GEDANKEN IN STICHWORTEN:

ZU DEN LEITFRAGEN

Vorbemerkung: Grundsätzlich ist die Bereitschaft des Bundesinnenministers zu begrüßen, sich in einen Dialog mit Vertretern der Internet-Community und den in diesem Kontext zuständigen staatlichen Stellen zu den "Perspektiven deutscher Netzpolitik" und speziell mit den Fragen von "Datenschutz und Datensicherheit im Internet" zu begeben.

Die Glaubwürdigkeit eines Dialogs muß sich aber daran messen lassen, ob die diskutierten Lösungsansätze tatsächlich Ihren Weg in die Umsetzungsprozesse der politischen Willensbildung finden.

Die Abkehr von Konzepten der "inneren Sicherheit" zu einem "inneren Frieden" kann im Bereich der Sicherheitspolitik mit dem Internet exemplarisch begonnen werden, das Internet würde sich als Medium zur Neuorganisation des Verhältnisses des Staates zu seinem Bürger anbieten. Nicht der maschinenlesbare Bürger, sondern die maschinenlesbare Regierung und die Förderung plebeszitärer Elemente müssen das Leitbild sein.

Innenpolitik in einer Informationsgesellschaft muß damit beginnen, den *Bürger im Netz* in seiner Position nachhaltig zu verstehen, um die **Durchsetzung seiner Grundrechte** und die **Abwehr gegenüber demokratiefeindichen Prozessen** zu stärken.

Erste Diskussionsrunde: Herausforderungen

1. Welche Anreize können Gesellschaft/Politik/Gesetzgeber setzen, um den Datenschutz im Internet und den Selbstdatenschutz zu verbessern?

1.1 Abkehr von **anlaßunabhängigen** staatlichen Überwachungs Maßnahmen (d.h. gegen profilaktische Vorratsdatenspeicherung, KFZ-Kennzeichenerfassung, Videoüberwachung auf Demonstrationen etc.)

1.2 Symbolische und faktische Reduktion enstandener staatlicher Datenansammlungen; **Datenamnesie** zur Wiederherstellung des inneren Friedens (Kontext Vorratsdatenspeicherung etc)

1.3 Grundsätzliche Abkehr bei der Definition des Löschens staatlicher Datenbestände vom Verständniss der Handhabe "als gelöscht markiert"; Klarstellung und technische Umsetzung der tatsächlichen Vernichtung im Sinne der Entziehung der Datenbestände der technischen Rekonstruierbarkeit (insb. bei Sicherheitsbehörden). GGf. Einführung eines "**Bundesdatenlöschbeauftragten**" mit geeigneter technischer Ausstattung.

1.4 Förderung anonymer und pseudonymer Teilnahme am Internet und an Telekommunikationsdiensten; Prüfung der Erforderlichkeit entsprechender Speicherungen auch im Rahmen der gesetzlichen Pflichten, Klarstellung daß **anonyme Teilhabe** an demokratischen Prozessen ein Grundrecht ist.

1.5 **Vorbildliche Vorgehensweise** staatlicher Stellen durch **Datenbriefeinführung** und obligatorische proaktive Darlegung von Zugriffs- und Übermittlungsverfahren im Vorfeld staatlicher Datenerfassung (Melderechtswesen, Bürgerämter etc.); Förderung der Widerspruchsmöglichkeiten (Opt-In statt Opt-Out etc.).

Andy Müller-Maguhn (amm@ccc.de) für den Chaos Computer Club e.V., Postfach 64 02 36, D-10048 Berlin

2. Welche Mittel können Provider und Diensteanbieter den Bürgern an die Hand geben, um ihre Daten und ihre IT besser zu schützen (Spamfilter, Virenschutz…)?

2.1 Förderung von Verschlüsselungstechnologien; verpflichtende Einführung von **Warnhinweisen** bei unverschlüsselter Handhabe und Übermittlung Personenbezogener Daten ("Die Nutzung dieses Dienstes gefährdet Ihre Privatssphäre").

2.2 Unterstützung des Einsatzes von Verschlüsselung nicht nur für grenzüberschreitende agierende Unternehmen, sondern auch für Bürger durch entsprechende Kampagnen und Wirtschaftsförderung von **Privacy Enhancing Technology** Produkten.

2.3 **Warnungen** vor der Nutzung bestimmter Dienste, die technische bedingt kein hohes Datenschutzniveau garantieren könnten für sensitive Anwendungen (Preisgabe persönlicher Lebensumstände, finanzielle Transaktionen etc). Damit ist gleichzeitig ein Anreizsystem für Anbieter geschaffen, ein entsprechend passables Datenschutzniveau technisch zu realisieren.

3. Wie können Datensicherheit, Datensparsamkeit, Zweckbindung und Transparenz beim Umgang mit personenbezogenen Daten technisch unterstützt werden?

3.1 Berücksichtigung der entstehenden **Begehrlichkeiten** bei jedweden staatlich direkt oder indirekt geforderten bzw. geförderten Datenerhebungen. Jährliche Pflichtinformation durch Datenbrief; Prüfung der Notwendigkeit der anhaltenden Speicherung

3.2 Berücksichtigung der durch technische Realisierung und internationale Verbindlichkeiten entstehenden Gefahren, insb. bei Verpflichtungen zur Datenübermittlung, die über den Rahmen eines faktischen Bedarfs hinausgehen. **Datendiät** durch regelmässige Prüfung der **Reduktion** der Datenbestände auf die für den Zweck erforderliche Mindestmenge bzw. Definition von Verfallsdaten.

4. Wie können Datenschutz und Datensicherheit von gehosteten Angeboten (Cloud-Computing) sichergestellt werden?

4.1 Verpflichtung der Anbieter, die **Jurisdiktionen offenzulegen**, in denen die Daten der Nutzer verarbeitet werden. Gesetzliche Verpflichtung zur Aufnahme zusätzlicher Warnhinweise, wenn keine dem deutschen Recht vergleichbaren juristischen Grundlagen nach Bewertung des Bundestdatenschutzbeauftragten bestehen.

4.2 Unterstützung des Verständnisses der Benutzen, was Datenhandhabe in anderen Jurisdiktionen bedeutet durch entsprechende **vergleichende Bewertung** der rechtlichen Grundlagen im Bezug auf Datenschutz durch den Bundesdatenschutzbeauftragten.

5. Wie kann eine faire Verantwortungsverteilung zwischen Staat, Anbietern und Bürgern bei der Datensicherheit aussehen?

5.1 Staatliche Rahmenbedingungen, die eine **verpflichtende Klarstellung** für Diensteanbieter vorsehen, wer in der Verantwortung für welche Aspekte der Nutzung des Dienstes im Kontext sensitiver Daten steht.

5.2 Unterstützung des Schutzes privater Daten und der **Wahrung der digitalen Intimsphäre** durch Aufklärungskampagnen und klare Ausgrenzung spezifischer Datenbestände auch bei staatlicher Erfassung um Mißbrauch auszuschließen.

Andy Müller-Maguhn (amm@ccc.de) für den Chaos Computer Club e.V., Postfach 64 02 36, D-10048 Berlin

Zweite Diskussionsrunde:: Handlungsoptionen der Politik

1. Wie kann durch die Anpassung des Datenschutzrechts der Datenschutz im Internet gefördert werden?

1.1 Persönliche **Haftung** der Geschäftsführer von Unternehmen für **Datenverbrechen**, d.h. die unautorisierte Weitergabe oder Übermittlung von Personenbezogenen Daten an Drittstellen oder in Jurisdiktionen ohne ädequates Datenschutzniveau

1.2 **Datenbrief:** Regelmässige (jährliche) schriftliche Mittelung an die Benutzer, welche Daten in welchem Umfang auf welcher Grundlage gespeichert werden und wie der Benutzer eine Löschung bzw. Korrektur der Daten erwirken kann. Gesetzliche Grundlage für Unternehmen ab einer bestimmten Größe.

2. Welche Rollen können einer Stiftung Datenschutz zukommen?

2.1 Untersuchung und Aufklärung der Untersuchung von **Datenunfällen** und sonstigen Datenverbrechen im Kontext der Handhabe personenbezogener Daten in öffentlich transparenter Form; Klärung etwaiger Gesetzes- oder Regelungslücken zusammen mit dem Systembetreiber und den gesetzliche zuständigen Stellen

2.2 Öffentliche Untersuchung der **Vertrauenswürdigkeit** von Schutzinstrumenten und Anbietern im Bezug auf die Handhabe persönlicher und intimer Daten (Stiftung Datentest)

2.3 Konzeptionelle Untersuchung von staatlicher und privater Datenverarbeitung und Entwicklung von datensparsamen Konzepten. Förderung der Diskussion um derartige Ansätze.

3. Wie können De-Mail und elektronischer Personalausweis als Angebote für besseren Selbstdatenschutz eingesetzt werden?

3.1 De-Mail ist konzeptionell problematisch als daß gerade die Stärkung der Identifikation (und somit unter Vernachlässigung des Rechts auf Anonymität der Nutzer) von E-Mails hier durch technische Konzepte unter **zentraler staatlicher Handhabe** beantwortet wird. Dadurch wird technischer und sonstiger Mißbrauch nicht ausgeschlossen, sondern in der Wirkung potentiell Verstärkt, insb. m Kontext der Rechtswirksamkeit der elektronischen Unterschrift (Signatur).

3.2 Der Elektronische Personalausweis ist leider ein Präzdenzfall der Vermischung von staatlichen und wirtschaftlichen Interessen, der selbst als Mißbrauch staatliche erhobener Daten für privatwirtschaftliche Interessen bezeichnet werden kann (**Verstoss gegen die Zweckbindung**).

3.3 Beide Projekte zementieren ein grundsätzliches Mißverständisses im Bezug auf die Erreichung von besserer rechtsverbindlichkeit im elektronischen Marktgeschehen. **Nicht bessere Identifizierung** der Teilnehmer (Nachweis der Echtheit, daß die von Ihnen angegebenen Daten echt sind), **sondern bessere Authentifizierung** (Nachweis der Berechtigung zur Teillnahme an einem Dienst oder Bezug einer Ware oder einer Dienstleistung) sind der Schlüssel für die Risikoeingrenzung.

Andy Müller-Maguhn (amm@ccc.de) für den Chaos Computer Club e.V., Postfach 64 02 36, D-10048 Berlin

4. Welche Rolle kann das BSI übernehmen, um die Datensicherheit im öffentlichen und nicht-öffentlichen Bereich zu fördern?

4.1 Die **Interessenskonflikte** des BSI im Bezug auf die Unterstützung der öffentlichen Stellen zur Gewährleistung der technischen Sicherheit auf der einen und der Unterstützung von Ermittlungs- und anderen Sicherheitsbehörden zur forensischen und sonstigen Auswertung von Daten- und IT-Systemen **müssen zunächst strukturell ausgeräumt werden**, um die **Glaubwürdigkeit** des BSI als Beratungsinstanz für den Bürger sicherzustellen.

4.2 Insbesondere Erkenntnisse zur Einstufung höherwertiger IT-Systeme (z.B. kryptographischer Systeme) sollten vom BSI nicht nur erarbeitet, sondern auch einer breiten Öffentlichkeit zugänglich gemacht werden. Wünschenswert wäre, wenn hier nicht nur die Algorithmen und Schlüssellängen entsprechend klassifiziert würden, sondern auch die **Produkte und Dienste** die diese Algorithmen bzw. Schlüssellängen nutzen einer öffentlichen Warnung zuzuführen.

Andy Müller-Maguhn (amm@ccc.de) für den Chaos Computer Club e.V., Postfach 64 02 36, D-10048 Berlin