Der Preis moderner Hochschulkommunikation: Daten- und Netzunsicherheiten

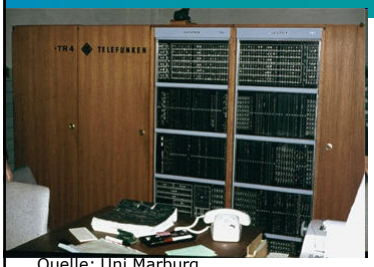
Prof. Dr. Rainer W. Gerling
Datenschutz- und IT-Sicherheitsbeauftragter
Max-Planck-Gesellschaft

Das Hochschul-Rechenzentrum: Sicht der RZ-Leiter

Quelle: LRZ

Quelle: FZ Jülich

Das Hochschul-Rechenzentrum: Sicht der User

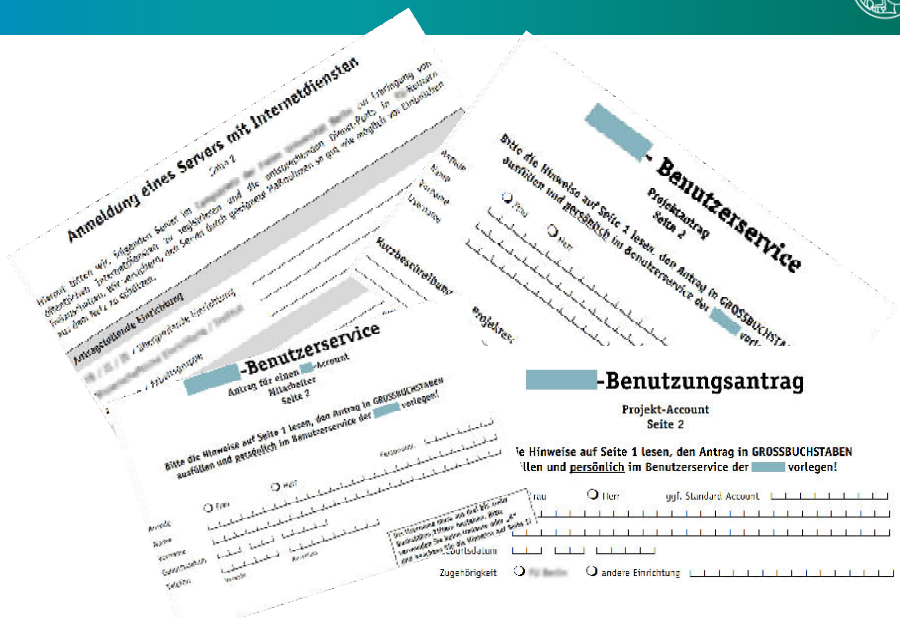


Quelle: Uni Marburg

Quelle: ChariPro

Quelle: GWDG

Formulare und Anträge



Die Erkenntnis!

Das kann ich besser!

Die Lösung!

Selber Machen!

Was es so alles gibt

Personal Outsourcing

- Mitarbeiter neigen heute dazu, an der EDV vorbei, IT-Dienstleistungen out zu sourcen.

- Vorteile
  - ✚ keine langwierigen Genehmigungsverfahren
  - ✚ der Dienst ist aus der privaten Nutzung bekannt
  - ✚ Hochschulübergreifende Dienste sind leicht zu realisieren
- Nachteile
  - – kein Vertrag zur Auftragsdatenverarbeitung
  - – unkontrollierte und unbekannte Datenflüsse
  - – Verletzung der arbeitsvertraglichen Schweigepflicht
  - – Verletzung des Datengeheimnisses
  - – Verletzung von Persönlichkeitsrechten
  - – interne Sicherheitsvorgaben, Dienstvereinbarungen und Nutzerordnungen werden umgangen
  - – technische Sicherheitsmaßnahmen werden unterlaufen

FreeMailer

- E-Mail bei FreeMailer mit forward in der Hochschule
  - Die Mitarbeiter setzen in der Hochschule nur noch ein forward nach GoogleMail/GMX/Web.de
    - Vacation-Nachricht von web.de bei E-Mail an Dienstadresse in der Hochschule
- Ist das akzeptabel?
- Hochschul-Daten bei Dritten (z.B. bei Google auch gleich im Ausland)
- Keine Forwards ohne Genehmigung zulassen?
  - Realistisch?

RUPRECHT-KARLS-UNIVERSITÄT HEIDELBERG
URZ-Startseite > E-Mail und WWW > E-Mail >

Vorsicht bei der Weiterleitung dienstlicher E-Mails

Automatisches Forwarden von sensiblen Daten nicht mehr zulässig – Umkehrung der Haftung im Schadensfall

In einem Rundschreiben an alle Beschäftigen der Universität wies das Rektorat jüngst darauf hin, dass die Weiterleitung dienstlicher E-Mails auf einen externen Mail-Server generell untersagt ist. Seither gingen am URZ zahlreiche Rückfragen ein, weshalb wir im Folgenden die wichtigsten Punkte klarstellen möchten.

Terminkalender

- Gruppen-Terminalkalender irgendwo Google kalender
  - Alle Daten inklusive Besprechungsinhalte beim Dienstleister
  - „Doodle: einfach abmachen“
    - Termine abstimmen
    - Umfragen erstellen
    - Aussage der User: Unverzichtbar

Doodle®

- Versuchen Sie mal über mehrere Hochschulen und zusätzlich mit (örtlichen) Unternehmen einen Termin abzustimmen.

z.B. Doodle

- http://www.doodle.ch/participation.html?pollId=et6dguqr7a9fqzhw

	Oktober 2008				November 2008		
	Mi 22		Do 23		Di 4		
	10:00	14:30	09:30	11:00	08:30	14:00	16:30
bea	OK		OK			OK	OK
gf				OK			
lmaa	OK	OK	OK	OK	OK	OK	OK
anneliese	OK		OK			OK	
Moffel		OK			OK		OK
Jona		OK			OK		
1234	OK	OK	OK	OK			
Ihr Name	☐	☐	☐	☐	☐	☐	☐
Anzahl	4	4	4	3	3	3	3

Teilnehmen

z.B. DFN Terminplaner

- https://terminplaner.dfn.de/foodle.php?id=ttpivxhmg0uymigc

Test Termin

Wichtige vertrauliche Besprechung

Dieser Terminplaner hat ein Ablaufdatum
2010-06-17 16:00 (expires in 3 Tagen)

Ihre hier gemachten Angaben sind für alle Personen sichtbar, die auf diese Terminplanung zugreifen können. Alle Ihre Angaben werden ausschließlich für die Zwecke dieser Terminplanung gespeichert und zum oben genannten Ablaufdatum gelöscht.

Eigene Antwort

Tragen Sie unter Angabe eines Pseudonyms oder Ihres Names Ihre bevorzugten Zeiten für diesen Termin ein. Optional können Sie einen Kommentar verfassen, der dann für alle Personen sichtbar ist, die auf diesen Terminplan zugreifen können. Wenn Sie dieser Seite (https://terminplaner.dfn.de) erlauben ein Cookie zu speichern, dann können Sie Ihre Angaben später noch ändern.

Name	14. Jun 2010 16:00	15. Jun 2010 9:00	16. Jun 2010 14:00	
Max Mustermann	☑	☑	☐	Bestätigen

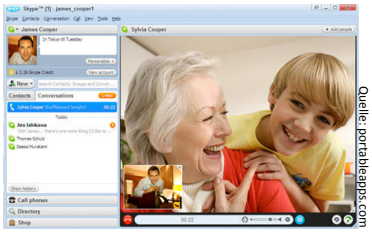
Bisherige Antworten

Nachfolgend sehen Sie die bisherigen Antworten auf diesen Terminplan. Sofern ein Teilnehmer einen Kommentar hinterlassen hat, erscheint vor seinem Namen ein Symbol. Klicken Sie auf das Symbol, wenn Sie den betreffenden Kommentar lesen wollen.

Name	14. Jun 2010 16:00	15. Jun 2010 9:00	16. Jun 2010 14:00	Aktualisiert vor
Max Mustermann	✓	✓	✗	0 Sek
Demo user	✗	✓	✓	1 Min
Ergebnis	1	2	1	

skype

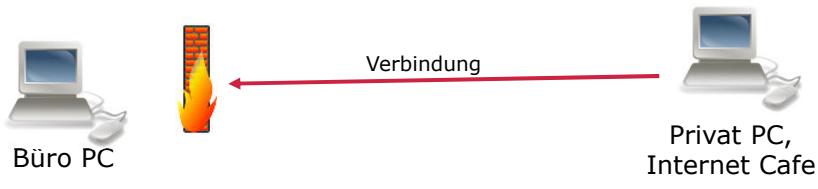
- Kostenlose Video- und Sprachtelefonie
  - Die gesamte Kommunikation ist verschlüsselt, aber nicht offen gelegt
  - Das am besten gegen Analyse geschützte Programm der Welt
  - Auch im „Ruhezustand" fließen Daten
  - Bohrt sich ein Loch in fast jede Firewall
    - New Generation Firewalls können helfen
  - Startet ohne Installation vom USB-Stick
  - Dateiaustausch
- Vermeintliche „Lösung" für:
  - Verbot Privatgespräche
  - Keine Amtsberechtigung
  - Keine Auslandsberechtigung


Quelle: portableapps.com

- In einigen Hochschulen (verboten) unerwünscht
- Daheim durchaus ok!

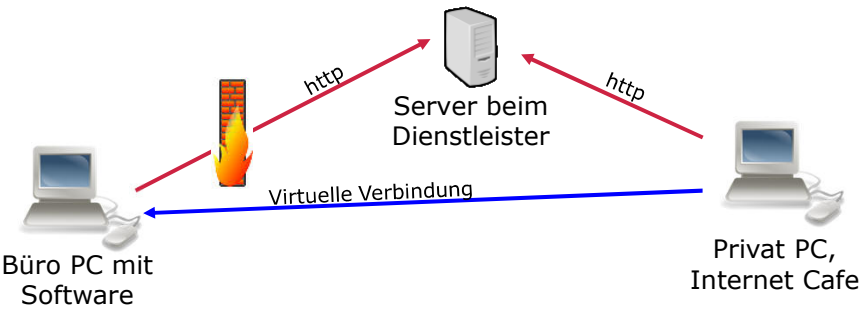
Zugriff ins Büro

- Zugriff von außen auf den PC im Unternehmen
  - Remote Desktop, VNC, …
- Die Hochschul-Firewall blockt die eingehende Verbindung
- Ein Trick hilft



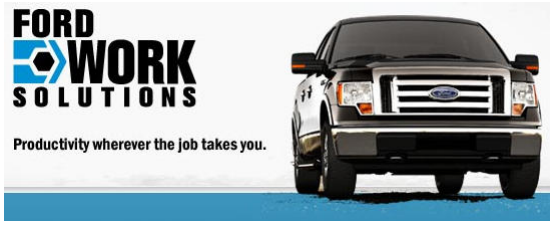
Mein Desktop

- Mitarbeiter installieren und nutzen die kostenlose Software eines Dienstleisters
- Einige Dienstleister können über die Firewall gut blockiert werden.
- Sieht der Dienstleister den Datenverkehr?

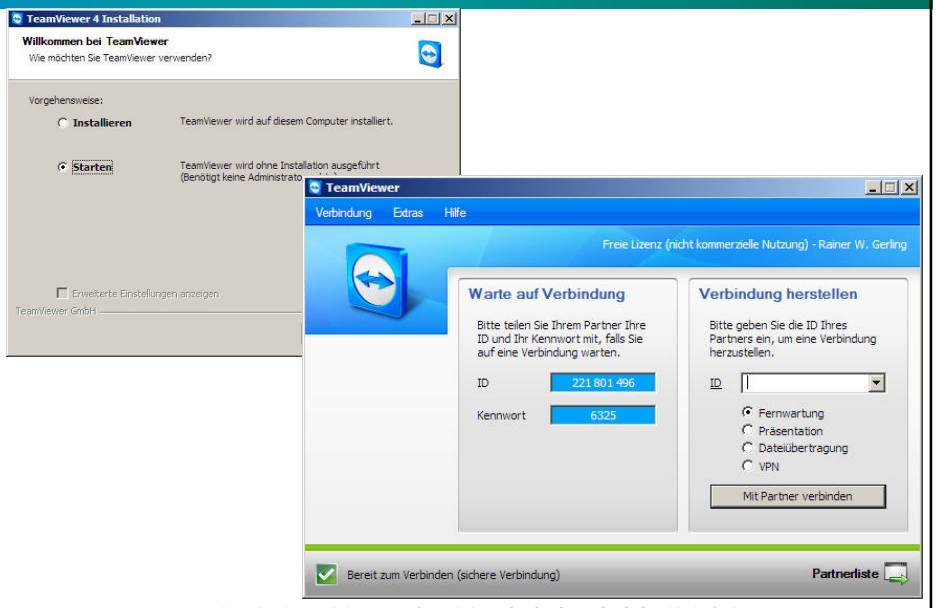


LogMeIn

- „Sie können sogar über Ihr iPhone/iPad oder das Armaturenbrett Ihres Ford auf Ihren PC zugreifen."

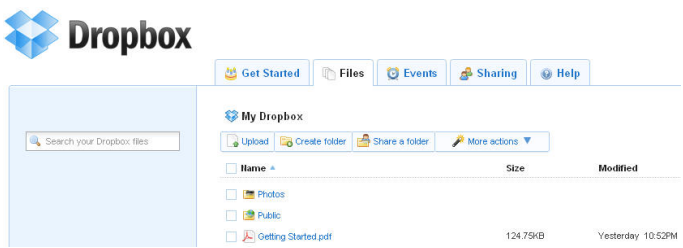


Teamviewer



Datenspeicherung bei Dienstleistern

- Daten können im Sinne von „Netzwerklaufwerk" beim Dienstleister gespeichert werden
  - Gegen geringe Gebühr beliebig groß
  - Kostenlose Angebote
    - Windows Live Skydrive (25 GB)
    - Telekom Cloud (25 GB)
    - Starto HiDrive free (5 GB)
    - DropBox (2 GB)
    - GMX (1 GB)

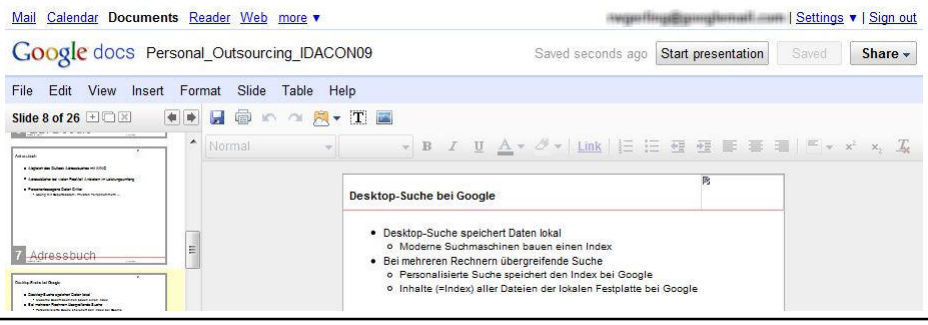


Cloud Verschlüsselung

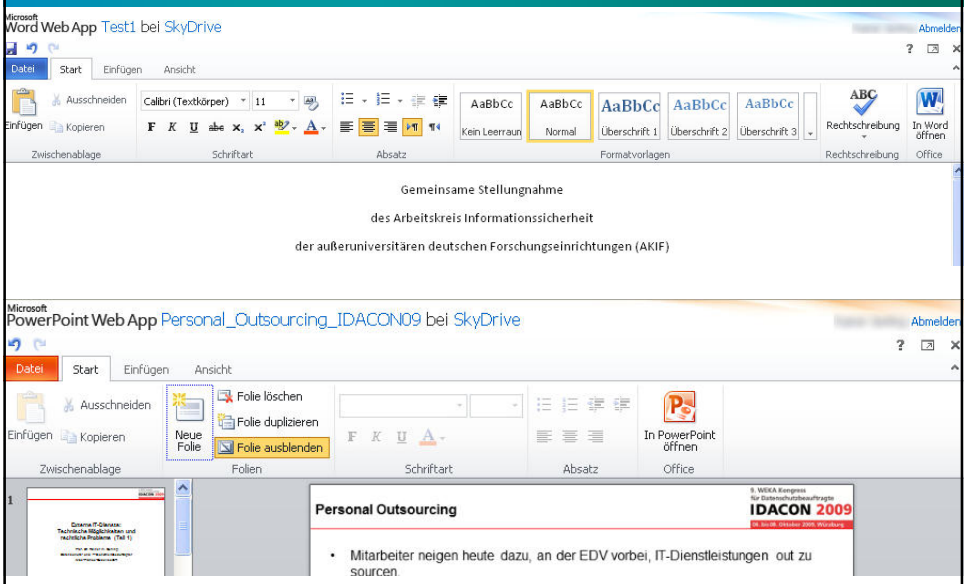
- Verschlüsselte Speicherung ist leider kaum ein Thema
- Teamdrive als Software
  - Datenschutzzertifikat des ULD
  - 2 GB kostenlos
  - Eigener Server möglich
- DropBox verschlüsselt
  - BoxCryptor/EncFS
    - Windows/Mac/Linux/iOS/Android
    - Bis zu 2 GB Kostenlos
  - Kommerzielle Lösungen
    - Z.B. Sophos Encryption für Cloud Storage
- SpiderOak
  - Kostenlos mit Verschlüsselung auf dem Klienten
  - Windows/Mac/Linux

Online-Officeprogramme

- Word, Excel und Co. als Applet im Browser
- Datenspeicherung ist zwar lokal auf der Festplatte möglich aber
- Überall Zugang nur bei der Speicherung beim Dienstleister
  - Google text & tabellen
    - Textverarbeitung, Tabellenkalkulation, Präsentation
  - Microsoft Office 2010 Web Apps
    - „the online companion to Word, Excel®, PowerPoint® and OneNote® applications"

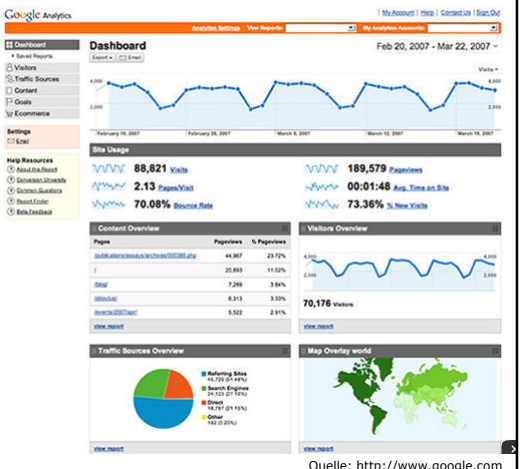


Microsoft Office Web Apps



Google Analytics

- Ein Dienst zur Analyse des Nutzerverhaltens auf einer Web-Seite
  - weltweit mehr als 5 Mill. Accounts
  - es wird ca. 21 KBytes Javascript Code in die Seite eingefügt
- Überträgt Nutzungsdaten (incl. IP-Adresse) der Besucher einer Web-Seite an Google
- Datenschutz
  - rechtlich in Deutschland nicht zulässig
  - Information der Besucher der Webseite mit opt-out



Quelle: http://www.google.com

Adressbuch

- Abgleich des Outlook Adressbuches mit Sozialen Netzen und Mail-Anbietern
  - Sind da alle mit einverstanden
- Adressbücher bei vielen FreeMail Anbietern im Leistungsumfang
- Personenbezogene Daten Dritter
  - Häufig mit Geburtsdatum, Privaten Telfonnummern …
- Einige Anbieter nutzten anschließend alle Adressen aus dem Abgleich(versuch)
- Mobile Dienste laden Telefonbuch zum Dienstanbieter hoch

WhatsApp

- Bei jedem Start der Software werden die Teleffummnernübertargen

0160-88012345

0161-12345678
0183-23456789
…

0161-12345678

0160-88012345
0172-23456789
…

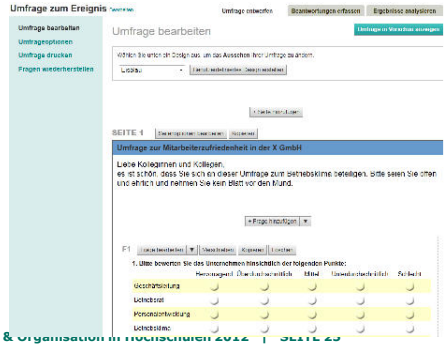
WhatsApp

0160-88012345
0161-12345678
0170-45678923
0171-67891234
…

iPhone,
BlackBerry,
Nokia, Android,
Windows Phone

SurveyMonkey

- Mal schnell eine Umfrage machen
  - Marktforschung, Kundenzufriedenheit
  - Mitarbeiterzufriedenheit
  - Kundenfeedback
  - Produktplanung, -optimierung
  - Ausbildung & Schulung, Auswertung
- http://www.surveymonkey.com/s/G2QXVQ3
  - Link per E-Mail verschicken
  - An allen Kontrollen vorbei
  - Kostenlos:
    - 10 Fragen/Umfrage
    - 100 Beantwortungen
    - Genug für ein Team/eine Abteilung/ein Projekt



Skymem.com

- Sie haben eine Datei mit E-Mail-Adressen
  - Eine Log-Datei
  - Ein Firmen-Telefonbuch
  - Ein Forum
  - ….
- Die E-Mail-Adressen manuell zu extrahieren, ist mühsam
- Skymem macht das automatisch, aber
  - Alle Dateien sind öffentlich!!!!!
  - Ein Paradies für Spammer

Do not post your confidential data here! All data is public!

- Hochschuldaten haben dort nichts verloren

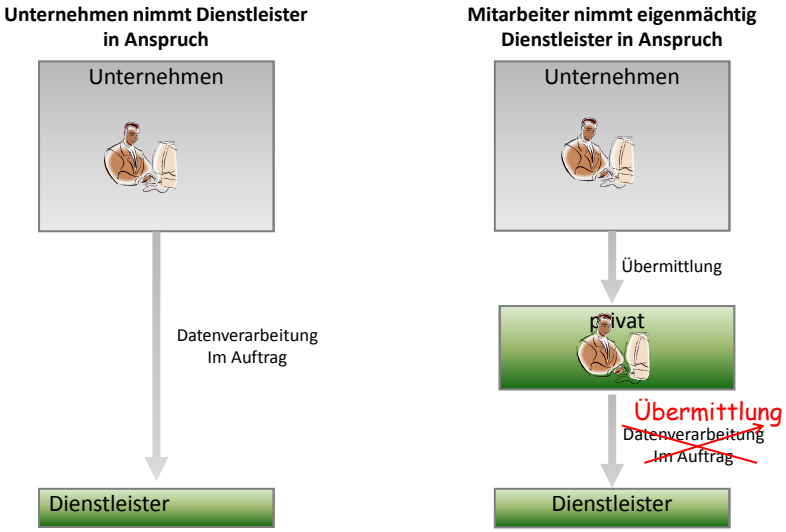
Size: 1058470(byte); - Your IPAddress: 84. - Current Time:4/25/2011 3:15:17 PM

[redacted]bravo@yahoo.com,Den[redacted]765 Treasure Ave,Wa[redacted]6.166,2011-03-03 07:45:00,
[redacted]@bellsouth.net,Dennis [redacted] Bogey Way,Henders[redacted]2/11/2011 8:16,
[redacted]rtez69@yahoo.com,De[redacted],6593 Wagner,Detroi[redacted]eb 8 2011 16:30:12,
[redacted]emay1953@yahoo.con[redacted]ay,276 Gilford Aven[redacted]2.70,02/11/2011 7:12,

Rechnen

- Die Beantragung von Rechenzeit ist aufwendig
- Man braucht sofort schnelle Ergebnisse
- CPU-Zeit kaufen, mit der Kreditkarte bezahlen und zur Erstattung einreichen
- Ausprobieren mit kostenloser Rechenzeit

Die rechtliche Beurteilung



Heimatschutz vs. Die Wolke

Patriot Act und Cloud Computing

Zugriff auf Zuruf?

Arnd Böken

Die Nennung des amerikanischen „Patriot Act" löst bei vielen Unbehagen aus, steht das Gesetz doch für den potenziellen Zugriff von US-Behörden auf Cloud-Daten deutscher Unternehmen. Die Datenschützer wollen die Notbremse ziehen, europäische Politiker arbeiten schon an einem Gesetz. Was sollen deutsche Unternehmen nun tun?

- **Microsoft** garantiert keinen Verbleib von Daten in einer EU/EWR-Cloud, das hatte schon Gordon Frazer im Juni klargestellt.
- Die Cloud-Anbieter **Salesforce**, **IBM**, **Amazon** und **Google** reagierten nicht auf die Anfrage.

Quelle: iX 1/2012

Gemeinsame Stellungnahme

Gemeinsame Stellungnahme

des Arbeitskreises Informationssicherheit
der außeruniversitären deutschen Forschungseinrichtungen (AKIF)
und
des Arbeitskreises der Datenschutzbeauftragten
der Helmholtz-Gemeinschaft Deutscher Forschungszentren e.V.
zur

Unberechtigten Nutzung externer IT-Dienstleistungen

Regelung

- Unberechtigten Nutzung externer IT-Dienstleistungen
  - Eine eigenmächtige, ungeprüfte und damit unberechtigte Nutzung externer Dienstleistungen durch Beschäftigte und sonstige in der Forschungseinrichtung tätige Personen ist sowohl aus datenschutzrechtlichen als auch aus IT-sicherheitstechnischen Gründen abzulehnen und gefährdet die Forschungseinrichtung!
- Vollständiger Vorschlag für eine Regelung über den DFN-Verein verfügbar

Gegenmaßnahmen

- Bewusstsein bei den Beschäftigten schaffen
  - Mitarbeiter stellen Supportanfragen beim Helpdesk, da Mail-Forward nach Google nicht funktioniert
- Was kann eine Universität dagegen halten?
  - Firewalls? Verbote?
    - z.B. Forwards nur mit Genehmigung zulassen; technisch unterbinden
  - Uni-RZ muss eine vergleichbare Dienstleistungsqualität zur Verfügung stellen

Das geht nur gemeinsam.

Die wichtigsten Tools

- Dropbox-Alternative
  - Den Charme macht der Klient aus
  - Zumindest Verschlüsseln
    - BoxCryptor/EncFS
- Office in der Wolke
  - Microsoft / SharePoint
- Google Analytics Alternative
  - Piwik
- Kollaboration/Wiki/…
  - Doodle → DFN Terminplaner
- Telefone: Skype vs. DFNFernsprechen
  - Cisco unterstützt uns mit Cisco Jabber Video for TelePresence (FreeMovi)
- Und alles muss tauglich sein

Gemeinsame Stellungnahme

des Arbeitskreises Informationssicherheit
der außeruniversitären deutschen Forschungseinrichtungen (AKIF)
und
des Arbeitskreises der Datenschutzbeauftragten
der Helmholtz-Gemeinschaft Deutscher Forschungszentren e.V.
zur

Unberechtigten Nutzung externer IT-Dienstleistungen

In Forschungseinrichtungen nutzen Beschäftigte und sonstige dort tätige Personen ohne Genehmigung und Beteiligung der eigenen IT-Abteilung oder sonstiger administrativer Abteilungen Dienstleistungen externer Diensteanbieter, weil diese vermeintlich besser, effizienter oder einfacher zu bedienen sind. Insbesondere sind die diversen Dienste von Google, Microsoft Live und anderen zu nennen. Allen diesen Diensten ist gemeinsam, dass der Nutzer - und damit letzendlich auch die Forschungseinrichtung - aufgrund bestehender Bedingungen der Nutzung, einem unklaren Speicherort der Daten und der Übertragung von Nutzungsrechten an die Diensteanbieter die Kontrolle über die Daten verliert.

Da es sowohl arbeitsvertragliche Verschwiegenheitspflichten als auch gesetzliche Vorgaben bezüglich der Verarbeitung personenbezogener Daten, Verkehrsdaten im Telekommunikationsbereich und Nutzungsdaten im Telemedienbereich - um nur einige Datenarten zu nennen - gibt, kann ein solcher externer Dienstleister nur genutzt werden, wenn den gesetzlichen und sonstigen Belangen durch angemessene Verträge zwischen der Forschungseinrichtung und dem Dienstleister Rechnung getragen wird. Kriterien für die Auswahl von IT-Dienstleistern sind Datensicherheit, Datenschutz und der Schutz der Forschungsdaten vor Missbrauch. Dies ist durch die zuständigen administrativen Stellen der Forschungseinrichtung sicher zu stellen!

Eine eigenmächtige, ungeprüfte und damit unberechtigte Nutzung externer Dienstleistungen durch Beschäftigte und sonstige in Forschungseinrichtungen tätige Personen ist sowohl aus datenschutzrechtlichen als auch aus IT-sicherheitstechnischen Gründen abzulehnen und gefährdet die Forschungs-einrichtung!

Leipzig/Halle im Oktober 2009

Dr. Karen Altermann
Vorsitzende des Arbeitskreises
der DSB der HGF

Prof. Dr. Rainer W. Gerling
Vorsitzender des Sprecherkreises
des AKIF

