Anwendung vorhandener Sicherheitsmechanismen fördern und zugleich das subjektive Sicherheitsgefühl und damit auch das Vertrauen der Nutzer in die Informationstechnologie und Dienste der Informationsgesellschaft stärken.
- In diesem Sinne wollen die in der AG versammelten Akteure zusammenwirken. Ein starkes Augenmerk soll dabei auf privaten Nutzern, gerade auch Computer-Neulingen, sowie kleinen und mittelständischen Unternehmen liegen; hier besteht in besonderem Maße Aufklärungs- und Informationsbedarf.
- Daher sieht die Arbeitsgruppe die Neuaufstellung der bisherigen Sicherheitsinitiative „Deutschland sicher im Netz“ in Form eines eingetragenen Vereins als ideale

Maßnahme, um eine übergreifende und auf Dauer angelegte Plattform für alle Fragen der Sensibilisierung und Aufklärung rund um IT- und Internetsicherheit zu schaffen. Als Gründungsmitglieder des Vereins sind die Verbände BITKOM und eco, die Freiwillige Selbstkontrolle Multimedia (FSM), das Deutsche Kinderhilfswerk, der TeleTrust Deutschland e.V. sowie die Unternehmen Deutsche Telekom, der deutsche Sparkassenverlag, eBay, Microsoft, Utimaco und Verisign mit dabei. Andere Organisationen, darunter die weiteren Teilnehmer der Arbeitsgruppe „Sicherheit und Vertrauen“ beim IT-Gipfel, prüfen aktuell, in welcher Form sie bestmöglich zu dem gemeinsamen Ziel beitragen können.

- Die öffentliche Hand unterstützt nachdrücklich diese Initiative von Wirtschaft, NGOs, Verbänden und Wissenschaft und wird die Arbeit des Vereins in enger Kooperation nach besten Kräften unterstützen. Die anbieter- und technologieneutrale Initiative sollte zu einer zentralen Awareness- und Informationsplattform für die Zielgruppe Bürger und KMU für alle Fragen der Sicherheit in Informationstechnologie und Diensten der Informationsgesellschaft werden. Als Ausdruck der dauerhaften Unterstützung wird der Bundesinnenminister Dr. Schäuble die Schirmherrschaft des „Deutschland sicher im Netz e.V.“ übernehmen.
- Neben dem Bundesinnenministerium wird insbesondere auch das Bundesamt für die Sicherheit in der Informationstechnik (BSI) mit dem Verein kooperieren. Der Verein wiederum wird mit seiner Arbeit die Bundesregierung bei der Umsetzung des Nationalen Plans zum Schutz der Informationsinfrastrukturen für die Zielgruppe Bürgerinnen und Bürger sowie kleine und mittelständische Unternehmen unterstützen.
- Der „Deutschland sicher im Netz e.V.“ soll mit konkreten Maßnahmen, deren Realisierung einzelne Beteiligte in Form von Handlungsversprechen übernehmen, wesentliche Beiträge zu einer Steigerung von Sicherheit und Vertrauen in IT und Internet leisten. Die operative Aufgabe des Vereins liegt insbesondere in der Stärkung des Bewusstseins für IT- und Internet Sicherheit durch Aufklären, Informieren, Sensibilisieren und das Bereitstellen von Handlungsanweisungen.
- Die Informationen und Handlungsempfehlungen sind auch gerade auf die Bedürfnisse von Einsteigern der Computer- und Internetnutzung – sowohl in der jüngeren wie der älteren Generation – abzustellen. Dazu sollten auch nicht nur das Internet, sondern auch konventionelle Medien (z.B: Broschüren, Presse, Fernsehen) genutzt werden, um auch die besonders schutzbedürftigen Wenignutzer und Einsteiger zu erreichen. Hierzu gehört auch eine frühe Wissensvermittlung in Schulen und selbst Kindergärten zum sicheren Umgang mit neuen Medien und Computern. Ein bereits im Kindesalter geschaffenes Risikobewusstsein führt langfristig zu einem besseren Umgang mit digitalen Medien und etabliert ein Selbstverständnis der digitalen Sicherheit. Hierzu ist die Zusammenarbeit von öffentlicher Hand und Wirtschaft in besonderer Weise erforderlich, um über erste vielversprechende Projekte hinaus eine Breitenwirkung zu erzielen.

- Exemplarisch wurden an drei Risikogruppen konkrete Lösungsansätze zur Steigerung von Sicherheit und Vertrauen in IT und Internet herausgearbeitet:
    - **Identitätsschutz:** Der Identitätsschutz als ein wesentliches Element von Sicherheit und Vertrauen in IT und Internet erfordert technische, organisatorische, rechtliche und nicht zuletzt edukative Maßnahmen. Zur Verbesserung des Identitätsschutzes durch technische Maßnahmen werden bereits erhebliche Anstrengungen unternommen. So wurden in sicherheitskritischen Bereichen, z.B. Online-Banking, in Deutschland verbesserte Authentisierungsverfahren entwickelt (iTAN, mTAN, eTAN), die im internationalen Vergleich vorbildlich sind. Weitere Fortschritte sind durch die Einführung des elektronischen Personalausweises und die Förderung von Bürgerportalen im Rahmen des Programms E-Government 2.0 zu erwarten. Auf der Ebene der Browser bieten verschiedene Anbieter kostenlose Software zur Erkennung gefälschter Webseite an. Banken und E-Commerce-Anbieter verbessern die Aufklärung ihrer Kunden und werben verstärkt für den Einsatz von Virenschutzprogrammen. Zur Information und Aufklärung der Nutzer platzieren etwa zahlreiche Anbieter und Verbände in ihren Internetangeboten an prominenter Stelle Sicherheitshinweise, etwa zum Phishing. Behörden wie das BSI oder das Bundeskriminalamt und Organisationen wie „Deutschland sicher im Netz“ oder die Arbeitsgruppe Identitätsschutz im Internet e.V. (a-i3) klären durch Informationsportale über aktuelle Gefahren und Abwehrmaßnahmen auf und bieten sogar konkrete Beratungsangebote für Betroffene. Gesetzliche Maßnahmen wirken unterstützend, etwa mit Anpassungen des Computerstrafrechts. Weitere Anstrengungen können sich auf die Erarbeitung von Verhaltensstandards für Anbieter (Sicherheit von Websites) und Nutzer (z.B. Einsatz von Virenschutz) richten, die die schwierige Balance zwischen hinreichender Sicherheit einerseits und der Vermeidung von Nutzungsbarrieren andererseits wahren.
    - **Datensicherheit**: Die Risiken und Angriffsmöglichkeiten im Bereich Datensicherheit sind vielfältig, so dass ein Bündel von Maßnahmen ergriffen werden muss. Dabei sind die Anforderungen im geschäftlichen Verkehr höher als im privaten Bereich, aber auch dort ist das Thema nicht zu vernachlässigen. Endgeräte bzw. Netzwerke müssen durch Firewalls und Virenschutz gegen Angriffe von außen geschützt sein.. Klare Zugriffsregeln verbunden mit entsprechenden technischen Zugriffsschranken können sicherstellen, dass kein Missbrauch über den Zugriff auf bewegliche Trägermedien oder durch interne Kräfte im eigenen Netzwerk erfolgt. Besonderer Schutz ist für mobile Endgeräte oder Speichermedien erforderlich, um einen unberechtigten Zugriff auf die dort gespeicherten Daten bei Abhandenkommen der Geräte zu verhindern. Auch beim Einsatz drahtloser Übertragungswege ist eine angemessene Verschlüsselung wichtig. Jede Zugriffsschutz- oder Verschlüsselungstechnologie kann nur dann wirksam schützen, wenn auch die eingesetzten Schlüssel sicher vor unbefugtem Zugriff verwahrt sind. Hier

bietet z.B. die Ablage der Schlüssel in zertifizierten Krypto-Smartcards oder Hardware-Sicherheitsmodulen die notwendige Sicherheit.

- **Jugendmedienschutz:** Vertrauen und Sicherheit in neue Medien wird langfristig nur durch ein effektives und an den Besonderheiten dieser Medien ausgerichtetes Jugendschutzsystem wachsen. Deshalb werden Anbieter auch weiterhin in kooperativer Weise mit dem Staat sowohl technische Mittel fortentwickeln, um einen besseren Kinder- und Jugendschutz zu ermöglichen, als auch durch Aufklärung und Information zur Nutzung dieser Mittel und vor allem zur Stärkung der Medienkompetenz beitragen. Dies kann nur in einem kooperativen Ansatz gelingen. Gemeinsame Plattformen wie „Deutschland sicher im Netz“ haben daher einen Schwerpunkt auf die Förderung des Kinder- und Jugendschutzes gelegt. Das im Rahmen dieser Initiative gestartete Portal „Internauten.de“ ist nur ein Beispiel, wie Kinder, aber auch Eltern und Lehrkräfte auf die Gefahren neuer Medien vorbereitet werden können. Die laufende Evaluation der geltenden Rechtslage zum Jugendmedienschutz auf Länder- und Bundesebene sollte zudem einen Beitrag dazu leisten, die Diskussion um eine Stärkung dieser Schutzmechanismen sachlich zu führen und auf tatsächlich zielführende Maßnahmen zu lenken.

Teilnehmer der Arbeitsgruppe „Sicherheit und Vertrauen in IT und Internet“:

- eBay GmbH: Dr. Stefan Groß-Selbeck (Leitung)
- Bundesministerium des Innern: Staatssekretär Dr. August Hanning
- Bundesamt für die Sicherheit in der Informationstechnik (BSI): Dr. Udo Helmbrecht
- Bundesverband Deutscher Banken e.V.: Dr. Waldemar Grudzien
- Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien e.V. (BITKOM): Dr. Mario Tobias
- Deutsche Telekom AG: Andreas Kindt
- Hewlett-Packard Deutschland GmbH: Edgar Aschenbrenner
- Microsoft Deutschland GmbH: Dorothee Belz
- Ruhr-Uni-Bochum, Horst-Görtz-Institut / Arbeitsgruppe Identitätsschutz im Internet e.V. (a-i3): Prof. Dr. Georg Borges, Prof. Dr. Jörg Schwenk
- Utimaco Safeware AG: Martin Wülfert