Neue Webdienste – Regelung und Bewertung in der Fraunhofer-Gesellschaft

Dr. Ulrich Pordesch (ZV-3C, IT-Sicherheitskoordinator der Fraunhofer Gesellschaft)

Informationsrechtstag, Darmstadt, 26.11.2010

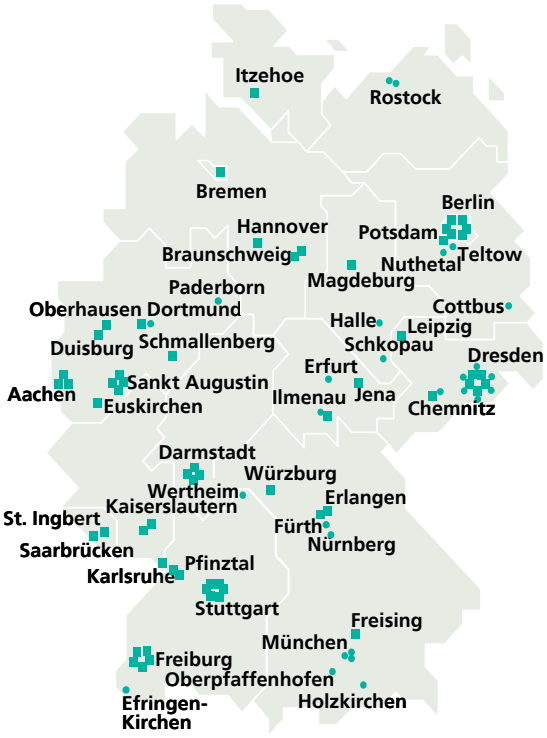
© Fraunhofer IT-Sicherheitskoordinator 3C

Fraunhofer

Fraunhofer Gesellschaft e.V.

- **Anwendungorientierte Forschung in technischen Bereichen**
- **Ca. 1,6 Milliarden € jährl. Forschungsvolumen, 1/3 grundfinanziert durch Bund und Länder 2/3 öffentlich geförderte und Industrieprojekte**
- **Ca 17000 Mitarbeiter in 60 Instituten in Darmstadt: SIT, LBF, IGD**

Fraunhofer



© Fraunhofer IT-Sicherheitskoordinator 3C

Cloud Computing als Forschungsgegenstand von Fraunhofer

Studie: Cloud Computing Sicherheit

Fraunhofer SIT

Fraunhofer CLOUD

Über uns
- Mitgliedsinstitute
- Historie
- Cloud Computing für die Logistik

Was ist die Cloud?
Leistungsspektrum
Projekte
Veranstaltungen
Kontakt

→ Fraunhofer-Gesellschaft

Die Institute der Fraunhofer-Allianz Cloud Computing:

Startseite > Über uns

Über uns

Fraunhofer-Allianz Cloud Computing

©iStockphoto - Okea

Die Fraunhofer-Allianz Cloud Computing

In einer Fraunhofer-Allianz organisieren sich Fachgruppen verschiedener Fraunhofer-Institute, die mit ihren Einzelkompetenzen ein gemeinsames, integratives Geschäftsfeld bearbeiten.

Mitglieder der Fraunhofer-Allianz Cloud Computing sind die Fraunhofer-Institute:

AI

Programm IT-Grundschutz-Tag 25.11.2010

Thema: Sicherheitsaspekte von Cloud Computing

Bundesamt für Sicherheit in der Informationstechnik

Der 4. IT-Grundschutz-Tag 2010 findet mit unserem Kooperationspartner, der Fraunhofer SIT, in Darmstadt statt.

© Fraunhofer IT-Sicherheitskoordinator 3C

Zusammenarbeit Hochschule / IT-Sicherheitskoordinator

- **IT-Sicherheit: Vermeiden, erkennen und aufklären**
  - Hackerangriffe
  - Missbrauch, rechtswidrige Nutzung
- **verwandte IT-Rechtsfragen, u.a.**
  - Datenschutz und -erklärungen
  - Rechtliche Anforderungen an Webdienste
  - Rechtmäßigkeit der Webserverprotokollierung


Fraunhofer Gesellschaft

Rechtliche Überprüfung
von Webauftritten
der Fraunhofer Gesellschaft

Praktikumsbericht

Darmstadt, Januar 2009

Bericht zur FhG-internen Verwendung.
Weitergabe nur mit Zustimmung des IT-Sicherheitskoordinators

Betreuer und Kontakt:
Dr. Ulrich Pordesch (3C), ulrich.pordesch@zv.fraunhofer.de

- **Zusammenarbeit bisher**
  - Informationsrechtliche **Praktika**
  - **Bachelorarbeiten**, z.B. Implementierung Verfahrensregister BDSG
  - SS 2010: **Seminar** „Informatik und Gesellschaft“, Bewertung neuer Webdienste

© Fraunhofer IT-Sicherheitskoordinator 3C

Cloud-Computing in der Fraunhofer Gesellschaft?

- **Infrastructure as a Service, Plattform as a Service kaum**
  - Netze, Rechner, Datenhaltung fast durchgängig in eigenen Räumen, Systemmanagement gelegentlich durch Dienstleister
  - Vorüberlegungen zu institutsübergreifender private Cloud
  - Cloud-Vorläufer: Grid Computing

- **Software as a Service kaum**
  - Cloud-Vorläufer: Outsourcing Lohnabrechnung, Spamfilterung
  - Office-Software, Kommunikationsplattformen,.. auf eigenen Systemen
  - Erste Anfragen: Sales-Force-Service als CRM

© Fraunhofer IT-Sicherheitskoordinator 3C

Inoffizielles „Cloud-Computing“ durch Mitarbeiter

- **Vorgekommen**
  - Synchronisierung von Terminen und Kontakten über Google-Mail
  - Terminfindung und Einladung über Doodle
  - Social Networking über XING, Twitter und Co
  - Bookmarking auch interner Ressourcen etwa über delicious
- **Möglich / vermutet**
  - Dokumentenverarbeitung über Google Docs
  - Textübersetzung bei babelfish.com oder translate.google
  - Mindmapping über mindmaster
  - Dokumentspeicherung bei Webmailern oder Dropbox
- **Cloud-Computing?**
  - Technisch teils ja: Google Docs, teils ortsgebunden (Doodle)
  - Rechtlich, aus Unternehmenssicht nur erheblich: Selbstorganisiertes Outsourcing von Daten und Datenverarbeitung an unbekannte, evtl. wechselnde Orte

© Fraunhofer IT-Sicherheitskoordinator 3C

Chancen und Risiken

- **Chancen aus Nutzersicht**
  - Ortsunabhängiges flexibles Arbeiten, zu Hause, im Urlaub, …
  - Oft kostenlos und sofort nutzbar, keine Warten auf die „träge“ Unternehmens-IT

- **Chancen aus Unternehmensicht**
  - Motivierte Mitarbeiter, hohe Verfügbarkeit
  - Kein teurer Aufbau eigener Services

- **Aber auch erhebliche Risiken**
  - Verletzung von Vorgaben und Richtlinien: BDSG, NDAs, Betriebsvereinbarungen..
  - Abfluss von Daten, Unternehmens Know-how: Hacker, Mitarbeiter, Wirtschaftsspione..
  - Schädigung/Gefährdung der unternehmnseigenen Infrastruktur
  - Reputationsschäden bei Datenskandalen, blamablen Statements,…

© Fraunhofer IT-Sicherheitskoordinator 3C

Konsequenzen?

- **Verbieten?**
  - Kundenanfordreungen können nicht ignoriert werden
  - Zu starke Einschränkungen gefährden Mitarbeitermotivation
  - Verwendung kaum kontrollierbar

- **Konsequenz: Versuch der Steuerung**
  - Regelungen, Dienstebewertung und Freigabeverfahren
  - Mitarbeitersensibilisierung

- **Herausforderung: Pragmatik**
  - Regelmäßig unpraktikabel (zu lange, zu teuer): Sicherheitstests, Rechtsgutachten
  - Gesucht sind handhabbare Regelungen, Prozesse, Hilfsmittel zu Risikominimierung

© Fraunhofer IT-Sicherheitskoordinator 3C

Regelung im IT-Sicherheitshandbuch

- Abschnitt „Webdienste“ in neuer Version, u.a.
  - Die eigenmächtige ungeprüfte Nutzung ist unzulässig.
  - Freigabe zur eigenen Nutzung erst nach einer Risikoanalyse im Hinblick auf Datenschutz und IT-Sicherheit und Prüfung der Nutzungsbedingungen
  - Die Freigabe im Institut erteilt der IT-Sicherheitsbeauftragte
  - Fraunhofer-weite Freigaben und Empfehlungen erarbeitet der IT-Sicherheitskoordinator
  - Gibt es fraunhofer-eigene vergleichbare Angebote keine Freigabe
  - Freigabe zur Nutzung auf Veranlassung von Partnern ist aber zu gestatten, wenn keine Gefährdung der eigenen IT-Infrastruktur erkennbar ist.
  - Werden Dokumente und personenbezogene Daten gespeichert, ist ein Dienstleistungsvertrag zwingend

© Fraunhofer IT-Sicherheitskoordinator 3C

Angestrebter abgestufter Bewertungs- und Freigabeprozess

- **Suche nach existierender Freigabe durch Mitarbeiter/Vorgesetzte**
  - Anhand Intraweb-Liste freigegebener und geprüfter Dienste, wenn nicht vorhanden ->
- **Schnellcheck durch lokalen IT-SiBe**
  - Checkliste mit den wichtigsten in 2-3 Stunden zu klärenden Fragen (Gefährdung eigener Infrastruktur, personenbezogene Daten
  - Kontextbezogene Freigabe zur Nutzung oder Eskalation ->
- **Bewertung beim ITSicherheitskoordinator**
  - Übergreifende Bewertung anhand Kriterienkatalog (Sicherheit, Recht, sonstige Aspekte)
  - Bei Bedarf: Rechtgutachten, Sicherheitstest durch Testlabor
  - Studie mit Bewertung und (ggf. an Bedingungen geknüpfte) Freigabe
  - Falls umstritten, zweifelhaft ->
- **Evtl. separat Vertragsaushandlung**
- **Ggf. Abstimmung mit einer Policy in Fraunhofer Gremien**

© Fraunhofer IT-Sicherheitskoordinator 3C

Schnellprüfung

- …
- Konkreter geschäftlicher Nutzen?
- Gleichwertiger Fraunhofer-eigener Dienst nicht vorhanden?
- Zustimmung Projektpartner oder legitimierende Vertragsregel?
- Anbieter bekannt und seriös?
- Keine Installation von Programmen (z.B. ActiveX) oder niedrige Sicherheitseinstellungen?
- Keine Personaldaten, sensiblen personenbezogenen Daten oder Betriebsgeheimnisse?
- Anbietersitz in der Europäischer Union?
- …

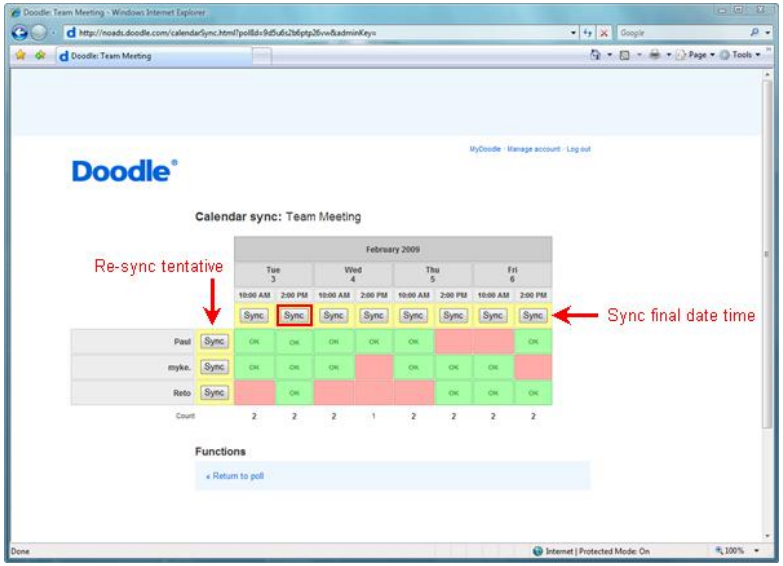
© Fraunhofer IT-Sicherheitskoordinator 3C

Bewertungsstudie

- **Dienstbeschreibung Webdienst, u.a.**
  - Anbieter und Herkunft, Finanzierung, Rollen, Datenexport,..
- **Technik, u.a.**
  - Server und Standorte, Technische Abläufe, Datenformate
- **Chancen und Risiken**
  - Kosten & Zeitersparnis, Kommunikationsförderung, Persönlichkeit..
  - Steuerungsverlust, Abhängigkeit, Know-how-Verlust, Reputationsschäden …
- **Technische Sicherheitsaspekte, insbesondere**
  - Datenarten, Betroffene, Schadenspotentiale, Sicherheitsmechanismen.
- **Rechtliche Sicherheitsaspekte, insbesondere**
  - Datenschutz, Lizenz- und Nutzungsvorausetzungen, Zulässigkeit der geschäftlichen Nutzung, Gerichtsstand / Anbieternationalität / Serverstandort
- **Schlussfolgerungen/ Handlungsempfehlung**

© Fraunhofer IT-Sicherheitskoordinator 3C

Beispiel: Terminabsprache über Doodle



© Fraunhofer IT-Sicherheitskoordinator 3C

Beispiel Doodle: Schnellprüfung

Ursprüngliche Vorbewertung:

○ …

☑ Konkreter geschäftlicher Nutzen?

☑ Gleichwertiger Fraunhofer-eigener Dienst nicht vorhanden?

☑ Zustimmung Projektpartner oder legitimierende Vertragsregel?

? Anbieter bekannt und seriös?

☑ Keine Installation von Programmen (z.B. ActiveX) oder niedrige Sicherheitseinstellungen?

? Keine Personaldaten, sensiblen personenbezogenen Daten oder Betriebsgeheimnisse?

☒ Anbietersitz in der Europäischer Union? *Schweiz*

○ …

© Fraunhofer IT-Sicherheitskoordinator 3C

Beispiel Doodle: Bewertungsstudie 2009 (1)

- **Mögliche Chancen, u.a.**
  - Zeit- und Kostenersparnis für die Mitarbeiter und Unternehmen
  - Aufwandsersparnis für eigene Angebote
  - Höhere Arbeitszufriedenheit
  - Mehr Kommunikation
- **Mögliche Risiken, u.a.**
  - Abhören von ungesicherten Verbindungen
  - Möglicherweise fehlerhafte oder manipulierte Plugins / ActiveX-Controls
  - Datenmissbrauch von Daten durch Betreiber
  - Verbreitung von Schadsoftware über hochgeladene Dateien
  - Kontakteabgleich, Zugriff auf Adressdaten
  - Hacken des Dienstes

© Fraunhofer IT-Sicherheitskoordinator 3C

Beispiel Doodle: Bewertungsstudie 2009 (2)

- **Rechtliche Aspekte, u.a.**
  - Gerichtsstand Zürich, schweizerisches Recht
  - Unklarheit über Datenspeicherung nach Accountlöschung bzw. Abschluss der Umfrage
  - Weitgehender Haftungsausschluss
  - Recht von Doodle zur Überprüfung von Inhalten und Konten
  - Steuerung von Werbeanzeigen durch Informationen, die bei Nutzung entstehen
  - Speicherung von IP-Adressen und E-Mail Adressen ohne Rechtsgrundlage

- **Handlungsempfehlung innerhalb der FhG**
  - Nutzung allenfalls ohne vollständige Klarnamen und Termininhalte, keine Uploads
  - Terminplaner des DFN nutzen (https://terminplaner.dfn.de/)

© Fraunhofer IT-Sicherheitskoordinator 3C

Zusammenfassung

- **Neue Webdienste mit Datenspeicherung im Netz sind eine große Herausforderung für die Unternehmenssicherheit**
- **Mit Regelungen muss man versuchen die chaotische Nutzung in den Griff zu bekommen.**
- **Neue Dienste sollten im Hinblick auf Gefährdungen der eigenen Infrastruktur, der Unternehmensgeheimnisse, rechtliche Zulässigkeit bewertet werden.**
- **Umfangreiche Test und Begutachtungen sind unpraktikabel. Ein abgestufter Prozess mit Schnellprüfungen, Studien und Policies könnte ein Weg sein.**

© Fraunhofer IT-Sicherheitskoordinator 3C

Ausblick

- **Bisher ist das Verfahren noch nicht voll ausgearbeitet und partiell erprobt**

- **Praktikabilität muss sich erweisen**
  - Ist der Aufwand leistbar?
  - Sind die Checklistenbewertungen und Vorbewertungen brauchbar oder werden sie pro Forma angewendet und umgangen?

- **Erleichterungen der unternehmensinternen Steuerung?**
  - Maßnahmen, Kriteriensysteme, Musterpolicies im BSI-Grundschutz?
  - Diensteklassen-bezogene AGB-Checklisten oder Technikchecklisten?
  - Zertifizierungen?

© Fraunhofer IT-Sicherheitskoordinator 3C

Danke für Ihre Aufmerksamkeit

Dr. Ulrich Pordesch
Fraunhofer Gesellschaft
IT-Sicherheitskoordinator
Rheinstraße 75
64295 Darmstadt

ulrich.pordesch@zv.fraunhofer.de
06151/869346

© Fraunhofer IT-Sicherheitskoordinator 3C