Elektronische Identitäten: Das alltägliche Datenschutzproblem

Walter Hötzendorfer
Arbeitsgruppe Rechtsinformatik, Universität Wien
walter.hoetzendorfer@univie.ac.at

Europa-Tagung

„Von Jägern, Sammlern und Piraten“
Datenschutz, Neue Medien und Technologien in der Europäischen Union

28. September 2012

Über mich

DI Mag. Walter Hötzendorfer

- Fachlicher Hintergrund
  - Wirtschaftsinformatik (TU Wien)
  - Jus (Uni Wien)
- Projektassistent in der Arbeitsgruppe Rechtsinformatik/Uni Wien
  - Projekte SMART (FP7), DIANA
- Dissertation zu den rechtlichen Aspekten föderierter elektronischer Identitäten (Schwerpunkt Datenschutz)
- Forschungsschwerpunkte:
  - Datenschutz
  - Datensicherheit
  - Elektronische Identitäten/Identity Federation/Trust Frameworks
  - Cloud Computing

Elektronische Identitäten

- Sammlungen von digitalen Informationen, die zu einem Individuum oder einer Organisation gehören.
- Digitale Repräsentationen von Teilen der gesamten Identität einer Person (Teilidentität)
- Eine Person hat somit in der Regel mehrere elektronische Identitäten
- Synonym: *digitale* Identitäten
  - Problematisch: eID, „*virtuelle* Identitäten“
- *Attribute*: die einzelnen gespeicherten Informationen

Prolog

Wie viele verschiedene Benutzerkonten haben Sie?

Wie viele Passwörter haben Sie?

Welche persönlichen Informationen haben Sie im Laufe der Zeit auf welchen Websites angegeben?

Vertrauen Sie den Betreibern all dieser Websites in entsprechendem Maße?

=> „Identitätskrise“ des Internet

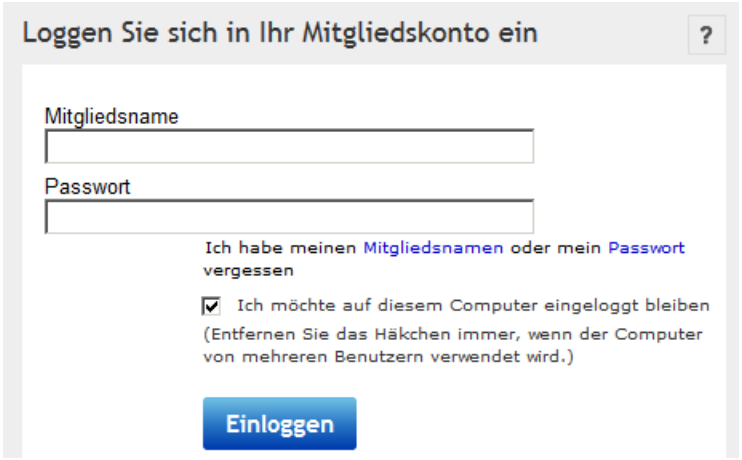
Das Grundproblem

- Identifikation unter Anwesenden:
  - Instinktiv/unbewusst/automatisch
  - Bekannte: Aussehen/Stimme
  - Fremde: Merkmale/Auftreten/Plausibilität
  - Diverse Ausweise
- Identifikation im Internet:
  - Nur auf Ebene der Geräte eindeutig
  - Gewohnte Mechanismen funktionieren nicht

  => Identitätsmanagement notwendig (d.h. Systeme zur Identifikation, Authentifizierung und zum Nachweis bestimmter Eigenschaften)

Identitätsmanagement

- Einerseits: staatliche Systeme
  - Bürgerkarte (AT), neuer Personalausweis (DE) etc.
  - Eindeutige Personenbindung, hohe Sicherheit
  - Geringe Verbreitung, nationale Zersplitterung
- Andererseits:



Serviceprovider

=

Identitätsprovider

Die „Identitätskrise“

- Zu viele Passwörter
- Sicherheit von Passwortauthentifizierung ist ohnehin begrenzt
- Zu viele Benutzerkonten
  - Mehr Daten preisgegeben als notwendig
  - Kein Überblick mehr
  - Daten veralten und werden inkonsistent/Wartung aufwendig
- Viele kritische Transaktionen im Internet noch immer nicht möglich (z.B. Eröffnung eines Bankkontos)
- Qualifizierte Angabe von Attributen im Internet noch immer nicht möglich (z.B. Angabe des Alters)

Lösungsansatz?

Identity Federation:

Organisationsübergreifende

Mehrfachverwendung elektronischer Identitäten

- Kein eigenes Benutzerkonto für jeden einzelnen Service mehr
- Z.B. Microsoft Passport, OpenID, Liberty Alliance Project, Google, Facebook)

Die „Identitätskrise“

Aber: Einzelne Benutzerkonten werden „zu wichtig“/einzelne Player zu mächtig

Beispiel Facebook:

- Einerseits: Man surft nicht mehr anonym, sondern immer häufiger mit der Facebook-Identität
  - Gewollt: Log In With Facebook 

  - Ungewollt: Cookies, „Like-Button überall“ 

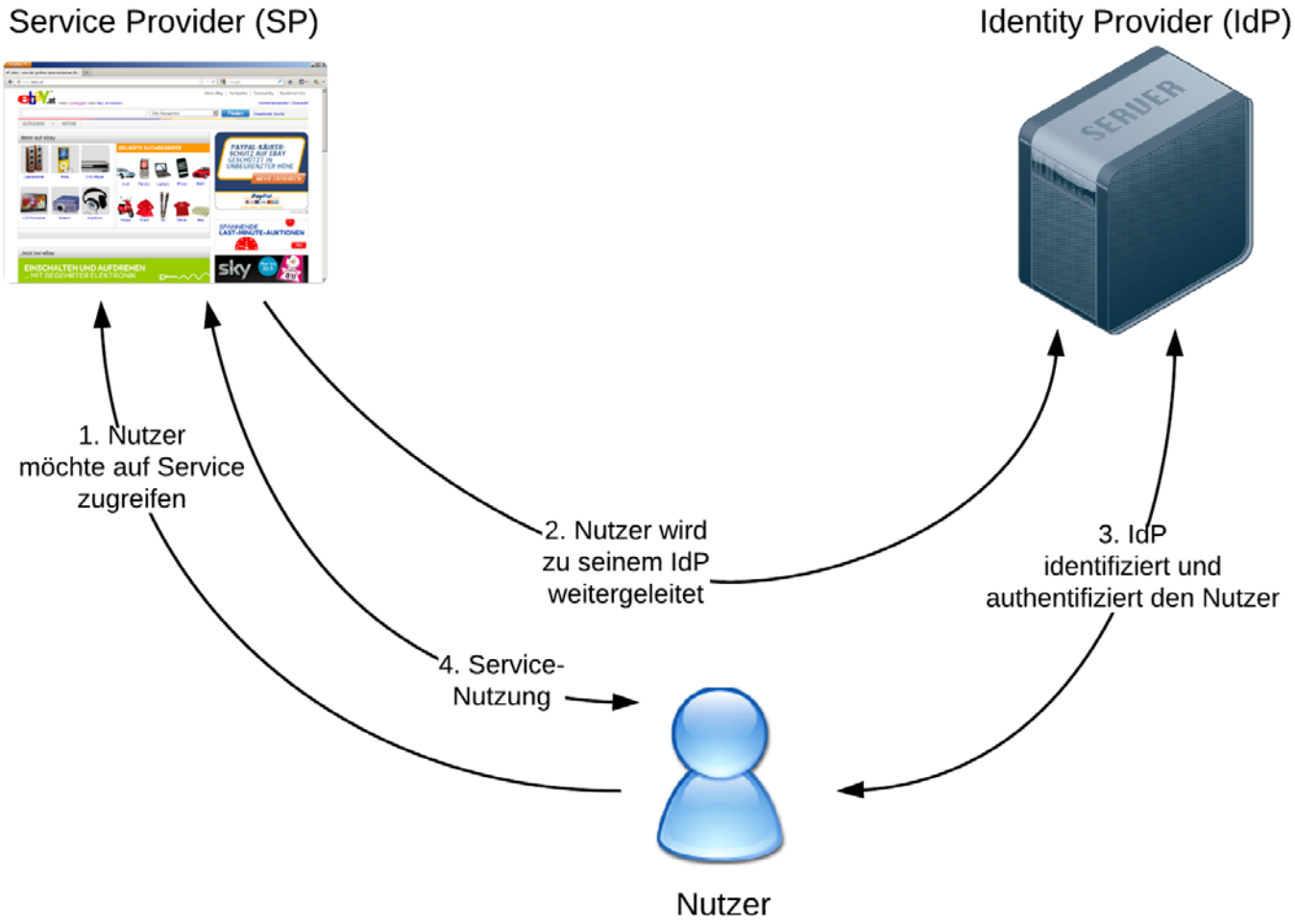
- Andererseits: immer mehr Funktionalität (Dritter) direkt auf Facebook

Gefahren:
- Einzelner Serviceprovider protokolliert einen großen Teil der Webaktivität eines Nutzers
- Bedeutung einer einzelnen elektronischen Identität zu groß, Schadenspotenzial hoch

Lösung?

- Neugestaltung des Umgangs mit elektronischen Identitäten im Internet
- Keine neue Technik, sondern neue Organisation: **Kollaboratives Identity-Federation-Modell**
  - Getrennte Rollen:
    - Service Provider
    - Identity Provider
    - Attribute Provider
    - …
  - Dezentrales, kollaboratives System
  - Technologieneutral
  - Nutzerorientiert
  - Mehrere Sicherheitsstufen der Authentifizierung und der Attribute (Assurance Levels) für verschiedene Anwendungsfälle

Schematischer Ablauf



Voraussetzungen

- Institutioneller Rahmen:
  „(Trust and) Identity Federation“/„Identity Ecosystem“/„Circle of Trust“)
  - Definierte Rollen, Regeln, Standards
    => Technische und organisatorische Interoperabilität
    => Institutionalisiertes Vertrauen
    => Datenschutz und Datensicherheit
  - Haftungsregime
  - Logging, Audit und Dispute Settlement
- Profitabilität der einzelnen Rollen

Identity Provider (IdP)

- Vom Service Provider rechtlich und wirtschaftlich unabhängig
- Partner des Nutzers (kein Interessenkonflikt)
- Haftet für die Richtigkeit von Angaben, die er macht
- Mehrere IdP: Nutzer kann auf dem Markt auswählen
- Mögliche IdP: Staatliche Identitätssysteme (Bürgerkarte, neuer Personalausweis)
  - Z.B. für höchste Sicherheitsstufe

Geht nicht?

- Auch in anderen Bereichen wurden solche Systeme erfolgreich etabliert
- Beispiel: Kreditkartenwesen
  - Organisationsrahmen mit verschiedenen Rollen
  - Geregeltes Haftungsregime, Streitschlichtungs-mechanismen, kalkulierbares Risiko
  - Jede Rolle potenziell profitabel (Selbsterhaltung)

Schwierig: Etablierung

- Administrative Arbeit für den Nutzer minimieren
  - Automatisierung
  - Law by Default
  - Law by Design
- Wirtschaftlichkeit; Potenziale:
  - Sicherheitsprobleme verursachen Kosten
  - Eigenes Identitätsmanagement der Service Provider verursacht Kosten
- Transformationsprozess/Aufbau
  - Interoperabilität

Ziele

- Sich „ausweisen“ und qualifizierte Angaben (z.B. des Alters) im Internet werden möglich
  - Nutzung des gesamten Potenzials des Internets
- Datenschutz/Anonymität/Nutzerorientierung:
  - Nutzer bestimmt und kann später nachvollziehen, wer welche Daten von ihm bekommt
  - Service Provider wissen nicht, wer der Nutzer ist, wenn dies nicht unbedingt notwendig ist
  - Identity Provider, Attribute Provider und andere Service Provider wissen nicht, welche Services der Nutzer verwendet
- Nur wenige Anmeldevorgänge/wenige Passwörter/wenige Karten
- Zwei-Wege-Authentifizierung

Initiativen

- NSTIC: National Strategy for Trusted Identities in Cyberspace (White House) http://www.nist.gov/nstic/index.html
- Kantara Initiative http://kantarainitiative.org/
- …
- Österreichische Initiative

Herausforderungen/Forschungsfragen

- Organisatorischer Aufbau
- Äußerer Rechtsrahmen, insbesondere:
  - Datenschutz
  - Haftung der beteiligten Organisationen gegenüber den Nutzern und den Serviceprovidern
- Innerer Rechtsrahmen, insbesondere:
  - Vertragliche Gestaltung der Rechtsbeziehungen der beteiligten Organisationen zueinander
  - Haftungsverhältnis der einzelnen Organisationen
- …

VIELEN DANK!

Kontakt

DI Mag. Walter Hötzendorfer

Arbeitsgruppe Rechtsinformatik,
Abteilung für Völkerrecht und Internationale Beziehungen,
Universität Wien
Schottenbastei 10-16/2/5
1010 Wien

walter.hoetzendorfer@univie.ac.at