Hans G. Zeger[1],

Sicherheit in der Informationstechnik - die neuen Herausforderungen

Betreiber von Onlinesystemen vernachlässigen Aufklärungs- und Hilfepflicht gegenüber den Benutzern - PET Techniken müssen zur Förderung der Privatsphäre forciert werden - Privacy Statements müssen das Versagen staatlichen Datenschutzes ausgleichen - laufendes Monitoring und Rating durch unabhängige Dritte müssen vertrauenswürdigen Betrieb von Onlinesystemen sicherstellen - im internationalen Online-Datenverkehr müssen EU-Bürger die Sicherheit haben, EU-Datenschutz zu geniessen - die informationstechnische Nutzung und Ausbeutung biometrischer Merkmale ist zurückzudrängen

HILFEPFLICHT DER ONLINEBETREIBER

Wenn Sie als Betreiber eines Onlinesystems, sei dies Telebanking, Online-Shoping oder ein Online-Chatservice, morgens aufstehen, haben Sie sich schon gefragt: Was habe ich bisher für die Sicherheit meiner Benutzer getan? Was kann ich heute für deren Sicheheit machen?

Oder fragen Sie sich bloß: Wie schütze ich mein System vor Angriffen? Wieviel Hacker- und DOS-Attacken werde ich heute abwehren müssen? Wie oft wird mich das Betriebssystem wieder in Stich lassen?

Vermutlich werden Sie sich bloß letztere Fragen stellen. Im Zeitalter isolierter Systeme war dies auch ausreichend, nicht jedoch heute.

Im Telebanking oder Onlineshopping werden Unmengen von Informationen zwischen ihrem - relativ sicheren - Systemen und einem von dem Konsumenten fundamental unverstandenen System hin und her transportiert.

Hilfestellngen und Aufklärungspflichten beschränken sich meist in allgemeinen Floskeln von Werbebroschüren, wie "sorgfältige Verwahrung von Passwörtern", "aufpassen" oder "PIN-Code und TAN-Code getrennt aufzubewahren".

Tatsächlich erhält jeder Online-Betreiber bei jedem Anmeldeversuch detaillierte Informationen, welcher Benutzer, welches System sich anmeldet, ob dieses überhaupt geeignet ist oder ob über dem benutzten Serviceprovider negative Sicherheitserfahrungen vorliegen.

Es ist verantwortungslos, den Menschen eine 128-bit-SSL Verschlüsselung vorzugaukeln und gleichzeitig zu protokollieren, dass das eingesetzte System des Konsumenten das überhaupt nicht kann!

In Deutschland werden gerade die Aufklärungspflichten der Banken gegenüber den Kunden verschärft, in Österreich derzeit bloß die Überwachungsmöglichkeiten!

BEDEUTUNG VON PET - TECHNIKEN

Privacy Enhanced Technices (PET) stellen eine wertvolle Ergänzung zur persönlichen Sicherung der Privatshäre dar. Es können dies

---

[1] Der Autor ist Obmann der "ARGE DATEN", Geschäftsführer der "e-commerce monitoring GmbH" und Architekt von e-rating.at, einem komplexen e-commerce-monitoring system. Weitere Informationen http://www.zeger.at

Verschlüsselungstechniken sein, Anonymisierungstechniken, aber auch Techniken die zu verbesserter Transparenz in der Internet-Nutzung führen. Sinnvoll wären auch Systeme und Produkte, die das Aufspühren von Benutzern (Usertracking) oder das Erzeugen von Interessensprofilen erschweren.

Warum werden heute praktisch nur Brwoser eingesetzt, die die Benutzer zu einem fast blinden Navigieren in der Internetlandschaft zwingen? Es gibt auch alternative Browser, die die Orientierung auf der virtuellen Internetlandkarte graphisch unterstützen. Warum wird bei den neuen Browser-Releases von MICROSOFT und NETSCAPE das hunderste Plugin integriert, der x-te Cookie- und Active-X-Manager, aber kein einziges Feature, dass die Benutzerorientierung erhöht?

PET-Techniken sind jedoch nicht für sich allein marktfähig, es ist dem einzelnen Benutzer nicht zuzumuten, aus der Fülle von Programmen und Techniken die jeweils besten für sich auszusuchen. Es bedarf daher der begleitenden Förderung und Unterstützung durch die öffentliche Hand, etwa durch Neuorientierung der Ausschreibungen zur IT-Technik, die den Einsatz von PET-Instrumenten zwingend vorschreiben.

SINN VON PRIVACY STATMENTS

Mit der 1995 verabschiedeten EU-Richtlinie Datenschutz wurde eine fundamentale Neuorientierung vorgenommen. Es bleibt den Betreibern und den Benutzern von Informationssysstemen weitgehend selbst überlassen, den Umfang und die Art der Datenverwendung zu vereinbaren. Diese Tatsache wurde von der IT-Industrie nach und nach erkannt. Mit der Konsequenz, dass umfassende und generelle Zustimmungserklärungen geschaffen wurden, die es dem Betreibern erlauben, praktisch alles mit Benutzerdaten zu machen und den Betroffenen völlig im unklaren lassen, was mit seinen Daten geschieht.

Durch weitestgehende Koordination und Absprachen finden sich dann die identen Formulierungen in allen Geschäftsbedingungen einer Branche, mit der Konsequenz, dass die Bürger bei der Auswahl seiner Bank, Versicherung oder seines Telekom-Anbieters keine Alternativen hat.

Die klassischen Preiskartelle werden heute mehr und mehr mit informationsrechtlichen Kartellen abgelöst.

Privacy Statements, die dem Bürger die Möglichkeit geben, Informationsströme zu durchschauen, wesentliche Entscheidungen über die Verwendung seiner Daten selbst zu treffen, könnten ein beutsames Gegengewicht zu vielen unfairen Geschäftsbedingungen darstellen.

WARUM MONITORING- UND RATING?

Online-Systeme sind durch hohe Flexibilität und Veränderbarkeit gekennzeichnet. Klassische Methoden der Zulassungs-Prüfung oder der punktuellen Berwertung sind für diese Systeme völlig ungeeignet und unzureichend.

Online-Systeme werden heute sprach- und länderspezifisch betrieben, auch technische Individualisierungen oder Individualisierungen auf Basis von Interessensprofilen finden statt. Diese Differenzierung schreitet immer weiter voran und wird früher oder später dazu führen, dass jeder einzelne von uns mit einer "persönlichen" Online-Umgebung konfrontiert wird.

Ein Alptraum, der gemeinsame Kommunikation und Verständigung immer mehr erschwert und letztlich nur mehr unter Kontrolle der Online-Betreiber ermöglicht.

Diesen Tendenzen wirken umfassende Bewertungs- und Monitoring-Maßnahmen durch unabhängige Dritte entgegen. Durch laufende Prüfung der Systeme können technische oder rechtlich bedenkliche Entwicklungen erkannt werden, Systeme werden besser vergleichbar und Teilnehmer haben eine verbesserte Orientierungsmöglichkeit über benutzerfreundliche Systeme.

Mit e-rating, einem im Aufbau befindlichen Bewertungssystem zum Thema e-commerce setzt die ARGE DATEN einen ersten Schritt in Richtung Monitoring. Mit sehr gutem Echo bei Konsumenten und jenen Shopbetreibern, die bemüht sind, faire Angebote und Bedingungen zu stellen.

TRANSPARENTES DATENSCHUTZRECHT

Innerhalb der EU werden die Bürger durch ein - relativ zum Rest der Welt gesehen - starkes Datenschutzrecht geschützt. Diese Bestimmungen waren im Zusammenhang mit klassischen Datenverarbeitern ausreichend. Gegenüber Behörden, regionalen Unternehmen und privaten Vereinen funktionieren diese Regelungen - mehr oder minder gut.

Völlig unzureichend und inadäquat sind die Regeln bei international betriebenen Onlinesystemen. Der "naive" Konsument, der etwa unter XY.at einen Shopbetreiber anwählt, jedoch automatisch auf dessen XY.de-Seite weitergeleitet wird und dann ein InFrame-Formular aus den USA ausfüllt, dabei vielleicht über vier Länder geleitet wird und dessen angezeigte Webseite aus Teilen von fünf Unternehmen zusammengesetzt ist, wird innerhalb von Sekundenbruchteilen mit vielleicht 3, 4 oder noch mehr unterschiedlichen Datenschutzregelungen konfrontiert.

Dies führt dazu, dass abhängig von technischen Zufälligkeiten und der betriebsinternen Organisation eines Unternehmens jeweils völlig unterschiedliche Datenschutzbestimmungen gelten.

Diese Situation ist für EU-Bürger unzumutbar. EU-Konsumenten müssen wieder die Sicherheit erhalten, dass bei Nutzung eines Onlinesystems innerhalb der Grenzen der EU, immer EU-Recht zu gelten hat.

Diese Forderung ist auch sachlich begründet. Online-Geschäfte können, entkleidet man sie von technischen Details, am ehestens mit Haustürgeschäften verglichen werden. Der Anbieter kommt letztlich zum Konsumenten und nicht umgekehrt.

KEINE INFORMATIONSTECHNISCHE AUSBEUTUNG BIOMETRISCHER MERKMALE

Als letztes noch eine Anmerkung zur Biometrie. Biometrische Identifikationsmethoden werden immer wieder als Allheilmittel zum Erreichen absoluter Sicherheit hingestellt.

Dies ist jedoch eine bewußte Irreführung. Selbst wenn einzelne biometrische Merkmale eindeutig und unverwechselbar sind, ist es nicht deren Erfassung und technische Interpretation. Ein einzelner Fingerabdruck ist einmalig und unverwechselbar. Und ist daher auch kein zweites Mal herstellbar! Ein und dieselbe Person ist nicht imstande, zwei idente Fingerabdrucke zu produzieren, biometrische Verfahren müssen daher immer vereinfachen, interpretieren und vergröbern.

Damit blieben aber biometrische Methoden genauso unsicher, wie andere technische Verfahren. Setzt jedoch die Verwendung einer Chip-Karte individuelle Entscheidungen des Betroffenen voraus, besitzt der Betroffene überhaupt eine

Chiparte, wo verwendet er diese, welche Karte verwendet er, werden Menschen bei biometrischen Verfahren dieser Entscheidungsfreiheit beraubt.

Wir alle hinterlassen ständig biometrische Spuren, die ausgewertet, genutzt und ausgebeutet werden können. In Österreich ist die Ausbeutung biometrischer Merkmale völlig ungeregelt und wir beobachten heftigste Bemühungen der Überwachungslobby, biometrische, also höchstpersönliche Merkmale als frei verfügbare und von jedermann nach Belieben verwertbare Infomation zu deklarieren.

Bemühen wir uns daher um rascheste Schaffung eines möglichst weitreichenden Verbots der Ausbeutung biometrischer Merkmale und auch zu einer EU-weiten Ächtung biometrischer Spionage.

RESÜMEE

Ein wesentlicher Teil des Versagens der NewEconomy und des gehemmten Wachstums in e-commerce und e-government sind durch das - berechtigte Mißtrauen - der Bürger in die Fairness und in das Verantwortungsbewußtsein der Anbieter begründet.

Die Betreiber nutzen ihren rechtlichen und technischen Informationsvorsprung einseitig und schamlos zu ihren Gunsten aus.

Es entstehen unfaire Geschäftsbedingungen, die selbst noch höchstgerichtlichen Entscheidungen ungeniert weiterverwendet werden (MOBILKOM/TELEKOM, UNIQUA).

Es werden Auskunfts- und Reklamationsrechte der Bürger ignoriert, es werden Daten der Bürger nach Belieben benutzt, gehandelt und veröffentlicht.

Sicherheitsrelevante Informationen oder Informationen, die die Privatsphäre der Bürger verletzten können, werden von den Onlinebetreiber nicht weitergegeben und verheimlicht.

Behörden und Unternehmen bauen heute nicht an einem Big Brother, der letztlich in einem undiffernezierten Datenmeer des gläsernen Bürgers ertrinken würde, sonderen an einem Labyrinth von gläsernen Mauern, das den Bürger in seinen Handlungen beschränkt und einengt und undurchschaubar macht, wer welche Informationen zu welchen Zwecken für oder gegen ihn benutzt.