Technische Hintergründe für das rechtliche Handeln im Internet

Rene Mayrhofer

Internet-Recht befindet sich grundsätzlich an der Schnittstelle zwischen Gesetzgebung und Technik. Wie an vielen Schnittstellen gibt es auch hier Schwierigkeiten zu überwinden, und zwar nicht nur in der Findung gemeinsamer Ziele, Arbeitsgruppen und schlussendlich Lösungen, sondern vor allem im gegenseitigen Verständnis der den jeweils anderen Bereich betreffenden Probleme. Dieser Vortrag soll die technischen Hintergründe einiger aktueller Themen an dieser Schnittstelle allgemein verständlich näher bringen. Die Auswahl an Themen, welche aus technischer Sicht einer Klärung durch die Gesetzgebung bedürfen bzw. derer, die durch neue Gesetze die Entwicklung neuer technischer Systeme erfordern, ist derzeit kaum mehr überschaubar und wächst weiter. Daher erfolgt in diesem Vortrag eine Konzentration auf die technischen Grundlagen für viele dieser Themen sowie auf eine kleine Auswahl von Themen, die von allgemeinem, auch öffentlichem bzw. gesellschaftlichem Interesse sind. Konkret werden die folgenden Themen angesprochen:

- **Grundlagen aus der Kryptographie**: Das wissenschaftliche Feld der Kryptographie, also der Lehre der Geheimschriften, liefert die notwendigen Methoden zur Umsetzung verschiedener Forderungen an sichere Systeme. Diese Forderungen sind üblicherweise *Vertraulichkeit*, *Integrität*, *Authentizität* und *Verbindlichkeit*. Zur Behandlung dieser Forderungen stehen im Wesentlichen die Techniken der *Verschlüsselung* und der *digitalen Signatur* zur Verfügung.
- **Qualifizierte Signatur**: Zur Erstellung von digitalen Signaturen die ähnliche Beweiskraft wie die handschriftliche Signatur besitzen sind zusätzlich zu technischen Erweiterungen auch organisatorische Strukturen nötig. Die nötigen technischen Änderungen betreffen hauptsächlich die sichere Speicherung des Schlüssels, der zur Erstellung von digitalen Signaturen immer nötig ist, während die organisatorischen Strukturen für eine eindeutige Bindung zwischen einer natürlichen oder juristischen Person (oder auch eines Computer-Systems) und eben diesen digitalen Schlüsseln sorgen.
- **Sichere Übermittlung von Emails und Dokumenten**: Die digitale Übermittlung von Information ist das erklärte Ziel des Internet selbst, und Email ist der am meisten verwendete Dienst zur direkten Übermittlung zwischen Personen. Allerdings wird die derzeit überwiegende Mehrheit aller Emails komplett ungesichert übertragen und weder vor Fälschung der Empfänger, Absender oder des Inhalts noch gegen Mitlesen durch Dritte geschützt. Mit aktuell verwendeten Email-Programmen lässt sich jedoch mit geringem Aufwand der Versand und Empfang von nach derzeitigen Standards gut gesicherten Emails erreichen.
- **Aktuelle Probleme in der Umsetzung**: Obwohl die entsprechenden technischen und organisatorischen Maßnahmen zur Sicherung von Systemen weitläufig bekannt und verfügbar sind, ist deren Beherrschung in praktischen Implementierungen nach wie vor schwierig. So werden oft Komponenten des ursprünglichen Konzepts bei der späteren Implementierung vertagt oder komplett entfernt, ohne eine erneute Betrachtung des Gesamtsystems in Bezug auf diese Auslassung zu unternehmen. Dadurch werden oft kritische Teile vernachlässigt, die, obwohl sie scheinbar nur ein Detail darstellen, durch ihr Fehlen die Gesamtsicherheit des schließlich implementierten Systems zunichte machen.
- **Digital Rights Management**: Zur Absicherung gegen missbräuchliche Verwendung elektronischer Dokumente werden derzeit so genannte DRM-Systeme in verschiedenen Ausprägungen eingeführt. Das Grundprinzip dabei ist jeweils eine Bindung der Dateien, also z.B. Musik- oder Filmdateien, an eine geographische Region oder an einzelne Computersysteme. Mittels DRM können Rechteinhaber die erlaubten Verwendungsarten detailliert festlegen und in der Datei selbst verankern.
- **Peer-to-Peer Systeme**: Peer-to-Peer, oft auch durch „P2P“ abgekürzt, bedeutet, dass die miteinander kommunizierenden Systeme gleichberechtigte Teilnehmer (sogenannte „Peers“) sind. Als Abkehr von der bekannten Trennung in Server und Client kann jeder Teilnehmer sowohl Dienste anbieten – in der Rolle eines klassischen Servers – als auch Dienste anderer Teilnehmer verwenden – in der Rolle eines Clients. Die auch durch Medienarbeit bekannteste Anwendung von

Peer-to-Peer Systemen ist der Dateiaustausch, bei dem durch entsprechende Programme ein direkter Zugriff auf die Dateien anderer Computersysteme und entsprechende Suchmöglichkeiten geschaffen werden, doch das Konzept ist vielseitiger und wird u.a. auch für Dienste wie Internet-Telefonie eingesetzt. Durch die Weiterentwicklung der Peer-to-Peer Konzepte entstanden bereits drei Generationen von Systemen, die jeweils unterschiedliche Daten zugänglich machen bzw. verschieden resistent gegen Strafverfolgung oder staatliche Zensur sind. Aktuellste Generationen von Peer-to-Peer Systemen verbergen zunehmend Daten wie die eindeutigen Internet-Adressen der jeweiligen Teilnehmer, die zur Identifizierung der Nutzer dienen könnten.

- **Spam**: Da Email einer der derzeit wichtigsten Dienste im Internet ist, besteht auch ein hohes Potenzial für Missbrauch. Neben Würmern, also schadhaften Programmen, die sich automatisch verbreiten, werden auch unaufgeforderte Werbebotschaften (oft als „Spam“ bezeichnet) immer häufiger per Email versandt und verursachen dadurch Aufwände in kaum schätzbarer Höhe. Zur Identifizierung der Absender solcher unerwünschter Emails sind im sogenannten Email-Header, also dem normalerweise vom Mailprogramm nicht angezeigten Vorspann, oft eindeutige Informationen enthalten, die zur Rückverfolgung verwendet werden können. Zur automatischen Unterdrückung von unerwünschten Emails, also Anti-Viren und Anti-Spam Maßnahmen, sind diese Informationen ebenfalls von großer Bedeutung, jedoch erfolgt zeitgemäße automatische Filterung auf verschiedenen Ebenen.

Diese Themen stellen eine subjektive Auswahl dar, sollten jedoch die derzeit am stärksten – auch durch die Tagespresse – diskutierten Gebiete abdecken. Der Vortrag ist auf Zuhörer ohne technischem Detailwissen ausgerichtet, Erfahrung im Umgang mit Computersystemen, also z.B. mit Webbrowsern und Emailprogrammen, wird jedoch angenommen.