Münchner Kreis Fachkonferenz, 29. März 2012

Sicherheit im Internet

Diskussionsergebnisse der offenen Podiumsdiskussion

Mario Hoffmann, Fraunhofer AISEC München

Hauptpunkte:

- DRM und TPM, Deep Package Inspection
- Sicherheitsniveau der Netzinfrastruktur
- Unterschiedliche Sicherheitslevel für unterschiedliche Anwendungen
- Sicherheitsstandards, Standardisierung und Regulierung
- Ausbildung der Juristen
- Cloud und Malware, Datenschutz/Identitäten
- Datenschutzniveau
- Nutzungsrechte und Monetarisierung personenbezogener Daten
- Eigentumsrecht an persönlichen Daten
- Nutzer- und Verbraucherschutz, informationelle Selbstbestimmung

DRM und TPM

Auditorium:

Klärung der Aussage: „Daten müssen sich selbst schützen können.“

Podium:

„Perimetersicherheit reicht nicht mehr”, Daten müssen für sich selbst sicher sein; Möglicher Ansatz **Digital Rights Management** (DRM). Aber: Rechte individuell an Daten zu binden, ist nach wie vor eine Herausforderung – Ansatz **sticky policy**. **Trusted Platform Module** (TPM) ist als Technologie im Betriebssystem eine Option, aber immer noch aufwändig in der Umsetzung.

Deep Package Inspection

Auditorium:

Deep package inspection (DPI) ist ein interessanter Ansatz zur Erkennung von Angriffsszenarien, scheint aber nicht mit Datenschutzanforderungen zusammen zu passen.

Podium :

Dies ist im Kontext Sperrverfügungen zu sehen, diese greifen jedoch in den Telekommunikationsprozess (gesetzlich schwierig) ein und funktionieren nicht gut.
These: Ohne Änderungen in der Regulierung und Gesetzgebung wird man DPI nicht einsetzen können.

Was sich in Zukunft in der Gesetzgebung ändert, bleibt abzuwarten? → **Netzneutralität**

Sicherheitsniveau der Netzinfrastruktur

Auditorium:

Inwiefern lassen sich die Telekommunikationsanbieter hinsichtlich des **Sicherheitsniveaus** im Netz mehr in die Pflicht zu nehmen?

Podium :

- Telko-Dienstleister sind in der Pflicht für ein **Mindestsicherheitsniveau**
- **Transparente Sicherheitsangebote**, die Kunden dazu buchen können
- Provider sind verpflichtet, in die Pakete reinzuschauen, um die Verarbeitung von bestimmten Inhalten zu unterbinden

Telkos bieten bereits **Sicherheitsdienstleistungen** an. Der Anwender entscheidet letztlich, was dann konkret kontrolliert werden soll. Aber: Security kostet natürlich Geld. Die Balance zwischen Incentive und Regulierung ist daher wichtig. Deutschland ist international auf einem guten Weg, Sicherheitsdienstleistung anzubieten.

Steuererleichterungen sind in diesem Zusammenhang jedoch nicht vorgesehen. Überzeugende **Geschäftsmodelle** sind für den Wettbewerb der bessere Weg, Sicherheitsdienstleistungen voranzubringen.

Ein Großteil der Netzinfrastruktur wird nicht mehr in Europa hergestellt. **Technologische Souveränität** wäre hier wünschenswert. Aus Cybersicherheitssicht sollen diese Kompetenzen wieder aufgebaut werden.

Unterschiedliche Sicherheitslevel für unterschiedliche Anwendungen

Auditorium:

Es wird sehr viel getan, um die Sicherheit im Internet zu erhöhen. Aber **absolute Sicherheit** ist nicht möglich. Muss man denn alle Informationsflüsse höchsten Sicherheitsanforderungen unterstellen? Für viele Anwendungen genügen doch sicher auch niedrigere Sicherheitslevel, oder?

Podium:

Das passiert bereits: Deutsche Banken **differenzieren** z.B. sehr sorgfältig zwischen vertrauenswürdigen und für das eigene Wirtschaften essentiellen Daten.

Sicherheitsstandards

Auditorium:

Sicherheit ist sehr aufwändig und heterogen. GSM ist doch ein gutes Beispiel für einen gemeinsam entwickelten Standard. Warum ist das nicht im Sicherheitskontext möglich (gewesen)?

Podium:

Standards entstehen durch die gemeinsame Arbeit von Unternehmen. Der Regulator hat hier nur geringe Einflussmöglichkeiten. Für DE-Mail sind beispielsweise einige Standards eingeflossen, andere mussten und müssen noch entwickelt werden

Bei GSM gab es beispielsweise nur wenige Player; das heutige Feld, z.B. bei Cloud, ist wesentlich komplexer. **Zertifizierungen** sind bei Cloud aber ein möglicher Ansatz, zumindest für einen Teil des Marktes.

Standardisierung bei GSM hat vor der Digitalisierung des Marktes begonnen. Im Gegensatz dazu hat dies bei eMail/DE-Mail erst sehr spät begonnen. Frage: Wie sieht die Welt in 10-15 Jahren aus? Da müssten jetzt Anstrengungen unternommen werden. **Zukunftsorientierte Standardisierung** wäre ein erfolgversprechender Ansatz.

Standardisierung und Regulierung

Auditorium:

Standardisierung ist nicht die alleinige Lösung. Absicherung der Netze könnte Geschäftsmodell der Carrier sein als zusätzliche Leistung. Was muss in der Regulierung gemacht werden, um solche Geschäftsmodelle zu unterstützen?

Podium:

Regulierung in Deutschland z.B. im Datenschutz wurde vor 10 Jahren kritisch und als einengend gesehen. Heutzutage muss man feststellen, dass die damaligen Befürchtungen bei den gegenwärtigen Datenmengen nun real geworden sind. Antiquierte, hemmende Regulierungen sind jedoch zu identifizieren.

Einwurf: Einen Anwalt konsultieren zu müssen, um ein Startup wegen der AGBs abzusichern, kann nicht sein. „Das muss einfacher gehen!“

Das **Europäische Datenschutzrecht** wird gegenwärtig novelliert. Ist das Deutsche Datenschutzrecht hier noch zeitgemäß? Nein, auch hier muss gründlich nachgebessert werden. Das **Persönlichkeitsrecht** muss wieder gestärkt werden. Zudem muss besser differenziert werden.

Ausbildung der Juristen

Auditorium:

Inwieweit sind unsere Juristen mit den Themen vertraut? Gibt es Ausbildungsbedarf?

Podium:

Bei Spezialzuständigkeiten hat sich einiges getan. Es gibt beispielsweise Schwerpunktstaatsanwaltschaften und spezialisierte Kanzleien. Ein guter Anfang ist gemacht.

Cloud und Malware

Auditorium:

Zurück zu Cloud: Inwiefern befällt heute schon **Malware** von virtuellen Servern die realen und wer haftet dann?

Podium:

Die üblichen AGBs schließen **Haftungen** in jeglicher Form in der Regel aus.

Die Verteilung von Verantwortlichkeiten ist hier kritisch zu sehen. Kunden sind vielfach nicht bereit, in die **öffentliche Cloud** zu gehen. Solange Cloud auf eine gewisse Domäne, wie SAP, beschränkt ist, kann **Vertrauen** entstehen. Es sind aber noch Forschungsfragen, wie **Zertifizierungen**, zu meistern.

Die meisten Unternehmen sehen noch nicht klar → Private, Public, Hybrid? **Branchenspezifische Clouds** sind eine weitere mögliche Ausprägung. In der **Cloud Security Alliance** werden diese Fragen diskutiert und in Dokumente gegossen. Von dort sind Standardisierungsimpulse möglich. Hier gibt es einen US-Schwerpunkt, wo von Europäischer Seite noch aufgeschlossen werden muss.

Cloud und Datenschutz/Identitäten

Auditorium:

These: Harmonisierte Cloud-Infrastrukturen in Europa sind notwendig, um die **Datenschutzproblematik** zu adressieren. Sind ergänzende regulatorische Maßnahmen notwendig?

Podium:

Das **BMWi-Programm Trusted Cloud** adressiert teilweise diese Fragestellungen. Das BSI hat ein Papier zu **Cloud-Sicherheitsanforderungen** veröffentlicht. Zertifizierungen sind eine weitere Maßnahme, die gegenwärtig untersucht wird. Diese Dinge sollen aber nur Hilfestellungen für Unternehmen sein.

Transaktionssicherheit in der Cloud sollte noch mit **Identitätsansätzen** verheiratet werden.

Datenschutzniveau

Auditorium:

Welches **Datenschutzniveau** brauchen wir? Welche Position bezieht die **ENISA**?

Podium:

ENISA ist eine Agentur, die die Artikel 29 Arbeitsgruppe und nationale Behörden unterstützt. Sie legt jedoch dem Europäischen Parlament oder der Kommission keine direkten Vorlagen vor, die beispielsweise zu Direktiven weiterentwickelt werden.

Nutzungsrechte und Monetarisierung personenbezogener Daten

Auditorium:

“**Nutzungsrechte** an meinen Daten” – Wie lässt sich das technisch adressieren und umsetzen?

Podium:

Stichwort: **Monetarisierung** von personenbezogen Daten. Wenn in Datenschutzbestimmungen entsprechend transparent gemacht wird, was mit Daten passieren kann, kann das zum Wettbewerbsvorteil werden. Wir könnten wissen, dass wir heutzutage bei vielen Anwendungen mit unseren Daten bezahle → z.B. Location Based Services, d.h. **Dienstleistung gegen Daten**.

Nachfrage: Aber was ist denn in 10 Jahren? These: Bedrohungen finden mehr und mehr auf der Applikationsebene statt. Die Geschäftsmodelle von Facebook und Google sind hierbei problematisch. **Transparenz und Privacy** sind treibende Themen.

Eigentumsrecht an persönlichen Daten

Auditorium:

Eigentumsrecht an persönlichen Daten. Ist es juristisch denkbar, dass wir so etwas bekommen und durchsetzen können?

Hinweis: Viele Datenerfasser um uns herum haben viele Auflagen, wie Ärzte, Versicherungen, Polizei, Arbeitgeber. Diese Daten werden nicht veröffentlicht. Das sollte ein Vorbild sein, um auch eBusiness-Transaktionen besser zu regulieren. Das sollte in Internet-Recht umgesetzt werden.

Podium:

Das Konzept “**Eigentumsrecht**” passt in diesem Zusammenhang nicht gut. Das Interesse an Kontrolle ist jedoch wichtig. Es erfordert neue Konzepte, da das strenge Eigentumsrecht der **Freiheit des Informationsaustauschs** entgegen spräche.

Wie sind juristische Fragen wie das “Eigentumsrecht” technisch auszugestalten? Das Gleiche gilt für “Das Recht auf vergessen”, das technisch kaum umzusetzen ist..

Die **Europäische Datenschutzdirektive** birgt sehr gute wichtige Ansätze, die im Detail juristisch gedeutet und technisch umgesetzt werden. Das funktioniert jedoch nicht von heute auf morgen.

Eigentumsrecht an Daten ist in der Tat nicht realisierbar. Zurückverlangen, Rückgaberecht von einmal herausgegebenen Daten ist nicht realistisch. **Unterschiedliche Grundrechte** müssen hier abgewogen werden; sie sind nicht immer konflikt- und widerspruchsfrei. Neue Konstruktionen sind sicher erforderlich.

Nutzer- und Verbraucherschutz, informationelle Selbstbestimmung

Auditorium:

Brauchen wir einen **Computer-/Internetführerschein**? Der Nutzer kann nicht wissen, wo und warum welche Informationen über sie gespeichert sind. Es muss der **Nutzer- und Verbraucherschutz** verbessert werden. Das ist eine gesellschaftliche Aufgabe, der Staat sollte diese Schutzfunktion ausfüllen.

Beispiel: **Informationelle Selbstbestimmung** könnte in der Diskussion “Eigentum am Bild” konkretisiert werden. Mit Hilfe des neuen Personalausweises könnten hier Zustimmungsprozesse etabliert werden.

Podium:

Juristisch ist das ein sehr **komplizierter Interessenausgleich**. Daten müssen prinzipiell frei sein, Urheberrecht und Datenschutzrecht schränken dies dann entsprechend ein. Das Recht am Bild ist wieder separat zu betrachten.

Die gesamtgesellschaftliche Entwicklung beeinflusst durch neue Technologien eröffnet weitere Perspektiven. Normen und Regularien können hier nur flankierend sein. Nicht alles, was deutsch wünschenswert wäre, lässt sich global durchsetzen.

Hinweis aus dem Auditorium: Aus der juristischen Praxis: Selbst wenn ich juristisch einen Titel erwirke, lassen sich viele Urteile nicht durchsetzen. **Im weltweiten Datenaustausch lassen sich z.B. Löschungsansprüche oft gar nicht durchsetzen.**