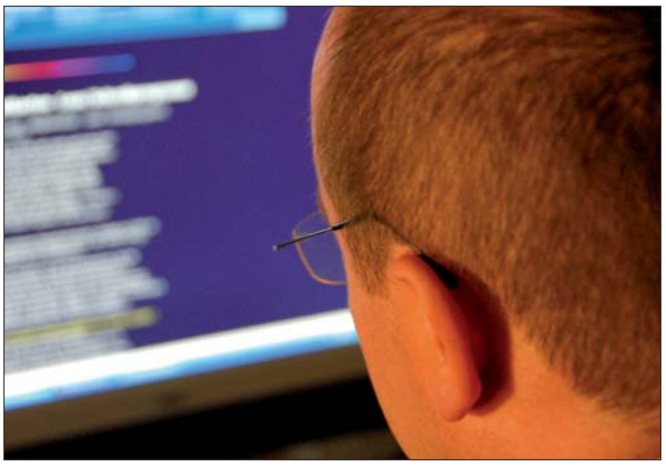
Zukunftsweisende Entwicklungen

Bei der D.A.CH Security 2007 in Klagenfurt haben Wissenschaftler neue Forschungsergebnisse zur Informationssicherheit vorgestellt.

Dass man sich im Internet anonym bewegen kann, glauben nur mehr wenige – man hinterlässt bei allen Vorgängen Spuren im Netz, die zu einem Benutzerprofil zusammengesetzt werden können. Suchmaschinen können ein Beispiel dafür sein, allein schon von den gestellten Anfragen her.

Google beispielsweise, das in Deutschland einen Marktanteil von etwa 80 Prozent der an Suchmaschinen gerichteten Anfragen hält (bei weltweit über 200 Millionen Suchanfragen pro Tag), kann als Trend-O-Meter der Gesellschaft bezeichnet werden. Aus der unter *google.com/press/zeitgeist.html* zur Verfügung gestellten Liste der Häufigkeit der Anfragen kann ersehen werden, welche Probleme die Menschen zu einem bestimmten Zeitpunkt bewegen. Nach den Anschlägen des 11. Septembers 2001 beispielsweise waren die meist angefragten Suchworte Pentagon und Osama bin Laden – auch ein Ansteigen beim Suchbegriff Nostradamus, dem Propheten des Weltuntergangs, war zu verzeichnen.

Weniger bekannt ist, und darauf hat Christian Russ (Universität Klagenfurt) hingewiesen, dass bei Anfragen in Suchmaschinen eine Benutzer-ID in Form eines Daten-Cookies am Rechner des Anfragenden abgelegt wird. Mit den vielfältigen anderen Diensten, die über reine Suchfunktionen hinaus angeboten werden, eröffnen sich Möglichkeiten eines Data-Minings, die letztlich ein Bild über den User ergeben. Aus der Auswertung dessen, was gesucht wird, wie häufig gesucht wird und wie man mit dem Ergebnis zufrieden ist, ergeben sich persönliche Interessen, über Mail-, Chat- und Weblogdienste kann in Erfahrung gebracht werden, welche Meinungen jemand vertritt, über die Nutzung von Satellitenaufnahmen, welche Weltgegenden ihn besonders interessieren.



Alle Vorgänge im Internet hinterlassen Spuren im Netz, die zu einem Benutzerprofil zusammengesetzt werden können.

Über Bildtauschtools verschickt und erhält man persönliche Bilder, und letztlich können manche Dienste nur genutzt werden, wenn beim Betreiber ein persönliches Geldkonto eingerichtet wird. Als Schutzmaßnahme empfiehlt Russ, Vorsicht und gesundes Misstrauen gegenüber Browsererweiterungen und Softwareangeboten walten zu lassen, in Online-Diensten keine Personalisierung zu nutzen, aktive Inhalte *(Active X, JavaSkript, Java, Flash)* einzuschränken sowie Administrator- und Standardnutzerbereich voneinander zu trennen. Cookies und Formulareinträge mit Autoausfüllmechanismus sollten gelöscht werden. Wer ein Übriges tun will, kann Anfragen über einen Mediatorservice durchführen – er muss dann allerdings wieder dem Mediator vertrauen.

Bewertungsprofile. Unter *meinprof.de* und *meinprof.at* tauchen im Internet Bewertungsprofile für Hochschullehrer auf. Ähnliches gibt es für Rechtsanwälte, Ärzte und Köche; auch Behörden können nach bestimmten Gesichtspunkten „gerankt" werden.

Der Frage, ob dadurch datenschutzrechtlich relevante Aussagen getroffen werden, ist Rechtsanwalt Dr. Lambert Grosskopf (Universität Bremen) nachgegangen, indem er das Grundrecht der Meinungsfreiheit dem Grundrecht auf Schutz personenbezogener Daten der Betroffenen gegenübergestellt hat. Allerdings können die wesentlichen Daten der Betroffenen wie Name, Titel, Schwerpunkt und Fachrichtung frei zugänglichen Quellen entnommen werden, sodass durch die Verwendung dieser Daten schutzwürdige Interessen nicht verletzt werden (§ 29 Abs 1 BDSG, § 8 Abs 2 DSG).

Die darauf aufbauende Bewertung ist durch die Freiheit der Meinungsäußerung gedeckt und findet wie im Medienwesen ihre Grenze nur dort, wo Beleidigungen erfolgen (Schmähkritik). „Die Regulierung von Meinungsäußerung fällt nicht in den Schutzzweck des Datenschutzes," betonte Grosskopf. Dem Recht, Auskunft über die Herkunft der Daten

D.A.CH SECURITY

Ziel der seit 2003 jährlich stattfindenden *D.A.CH Security* ist es, eine interdisziplinäre Übersicht zum aktuellen Stand der IT-Sicherheit in Industrie, Dienstleistung, Verwaltung und Wissenschaft zu geben in Deutschland, Österreich und der Schweiz.

Insbesondere sollen Aspekte aus den Bereichen Forschung und Entwicklung, Lehre, Aus- und Weiterbildung vorgestellt, relevante Anwendungen aufgezeigt sowie neue Technologien und daraus resultierende Produktentwicklungen konzeptionell dargestellt werden.

Die von Univ.-Prof. Dr. Patrick Horster geleitete Forschungsgruppe Systemsicherheit der Alpen-Adria-Universität Klagenfurt *(www.syssec.at)* veranstaltet jährlich auch den Österreichischen IT-Sicherheitstag, der, zum vierten Mal, am 7. November 2007 in Klagenfurt stattfinden wird.

FOTO: EGON WEISSHEIMER

Christian Russ: „Cookies und Formulareinträge mit Autoausfüllmechanismus sollten gelöscht werden."

zu verlangen (§ 34 Abs 1 BDSG, § 26 Abs 1 DSG) stehen nach deutschem Recht der Anspruch auf Wahrung des Geschäftsgeheimnisses des Betreibers des Bewertungsportals gegenüber, nach dem DSG seine überwiegenden berechtigten Interessen (§ 26 Abs 2 DSG), weil wohl kaum Bewertungen abgegeben werden, wenn in Erfahrung gebracht werden kann, von wem diese stammen. Für den Bewertenden gilt, dass jeder für seine eigenen Handlungen haftet; der Betreiber eines derartigen Portals haftet dann, wenn er von der erfolgten Beleidigung Kenntnis erhält. Eine bloße Distanzierung reicht nicht aus; der betreffende Inhalt muss tatsächlich gelöscht werden.

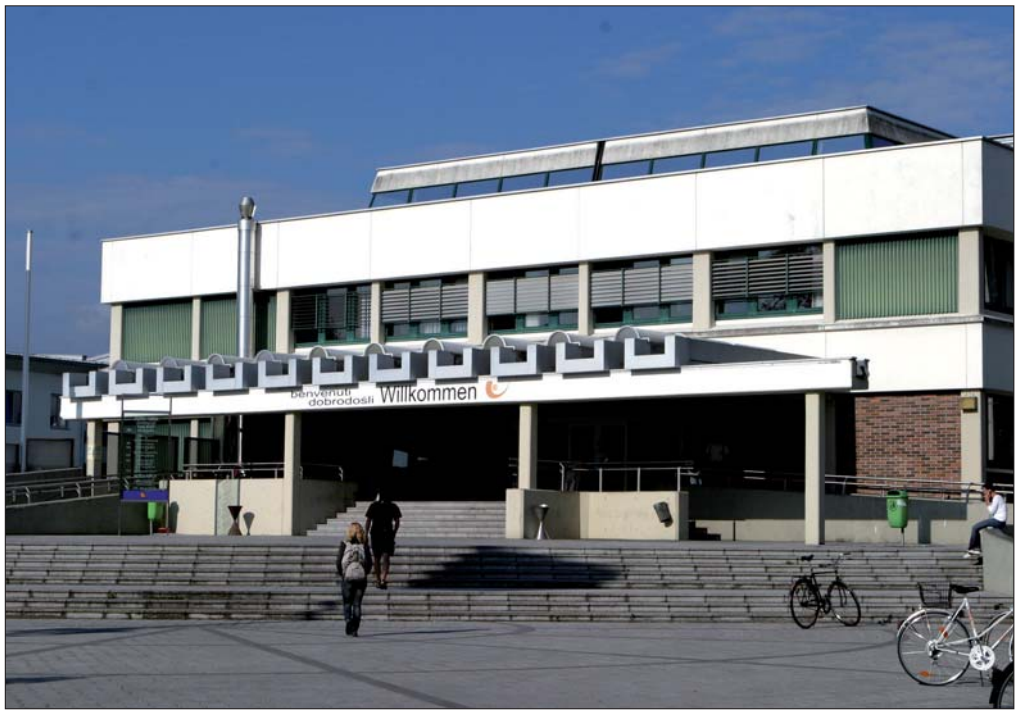
M-Commerce. Nach dem E-Commerce-Gesetz treffen den Diensteanbieter Transparenzpflichten (§ 5 ECG) und Informationspflichten für Vertragsabschlüsse (§ 9); er hat die Vertragsbestimmungen und die „Allgemeinen Geschäftsbedingungen" dem Nutzer so zur Verfügung zu stellen, dass er sie speichern und wiedergeben kann (§ 11).

Laut Nils Krüger vom „Oldenburger Forschungs- und Entwicklungsinstitut für Informatik-Werkzeuge und -Systeme" (OFFIS) stellt sich beim Handel mit Internet-Shops über mobile Geräte (PDA, Mobiltelefone mit Internetfunktion) das Problem, dass zum einen die Displays für die Anzeige der Daten nicht ausreichend groß sind, der auf diesen Geräten verfügbare Speicherplatz nicht ausreicht und die Übertragungsgeschwindigkeit zu gering ist. Als Ausweg wurde die Hinterlegung dieser Texte bei einem Treuhänder oder ihre Ausgabe in sprachlicher Form zur Diskussion gestellt.

Notfalldaten. Bei einem medizinischen Notfall werden zur Erstversorgung möglichst rasch Daten des Betroffenen benötigt, etwa über seine Blutgruppe, Rhesusfaktor, Allergien, Krankheiten wie Diabetes oder Herzerkrankungen, über Schrittmacher, Transplantate, verordnete Medikamente. Diese Gesundheitsdaten sind zum einen sensibel (§ 4 Z 2 DSG) und demgemäß entsprechend gesichert zu verwenden, andererseits sollen sie rasch zur Verfügung stehen. Ferner müssen sie eindeutig dem Betroffenen zugeordnet werden können, was auf Schwierigkeiten stößt, wenn beispielsweise ein Unfallopfer nicht ansprechbar ist.

Die im Jahr 2005 von den Sozialversicherungsträgern ausgestellten 8,2 Millionen E-Cards ermöglichen zwar noch keine Authentifizierung des Inhabers, da noch ein biometrisches Merkmal für die Zuordnung zu einer Person fehlt. Ob dieses Merkmal das Lichtbild des Versicherten sein wird oder ein Fingerabdruck, ist derzeit Gegenstand von Beratungen; ab 2010 soll es zur Verfügung stehen, berichtete Martina Heiligenbrunner von der FH Technikum Kärnten.

FOTO: KURT HICKISCH



Universität Klagenfurt: Seit 2003 findet hier jährlich die „D.A.CH Security“ statt.

Bis dahin könnte ein biometrisches Merkmal in ein Informationssystem eingespeichert und vom behandelnden Arzt verifiziert werden. Ansonsten kann die E-Card eine sichere Datenübertragung gewährleisten, wenn die auf der Karte enthaltene Funktion der Bürgerkarte aktiviert wird. Dies kann kostenlos über das Internet durchgeführt werden und bewirkt eine über die (eindeutige) ZMR-Zahl des Melderegisters erfolgende Personenbindung und ermöglich eine Verschlüsselung von Daten sowie auch die digitale Signatur elektronischer Dokumente in Form der Verwaltungssignatur, die nach der Verwaltungssignaturverordnung (VerwSigV) bei Bürgerkartenanwendungen bis 31. Dezember 2007 der sicheren Signatur gleichgestellt ist.

Die gesetzliche Grundlage für den Austausch von Gesundheitsdaten bildet das Gesundheitsreformgesetz 2005, BGBl I 2004/179, das bei der Übermittlung von Gesundheitsdaten auf elektronischem Weg deren Verschlüsselung fordert. Die Integrität der Daten muss durch digitale Signatur sichergestellt werden.

Im Rahmen des Projekt *CANIS (Carinthian-Notarzt-System; www.cti.ac.at/canis)* wurde die Anwendung der E-Card-Funktionalitäten in der Praxis untersucht und analysiert. Zu diesem Zweck wurden auf freiwilliger Basis Gesundheitsdaten von Patienten in ein Gesundheitssystem eingespeichert.

In der Anwendung wurden die E-Cards sowohl des Betroffenen als auch des Notarztes mit Kartenlesern über die mobilen Endgeräte (Tablet-PC, PDA mit integriertem Kartenleser) eingesetzt und es wurde dadurch eine sichere End-to-End-Verschlüsselung der Daten erreicht. Das über Spracherkennung verfasste Notarztprotokoll wurde mit der digitalen Signatur des Arztes unterfertigt. Die wechselseitige Datenübermittlung zwischen Notarzt und Informationssystem (Spital) erfolgte über GPS oder UMTS, und es hat sich gezeigt, dass auf der Basis der E-Card sowohl eine gesetzeskonforme Übermittlung von Gesundheitsdaten als auch eine Steigerung der Effektivität in der medizinischen Versorgung am Unfallort und bei der Aufnahme im Krankenhaus erreicht werden konnte.

Wasserzeichen. Es ist technisch möglich, digitale Audio-, Bild- oder Videodateien unter nicht merkbarer Einbuße an Qualität und gleichzeitig unwiderruflich mit einem individuell vergebenen Wasserzeichen zu versehen, was die Rückführbarkeit eines Werkes etwa auf seinen Urheber oder den berechtigten Nutzer ermöglicht. Während *Digital Rights Management* eine – mitunter mit Problemen behaftete – technische Schranke der Kopierbarkeit darstellt, ist das Wasserzeichen eine Art psychologischer Kopierschutz, ohne dass die technische Nutzung des Mediums beeinträchtigt ist.

Derartige Wasserzeichen können an Hand ihrer Kriterien automatisiert gesucht und verfolgt werden, indem beispielsweise Verbreitungswege wie etwa Tauschbörsen beobachtet werden.

Digitale Unterschrift. Die Handschrift ist ein verhaltensbasiertes biometrisches Merkmal; eine Unterschrift wird sowohl in der analogen als auch in der digitalen Kommunikation angewendet. Im digitalen Umfeld werden zunehmend mobile Stift-basierte Eingabegeräte verwendet – auch für handschriftliche Notizen. Die Handschrifterkennung beruht darauf, dass in bestimmten kleinen Zeitabschnitten (Abtastrate) die horizontale und vertikale Stiftposition gemessen werden, ferner der Druck, der auf den Sensor ausgeübt wird, und bei manchen Geräten auch die Höhen- und Seitenwinkel des Stiftes zur Schreiboberfläche. Laut Andrea Oermann (Universität Magdeburg) können die Erkenntnisse auch in der Forensik zur Prüfung der Echtheit digital abgegebener Handschriften verwendet werden.

Trends. Die breite Palette der etwa 50 zumeist parallel in zwei Hörsälen abgehaltenen Vorträge zeigte die Schwerpunkte künftiger praktischer Einsätze der Informationstechnologie auf. Die wissenschaftliche Forschung konzentriert sich demnach auf E-Health, berührungslose Identifikation (RFID), E-Government, sichere Systeme und Übertragungswege sowie den Schutz der Privatsphäre. Die von etwa 100 Teilnehmern besuchte Arbeitskonferenz am 12. und 13. Juni 2007 in der Alpen-Adria-Universität Klagenfurt wurde von Univ.-Prof. Dr. Patrick Horster, dem Vorsitzenden des Programmkomitees, eröffnet. Die Vorträge sind in einem Buch zusammengefasst. Dieser Tagungsband und die von den vorherigen Tagungen sind im Buchhandel erhältlich.

Kurt Hickisch

FOTO: KURT HICKISCH