Fachhochschule Gelsenkirchen

Sicherheits-Tipps für Cloud-Worker

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Fachhochschule Gelsenkirchen
http://www.internet-sicherheit.de

Cloud Computing
→ Einschätzung

- **Cloud Computing wird die Zukunft sein!**

- IT **Sicherheit** und **Vertrauen** sind die Enabler für:
  - wie schnell und
  - wie tief

  die Nutzung von Cloud Computing sein wird, insbesondere in Deutschland

Vertrauenswürdigkeit
→ Motivation

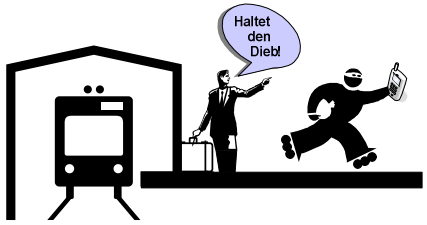
- **IT-Sicherheit / Datenschutz ist eine sich verändernde Herausforderung**
  - Das Internet geht über alle Grenzen und Kulturen hinaus!
  - Immer schnellere Entwicklung und Veränderung in der IT.
  - Die Nutzer müssen immer wieder neues Wissen erwerben, wie sie sich angemessen verhalten können.
  - Die zu schützenden Werte steigen ständig und ändern sich mit der Zeit.
  - Die Angriffsmodelle innovieren und Angreifer werden professioneller.
  - IT-Sicherheitsmechanismen werden komplexer, intelligenter und verteilter.
  - **Mit der Zeit werden die IT-Sicherheits- und Datenschutzprobleme immer größer!**

Wenn ich Angreifer wäre …
→ Aktuelle allgemeine Schwachstellen

- **Computer-Sicherheit**
  - Software-Qualität
  - Schwache Erkennungsrate bei Anti-Malware Produkten
  - …

- **Identity Management**

- **Webserver Sicherheit**

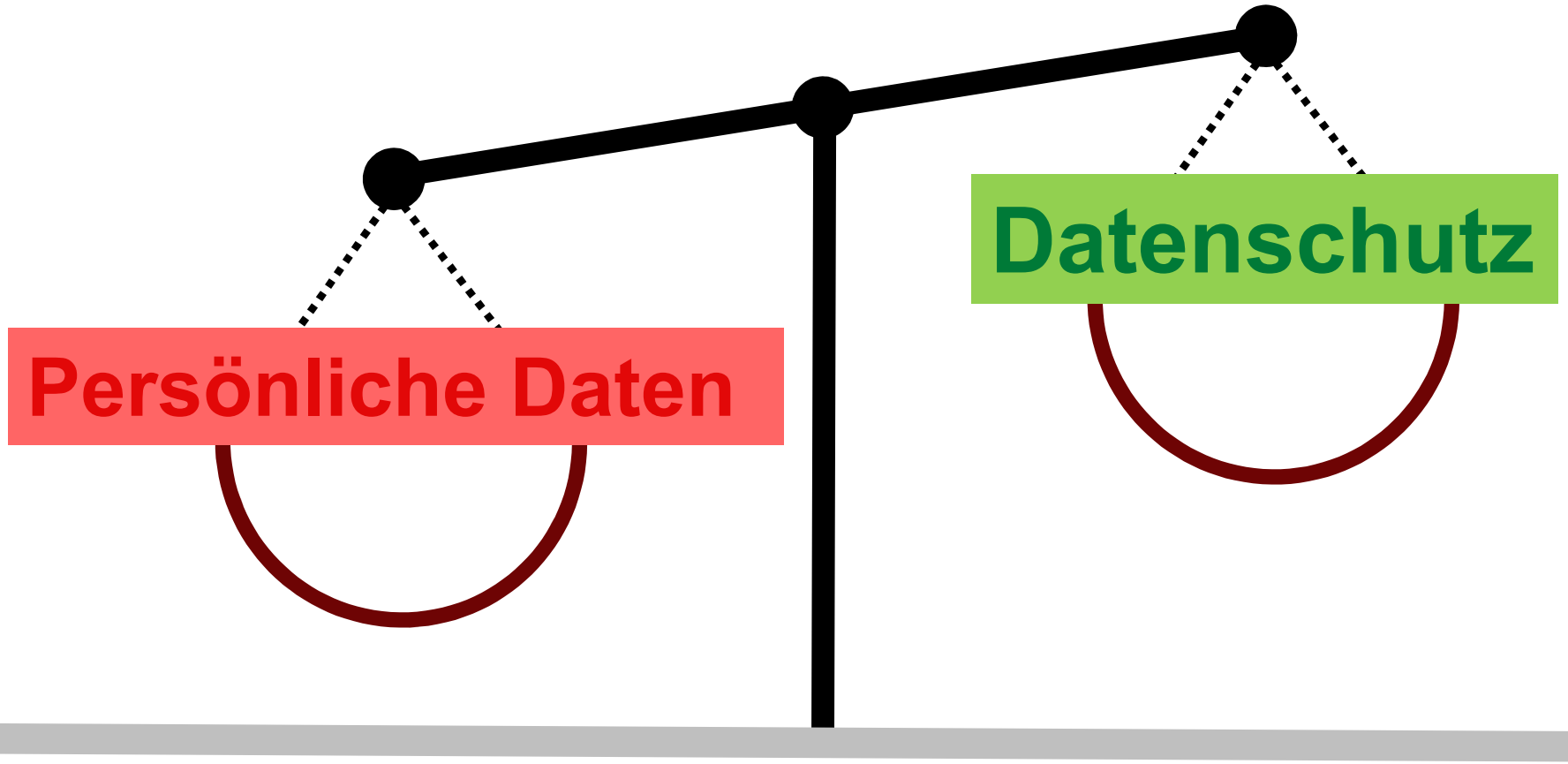


- **Mobile Geräte**
- **Internet-Nutzer**
- …

→ Professionalisierung der Internetkriminalität ←

Geschäftsmodell
→ Bezahlen mit persönlichen Daten

Persönlichen Daten sind ein Rohstoff des Internetzeitalters



Cloud Computing
→ Vorteile

- **Flexibilität**
  (von überall, zur jeder Zeit und mit vielen unterschiedlichen Geräten)
- **Geschwindigkeit**, Dienste sind sofort nutzbar
- Hohe **Verfügbarkeit** und **Robustheit ,** die ein Unternehmen selbst umsetzen kann
- Hohe physikalische Sicherheit
- …

Cloud Computing
→ Nachteile / Gefahren

- Dauerhafter und attraktiver zentraler Angriffspunkt
- Vernetzung bietet zusätzliche Angriffspunkte
- Ich kenne die Orte, wo meine Daten gespeichert sind nicht!
- Datenverlust (Platten-, Datenbank-, Anwendungsfehler, …)
- Wie kann ich sicher sein, dass die Daten noch existieren?
- Identitätsdiebstahl
- Session-Hijacking
- Schwachstellen bei Shared Services,
  Abgrenzung der Unternehmensdaten
- Datenlecks (Datenbank, Betriebssystem, …) – Hacker!
- …

Geschäftsmodell vs. IT Sicherheit
→ Dropbox (siehe crn.de)

Security und Cloud Storage

Freier Zugang für alle: Peinliche Sicherheitspanne bei Dropbox

von Lars Bube

Share

21.06.2011

Beim beliebten Cloud Storage Dienst Dropbox gab es gestern (Montag) eine mehr als peinliche Datenpanne. Für mehrere Stunden konnten sich die User mit jedem beliebigen Passwort in jeden Dropbox-Account einloggen, auch von Fremden.

Während bei Datenverlusten normalerweise immer eine Art von digitaler Fremdeinwirkung oder gar Gewalt mit im Spiel ist, schaffen es manche Unternehmen auch, sich ganz alleine ein Bein in Sachen IT-Sicherheit zu stellen. Jüngstes Beispiel ist das Unternehmen Dropbox, das Nutzern Online-Speicher in der Cloud anbietet, über den die abgelegten Dateien von jedem Internet-PC der Welt aus verfügbar sind.

US-Behörden dürfen auf europäische → Cloud-Daten zugreifen (heise-online.de)

30.06.2011 13:05

US-Behörden dürfen auf europäische Cloud-Daten zugreifen

Cloud-Anbieter wie Microsoft müssen US-Strafverfolgungsbehörden Zugriff auf von Kunden gespeicherte Daten gewähren, berichtet der US-Branchendienst *ZDNet*. Das betrifft auch in der EU ansässige Firmen und in europäischen Rechenzentren liegende Daten, wie Microsofts britischer Direktor Gordon Frazer anlässlich der Markteinführung von Microsofts Office 365 in London erklärte. Er antwortete damit auf die Frage, ob Microsoft zusichern könne, dass in seinen EU-Rechenzentren gespeicherte Daten Europa niemals verlassen könnten.

Da das Unternehmen seinen Firmensitz in den USA habe, müsse es die dortigen Gesetze befolgen, sagte Frazer. Das gilt insbesondere für den Patriot Act, der US-Strafverfolgern weitreichende Zugriffsrechte auf Daten gibt. Frazer zufolge würden Kunden über die Herausgabe von Daten "informiert, wann immer das möglich ist". Eine Garantie dafür könne er jedoch nicht geben. Denn in den USA kann das FBI mit einem National Security Letter (NSL) ein Redeverbot (Gag order) für den Betreffenden aussprechen. In diesem Fall darf er nicht einmal sagen,

Sicherheits-Tipps für Cloud-Worker → IT-Sicherheit

Überprüfen Sie beim Cloud-Anbieter:

- Stärke der Identifikation und Authentikation (Passworte, SecToken, nPA, …)
- Verschlüsselung der Kommunikation (HTTPS, usw.)
- Verschlüsselung der Daten im Client, bevor diese in die Cloud gesendet werden.
- Können Daten zu anderen Cloud-Anbieteren übertragen werden (Abhängigkeit)!
- …

Überprüfen Sie Ihre eigenen Zugangsgeräte (Notebook, SmartPhone, …)

- Anti-Maleware
- Personal Firewall
- Automatische UpDates (Betriebssystem, Anwendungen, …)
- …

Sicherheits-Tipps für Cloud-Worker
→ Vertrauenswürdigkeit des Anbieters

Überprüfen Sie folgenden Aspekte:

- AGBs /Verträge genau lesen und verstehen!
  - Was darf der Cloud-Anbieter mit Ihren Daten machen?
  - Passt Service-Level (Verarbeitungszeit, Verfügbarkeit, …)
  - Welche Verantwortung übernimmt er
  - Vergleichen Sie mit Ihren Compliance-Anforderungen
- Aus welschem Land kommt der Cloud-Anbieter?
- Welche Überprüfungen hat er gemacht?
  (eco, BSI, ISO 27001, …)
- Stellte er seine Software zur Verfügung (Open Source)?
- Referenzen – Stärken und Schwächen
  (Recherchieren und mit Referenzen telefonieren, …)
- …

Fazit
→ Komplexe Herausforderung

- **Die Cloud in Kombination mit Mobilität benötigt deutlich mehr Sicherheit und Vertrauenswürdigkeit, durch**
  - gute und sichere Soft- und Hardware (Lösung)
  - vertrauenswürdige Anbieter

  aber auch

  - hohes Sicherheitsbewusstsein der Nutzer

© Alex Slobodkin | istockphoto

Fachhochschule Gelsenkirchen

Sicherheits-Tipps für Cloud-Worker

Vielen Dank für Ihre Aufmerksamkeit
Fragen ?

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Fachhochschule Gelsenkirchen
http://www.internet-sicherheit.de