

Identitäten im WWW

Chancen und Risiken für Unternehmen

Sebastian Feld
feld [at] internet-sicherheit [dot] de

Institut für Internet-Sicherheit
<https://www.internet-sicherheit.de>
Fachhochschule Gelsenkirchen



Agenda

- Institut für Internet-Sicherheit
- Akuter Schutzbedarf
- Identitäten im Internet
- Web 2.0 und Sicherheit
- Ausblick
- Fazit

- **Institut für Internet-Sicherheit**
- Akuter Schutzbedarf
- Identitäten im Internet
- Web 2.0 und Sicherheit
- Ausblick
- Fazit

Wer wir sind

Eine Innovative, unabhängige und wissenschaftliche Einrichtung der Fachhochschule Gelsenkirchen

Unsere Aufgaben

Forschung, Entwicklung und anwendungsbezogene Lehre auf dem Gebiet der Internet-Sicherheit

Unser Team

Ca. 50 wissenschaftliche Mitarbeiter, Diplomanden und Studenten

Unser Ziel

Mehrwert an Vertrauenswürdigkeit und Sicherheit im Internet herstellen



■ Internes Hochschulinstitut

- Gegründet Mai 2005 mit Herrn Schily
- Leitender Direktor: Prof. Dr. Norbert Pohlmann
- Fachbereichsübergreifendes Institut
- Schwerpunkt IT-Sicherheit und verteilte Systeme
- Lehre-Schwerpunkt Master-Vertiefungsrichtung Kommunikationstechnik und Internet



■ Trusted Computing

- Sichere Betriebssysteme
- Network Access Control



■ Internet-Frühwarnsysteme

- Internet-Analyse
- Strukturelle Analyse des Internets



■ E-Mail-Sicherheit

- Anti-Spam
- E-Mail-Verlässlichkeit



■ Identity Management

- elektronischer Personalausweis
- Studie IdMS-Konzept



■ Sonstige

- Mobile Security, VoIP, Web Services Security, Branchenbuch IT-Sicherheit, Awareness

- Beratung
- Live-Hacking / Awareness Workshops
- Forschung und Entwicklung
- Studien
- Konzepte und Spezifikationen
- Prototypenentwicklung
- Benchmarking
- Umfragen
- Penetrationstests

mehrmals täglich am Innovationsstand - NRW

Live-Hacking

••• Institut für Internet-Sicherheit •••



Halle 9
Stand C16

if(is)
internet-sicherheit

CeBIT
Join the vision

- Internet-Frühwarnsystem
- Turaya Trusted Computing
- E-Mail Reputation Service
- Branchenbuch IT-Sicherheit

 Fachhochschule
Gelsenkirchen

Agenda

- Institut für Internet-Sicherheit
- **Akuter Schutzbedarf**
- Identitäten im Internet
- Web 2.0 und Sicherheit
- Ausblick
- Fazit

Grundsätzliche Problematik

- Fundamentaler Wandel
 - Informations- und Wissensgesellschaft
- Steigender **Wert von Informationen**
 - Persönliche Daten, Entwicklungsunterlagen, Strategiekonzepte, ...
 - → **Notwendigkeit von IT-Sicherheitsmaßnahmen**
- **Mangelndes Unrechtsbewusstsein** in der elektronischen Welt
 - Reale Welt: Zäune erklimmen, Türen aufbrechen, ...
 - Elektronische Welt: Mit Kaffee und Keksen vor Bildschirm
- Das Internet hat keine Grenzen
 - Geographisch, politisch, administrativ
 - Herausforderung: Notwendige und passende **Vertrauenswürdigkeit des Internets** und seiner Dienste

- Gewährleistung der **Vertraulichkeit**
 - Damit keine unautorisierten Personen in der Lage sind, übertragene oder gespeicherte Daten zu lesen.
- Gewährleistung der **Authentikation**
 - Damit wir bei einer elektronischen Kommunikation oder Transaktion wissen, wer unser Partner ist bzw. wer auf unsere Betriebsmittel zugreift.
- Gewährleistung der **Integrität**
 - Damit wir überprüfen können, ob übertragene und gespeicherte Daten unverändert, d.h. im Originalzustand sind.

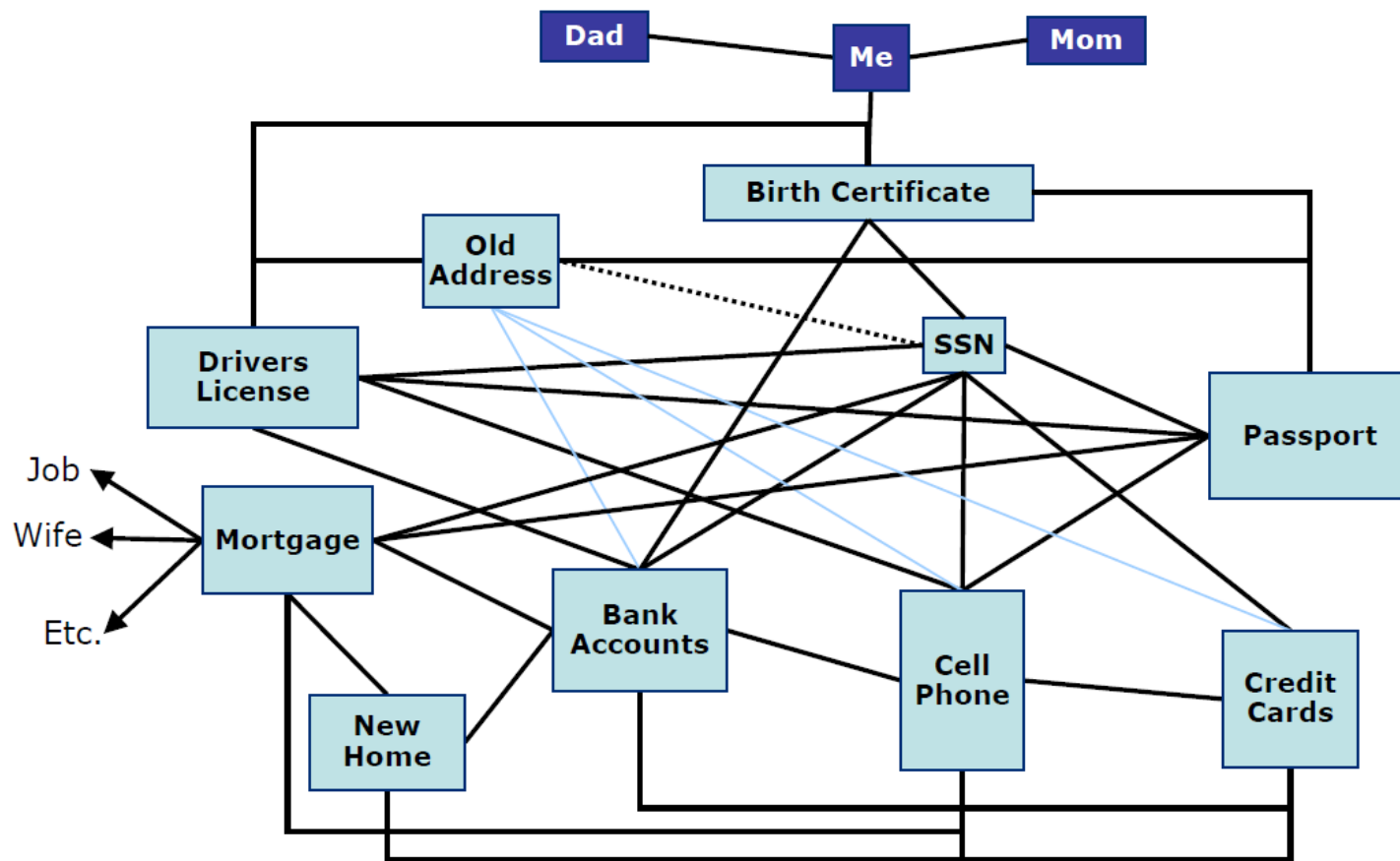
- Gewährleistung der **Verbindlichkeit**
 - Damit wir die Gewissheit haben, dass die elektronische Prozesse und die damit verbundenen Aktionen auch verbindlich sind.
- Gewährleistung der **Verfügbarkeit**
 - Damit wir die Gewissheit haben, dass die Daten und Dienste auch zur Verfügung stehen.

Aus dem Persönlichkeitsrecht:

- **Informationelle Selbstbestimmung**
 - Das Grundrecht zu haben, grundsätzlich selbst über die Preisgabe und Verwendung der eigenen persönlichen Daten zu bestimmen.

- Institut für Internet-Sicherheit
- Akuter Schutzbedarf
- **Identitäten im Internet**
- Web 2.0 und Sicherheit
- Ausblick
- Fazit

- Ein Zusammenschluss von Eigenschaften verschiedenster Art



- Erstellte Profile in Plattformen
 - Xing, Facebook, Myspace, ...
- Kombination der Profile
 - Verlinkungen zwischen den Diensten (gewollt und ungewollt)
- Veröffentlichte Inhalte
 - Webseiten, Blog-Einträge, Fotografien, ...
- Sämtliche Bewegungsspuren
 - Log-Daten der Server
 - Verbindungsdaten der ISPs

- Unterschiedliche Mechanismen stehen zur Verfügung
 - Bspw. Föderation / Single-Sign On
- Technologien, Protokolle und Formate sind weniger das Problem
 - OpenID, OAuth, Information Cards, SAML, ...
- Das **Vertrauen** ist das Problem!
 - Auslagerung der Authentifizierung
 - Identity Provider ↔ Service Provider
 - **Geschäftsmodell** des Identity Provider?
- Lösungen stehen noch aus...

- Institut für Internet-Sicherheit
- Akuter Schutzbedarf
- Identitäten im Internet
- **Web 2.0 und Sicherheit**
- Ausblick
- Fazit

- Neue Anwendungsmöglichkeiten
 - Internet erlangt **weitere Akzeptanz**, Hemmschwelle gesunken
 - Breitband-Anbindung ermöglicht Text, Audio, Video, ...
 - Vielfältige Möglichkeiten zur Präsentation
 - Informationen im „Web 2.0“
 - Anbieter stellt lediglich Infrastruktur und Dienste zur Verfügung
 - Nutzer bearbeitet Inhalte
 - **Interaktion** und **Kollaboration**
- Kein erkennbarer Unterschied zwischen **Autor** und **Nutzer** der Information

- Social Bookmarks
 - Persönliche, aber öffentliche Linklisten
 - Eigene Verbreitung und Bindung von Lesern, Besuchern, Kunden etc.
- Social Network
 - Nutzer können sich auf verschiedene Arten kennen lernen und miteinander kommunizieren
 - Möglichkeit zur Mundpropaganda, zusätzliches „Gesicht“
- Wiki
 - Seitensammlung im Internet, kann von jedem gelesen und verändert werden
 - Gezielte Steuerung der eigenen Darstellung
- Blog
 - Öffentliches Internet-“Tagebuch“, Leser können Kommentare verfassen
 - Möglichkeit zur Steigerung der Reputation, aber auch Gefahr der Verleumdung
- Medien-Plattform
 - Möglichkeit zur Veröffentlichung eigener Texte, Fotos, Videos, ...
 - Virales Marketing

- Wer kann die zahlreichen, **freiwillig** preisgegebenen Informationen einsehen?
 - Potentiell: Jeder!
 - Und: Theoretisch für immer!
 - Auch nicht öffentlich freigegebene Informationen können Sorge bereiten
 - **Server** des Anbieters hinreichend geschützt?
 - Werden personenbezogene Informationen an Dritte **weitergegeben**?
 - Wie ist die **rechtliche Situation** der vom Nutzer generierten und veröffentlichten Inhalte?
- Szenario-basierte Beantwortung der Fragen!

Social Networking mit Blick auf Datenschutz und Datensicherheit (1/5)

- „Social Network“-Anwendungen
 - Meist freie Dienste im Internet, bei denen Nutzer **Informationen über sich selbst** einspielt
 - Persönliche Angaben wie Hobbies, Musikgeschmack oder favorisierte Webseiten
 - Selbsterstellte Fotografien, Videos oder andere Inhalte
 - Über **Selbstbeschreibung** werden
 - alte Freunde wieder gefunden
 - neue Freundschaften geknüpft
 - Gruppen erstellt, um gemeinsame Interessen zu teilen
 - Hohe Wahrnehmung in der **virtuellen Szene** durch
 - Preisgabe vieler Informationen
 - Aktivität innerhalb der Anwendung

Social Networking mit Blick auf Datenschutz und Datensicherheit (2/5)

- Informationelle Selbstbestimmung
 - Analyse persönlicher Daten oder Weitergabe an Dritte?
 - Potentielles **Geschäftsmodell** eines Diensteanbieters
 - Weitergabe anonymisierter Daten
 - Weitergabe von Nutzungsprofilen oder Statistiken
 - Handhabung des Datenschutz wird von jeder Web 2.0 Anwendung explizit erklärt
 - Anbieter mit **strenger Achtung** der Datenschutzgesetze und **Gewährleistung** des Schutz personenbezogener Daten
 - Ausdrückliche Erwähnung der **Weitergabe** kritischer Informationen, um
 - Gesetzliche Bestimmungen
 - Nutzungsbedingungen
 - Rechte des Anbieters

Social Networking mit Blick auf Datenschutz und Datensicherheit (3/5)

- Externe Profilbildung
 - Möglichkeit zur Erstellung regelrechter **Soziogramme**
 - Kombination persönlicher Nutzerinformationen
 - Verlinkungen innerhalb des Netzwerks
 - Weitere Datenquellen und externe Verlinkungen
- Öffentliche Selbstdarstellung
 - Durch **genaues Abbilden** der eigenen Person wird man gefunden
 - Alter Freund aus der Grundschulzeit
 - Aber auch: Der oft zitierte Personalchef holt Informationen vor Bewerbungsgespräch ein

Social Networking mit Blick auf Datenschutz und Datensicherheit (4/5)

- Indirekte und relativ **anonyme** Kontaktknüpfung
 - Bekannte Fälle, dass Triebtäter über soziale Netzwerke Minderjährige ansprechen und Kontakte aufbauen
 - Abgleich der **Profildatenbanken** mit Daten von Sexualstraftätern oder sonstigen Vorbestraften?
 - Eigentlich positives Vorgehen...
 - Aber: Datenschutz? Gläserner Mensch!
 - Semantic Web als „Hilfsmittel“
 - Gespeicherte Informationen lesbar von Mensch und Maschine
 - **Kombination** unterschiedlicher Datensätze wie Nutzerprofile, Handyabrechnungen, Finanzbewegungen, Kommunikationsdaten, ...
 - Regelrechte **Rasterfahndung**

Social Networking mit Blick auf Datenschutz und Datensicherheit (5/5)

- Vielfältige Angriffsflächen
 - **Ungewissheit** des Gegenübers
 - Attraktivität für **Ausspähung** der Nutzerdaten
 - Aber auch Internet-Auktionshäuser und weitere Anwendungen
 - Angriff bspw. durch Phishing-Attacken
 - Mangelndes IT-**Sicherheitsbewusstsein**
 - Erspähte Zugangsdaten werden benutzt, um das Profil des Betroffenen zu manipulieren
 - „sozialer“ Schaden
 - Diebstahl
 - Wahrscheinlichkeit, dass der Geschädigte das Passwort mehrfach benutzt → **Identitätenkollaps**

- „User-generated Content“ und die rechtliche Situation
 - Wem gehören die Inhalte und welche **Lizenzen oder Rechte** gelten?
 - Wem gehören die Kommentare in Blogs?
 - **Verschiedene Ansätze**, z.B. Creative Commons-Lizenzen
- Content-Storing und -Sharing
 - Erneut: Distanzierung von Inhalt oder Beanspruchung der Rechte
 - Oft **fehlende Gewährleistung**, dass Daten unverändert, verfügbar und somit sicher sind
 - Vage Formulierungen in Nutzungsbedingungen und AGBs
 - „Wir fahren öfter Backups, als Sie die Dateien ändern können“
 - Harte Fakten wie **Verschlüsselung, Übertragungssicherheit** oder **Verfügbarkeit** werden weder konkret angesprochen noch garantiert

Agenda

- Institut für Internet-Sicherheit
- Akuter Schutzbedarf
- Identitäten im Internet
- Web 2.0 und die Sicherheit
- **Ausblick**
- Fazit

- 3 Faktoren
 - Wissen (Geheimnis → Passwort)
 - Besitz (Zertifikat → SmartCard)
 - Eigenschaft (Biometrie → Fingerabdruck)
- Vierter Faktor
 - Das Handeln!
 - Evaluation des **Risikos**
 - Verschiedene Parameter: Situationsbedingt, persönlich, historisch, ...
 - **Zusätzliche Ebene** über der herkömmlichen Authentifizierung
 - Als Beispiel
 - Normal: WinXP, Firefox, Deutschland
 - Riskant: Linux, Safari, Asien
 - Erst Prüfungen durchführen, dann die eigentliche Authentifizierung

- **Korrelation** personenbezogener Daten
 - **Keine isolierten Datensilos**
 - IdM-Infos, Geographische Positionen (GPS) , Log-Daten, ...
- Treffen von Vorhersagen
 - Konsolidierung der verfügbaren Channel (Lokation, Verbindungsdaten, ...)
 - Möglichkeit zur Prognose von **Aktionen** und **Verhalten**
 - Aber damit auch: Eine neue Welle von **Social Engineering**
- Vortrag Jeff Jonas (IBM), DIDW 2009

Agenda

- Institut für Internet-Sicherheit
- Akuter Schutzbedarf
- Identitäten im Internet
- Web 2.0 und die Sicherheit
- Ausblick
- **Fazit**

- Mehr IT-Sicherheitsbewusstsein!
 - Gefahren im Internet sind nicht **virtuell**, sondern durchaus **real**
 - Die Haustür wird immer abgeschlossen. Der PC auch?
 - **Sensibilisierung** für Gefahren (Phishing, Social Engineering)
- Das Internet vergisst nichts!
 - **Bewusstere** Preisgabe von Informationen
 - Ungewollte Leser/Betrachter, Rasterfahndung, Gläserner Mensch
- 2 Seiten der Medaille
 - Möglichkeiten und **Chancen** erkennen (Werbung, Vertriebskanäle)
 - Aber auch **Risiken** und Gefahren (Tor ins Unternehmen, Verleumdung)
- Vielversprechendes **Identity Management**
 - Usability, Kosteneinsparung, Prozessbeschleunigung, ...
 - **Sicherheit!**

Identitäten im WWW – Chancen und Risiken für Unternehmen

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

Sebastian Feld
feld [at] internet-sicherheit [dot] de

Institut für Internet-Sicherheit
<https://www.internet-sicherheit.de>
Fachhochschule Gelsenkirchen

