

ZIM

Zentrum für Informations- und Mediendienste

UNIVERSITÄT
DUISBURG
ESSEN

Offen im Denken

"It's not a question of if employees will bring their own mobile devices to work and connect to your systems. It's a matter of when."
Malcolm Harkins, CISO Intel

Bring Your Own Device - Auswirkungen mobiler Endgeräte auf Identitymanagement und Datenschutz

Dr.-Ing. Andreas Bischoff
Zentrum für Informations- und Mediendienste
Universität Duisburg-Essen

Herbsttreffen ZKI AK Verzeichnisdienste
Kaiserslautern 2013



Agenda

- Motivation
- Was ist das?
- Warum ist das (jetzt) ein Hype?
- BYOD an Hochschulen
- Voraussetzungen
- Nutzen - Vorteile - Dr. Jekyll
- Gefahren - Nachteile - Mr. Hyde
- Rechtliches
- Auswirkungen auf IDM
- Zusammenfassung - Tipps



Quelle: Wikipedia

Motivation

- Mobile Geräte
- Mobiles Internet
- Mobile Learning
- Android





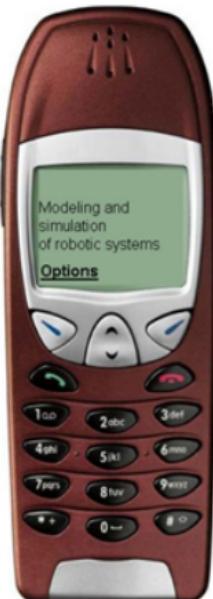
m-Learning Voraussetzungen II

Benutzbarkeit, Grafikauflösung:

- Mobiltelefone typisch: 176x220 (genug für kontextabhängiges Lernen / Informationsbeschaffung)
- Smartphones / PDAs bis zu 640x480 (genug für HTML oder PDF basiertes Material und für fernbediente Experimente)



WAP PocketPC 320x240 Pixel Smartphone 640x480 Smartphone 176 x 220 ^



This means:

$$\delta W = \mathbf{F}_i \Delta \mathbf{r}_i$$

If we now regard the complete open-chain kinematics as a whole consisting of n links and possessing k degrees of freedom of motion, it can be shown that:

$$\delta W = \sum_{j=1}^n \sum_{i=1}^k \mathbf{F}_j \frac{\partial \mathbf{r}_i}{\partial q_i} \delta q_i = 0 \quad (6)$$

Homogeneous transformations

We return to the description of general locations (position and orientation) in 3D space. As a result of our previous considerations we have found it sufficient in order to describe locations, that we apply a position vector \mathbf{d} to describe translations with respect to a reference frame, and an orientation matrix \mathbf{R} to describe rotations.

Figure 2.5 assumes, that the location of a cube is available via position vector and orientation matrix. Position P of the corner opposite to the bodies frame 1 is known relative to the body frame via \mathbf{p}_{1P} .

m-Learning Voraussetzungen II

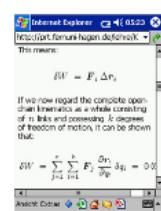
Benutzbarkeit, Grafikauflösung:

- Mobiltelefone typisch: 176x220 (genug für kontextabhängiges Lernen / Informationsbeschaffung)
 - Smartphones / PDAs bis zu 640x480 (genug für HTML oder PDF basiertes Material und für fernbediente Experimente)

WAP PocketPC 320x240 Pixel Smartphone 640x480 Smartphone 176 x 220



Ortsbezogene Wikipedia Sprachdienste
für Mobiltelefone und PDAs



Homogeneous transformations



Ortbezogene Anwendungen
und Dienste, München 2007

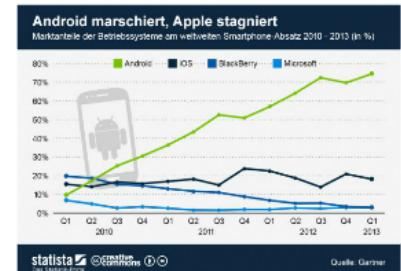




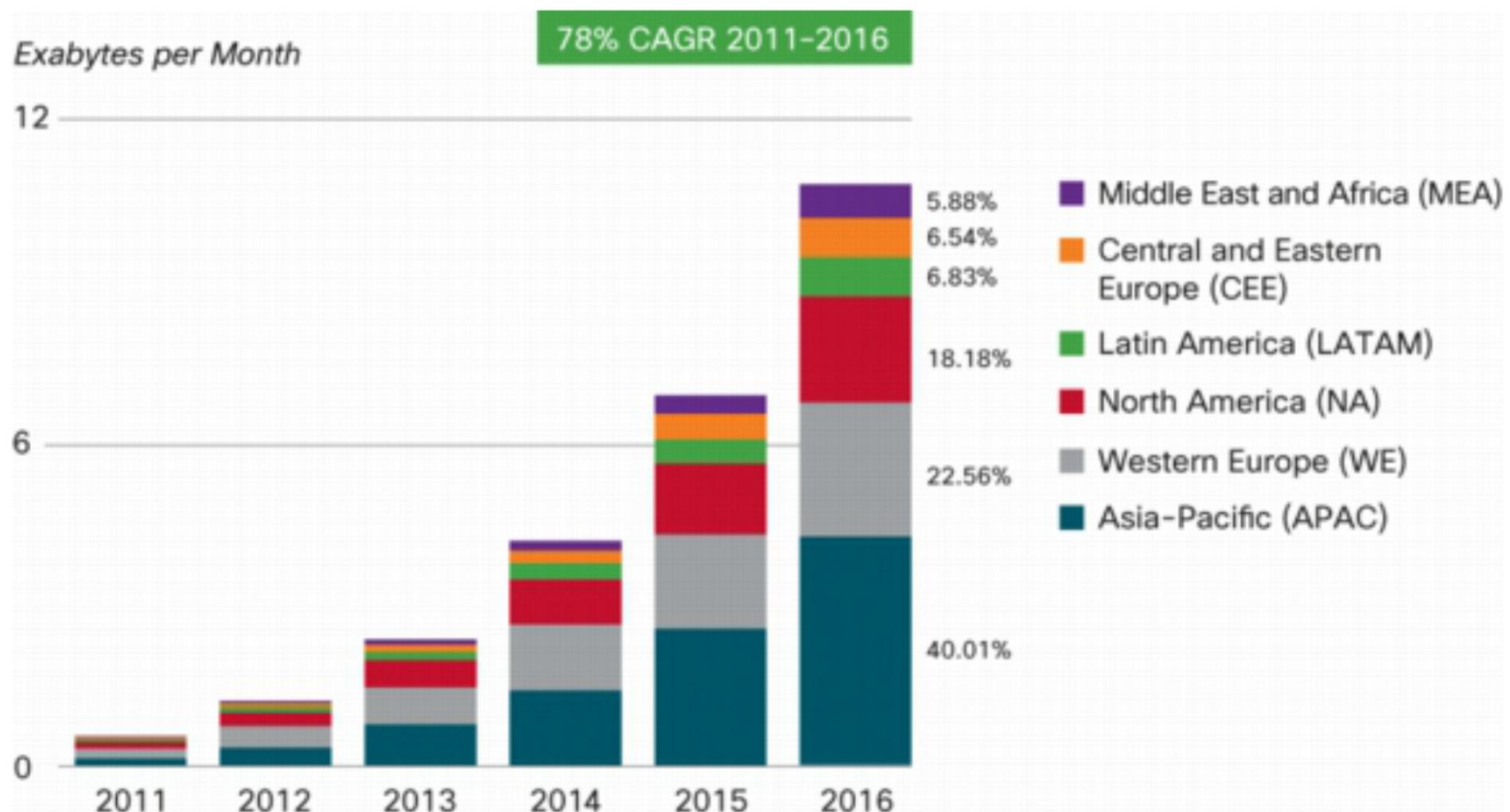
Was ist "Bring your own device" BYOD?

- Intel erlaubte es im Jahre 2009 seinen Beschäftigten ihre privaten Geräten am Arbeitsplatz zu nutzen
- Warum ist das ein Hype?
 - Kostenersparnis? - Nein!
 - Erfolg mobiler Geräte wie Smartphones, Tablets, Netbooks, Notebooks (verdrängen PCs)
 - Smartphones verdrängen herkömmliche Mobiltelefone in Deutschland
 - Nutzer bringen private Geräte mit und nutzen Sie auch für dienstliche Daten (E-Mail)
 - "It's not a question of if employees will bring their own mobile devices to work and connect to your systems. It's a matter of when."

Malcolm Harkins, CISO Intel



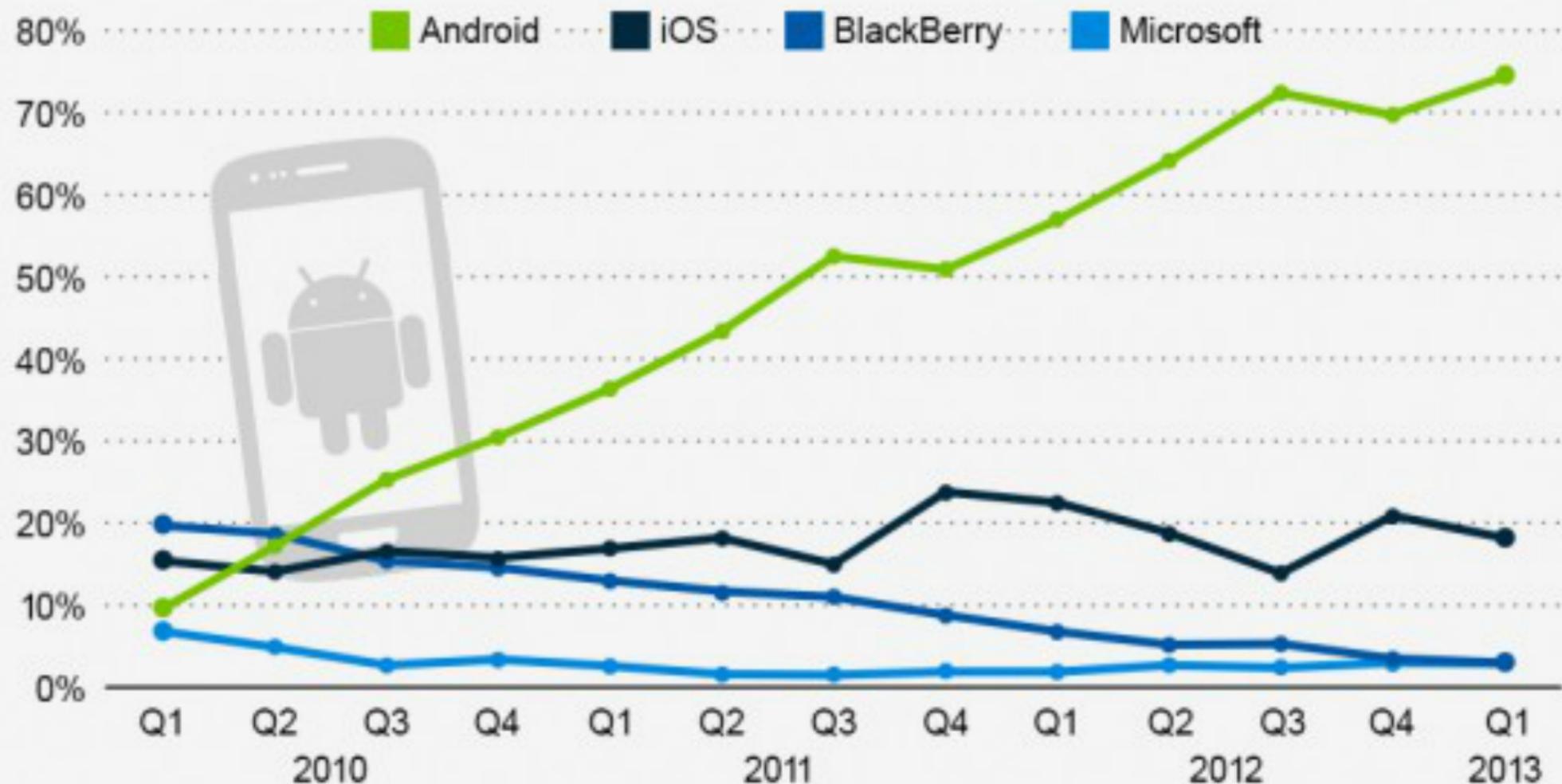
Mobiler Daten-Traffic = e-Funktion!



Source: Cisco VNI Mobile, 2012

Android marschiert, Apple stagniert

Marktanteile der Betriebssysteme am weltweiten Smartphone-Absatz 2010 - 2013 (in %)



BYOD an Hochschulen

- Lange Tradition bei wissenschaftlichen Mitarbeitern und Professoren
- "freier" Umgang mit der Thematik an Hochschulen
- WLAN-Ausbau eduroam für Studierende und Mitarbeiter
- preiswerte Netbooks → Studierende
- Preisverfall bei UMTS-Datenflatrates (2-10 € monatlich) und Smartphones (Android-Smartphones unter 100 €)
- Technische Voraussetzungen seit 5 Jahren vorhanden, Kosten 2007: 60-100€ pro Monat (24 Monate-Vertrag)
- Neue Szenarien über die mobile Nutzung des Webangebotes hinaus, mobile learning, Kommunikationsdienste
- Klinikum iPhones

Voraussetzungen - Technisch:

- Mobile Computing – Notebooks -Netbook -Tablets – Smartphones
- WLAN vs. UMTS, LTE (Kapazitätsgrenzen, Femtocel?)
- Offene Standards an der Hochschule (keine abgeschlossenen vereinheitlichten Welten)
- eduroam
 - In den eduroam-Netzen: „Jeder in seinem Subnetz“ - keine Broadcasts
- Sicherheit – Viren Scanner
- Trennung dienstlicher von privaten Daten
 - z.B. Containerlösungen
 - "Merkel-Phone" (Samsung Galaxy S2, S3 mit Mirokernel)
 - Blackberry 10 mit Microkernel (QNX)
 - gesicherter dienstlicher Bereich
 - Transportverschlüsselung
 - Storage-Verschlüsselung
- Remote Desktop
- Virtual Desktop Infrastructure (VDI)
- VPN für alle Plattformen
- Festplatten/Flash-Dateisystemverschlüsselung
- Webanwendungen/Virtual Desktop Infrastruktur





81



15:45

Fing

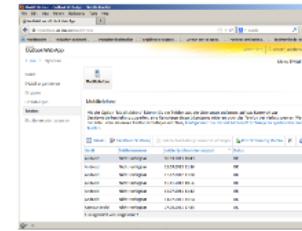


	"eduroam" Wireless network	444/444
	131.246.32.3 00:26:08:XX:XX:XX	eduroam-ipv4-0003.triple-a.uni-kl.de Apple
	131.246.32.4 14:F4:2A:XX:XX:XX	eduroam-ipv4-0004.triple-a.uni-kl.de
	131.246.32.6 78:E4:00:XX:XX:XX	MININT-BNS35BU Hon Hai Precision
	131.246.32.9 F8:DB:7F:XX:XX:XX	eduroam-ipv4-0009.triple-a.uni-kl.de HTC
	131.246.32.11 14:10:9F:XX:XX:XX	eduroam-ipv4-0011.triple-a.uni-kl.de
	131.246.32.14 10:68:3F:XX:XX:XX	eduroam-ipv4-0014.triple-a.uni-kl.de
	131.246.32.17 18:87:96:XX:XX:XX	eduroam-ipv4-0017.triple-a.uni-kl.de HTC
	131.246.32.18 60:21:C0:XX:XX:XX	eduroam-ipv4-0018.triple-a.uni-kl.de
	131.246.32.20 10:68:3F:XX:XX:XX	eduroam-ipv4-0020.triple-a.uni-kl.de
	131.246.32.22 74:E1:B6:XX:XX:XX	eduroam-ipv4-0022.triple-a.uni-kl.de Apple
	131.246.32.25 9C:4E:36:XX:YY:XX	eduroam-ipv4-0025.triple-a.uni-kl.de Intel



Voraussetzungen - Organisatorisch:

- Identitymanagement
- Verwaltungsmöglichkeiten externer Clients
(Beispiel Exchange2010, Remote wipe)
- Benutzerhilfen
- know how – Betriebssysteme – Mobilplattformen - Benutzerberatung - FAQ
 - früher: Early Adopter sorgten für Doku und konfigurierten selbst
 - heute: Kunden verlangen die Konfiguration als Dienstleistung
- Dienstvereinbarungen
- Speicherung und Verarbeitung dienstlicher Daten auf privaten Geräten.
- Mobile Device Management
 - Geräte sind oft nur für den Privatbetrieb gedacht, z.B. Android bis 4.2 nur ein Nutzerprofil
 - z.B. iPad, IOS: E-Mail-Client nicht deaktivierbar, auch nicht kurzfristig durch „falsches Passwort“
- Softwareverteilung - Lizenzen
- BYOD policy (Benutzerordnung)





Konto

E-Mail organisieren

Gruppen

Einstellungen

Telefon

Blockieren oder zulassen

**Mobiltelefone****Mobiltelefone**

Mit der Option "Mobiltelefone" können Sie ein Telefon aus der Liste unten entfernen, auf das Kennwort zur Gerätewiederherstellung zugreifen, eine Remotegeräte zurücksetzung initiieren oder das Telefon bei Verlust sperren. Wenn Sie der Liste unten ein neues Telefon hinzufügen möchten, konfigurieren Sie das mit Microsoft Exchange zu synchronisierende Telefon.

Details	Gerät zurücksetzen	Wiederherstellungskennwort anzeigen	Protokollierung starten	X	C
Gerät	Telefonnummer	Letzte Synchronisierungszeit	Status		
Android	Nicht verfügbar	18.03.2013 18:43	OK		
Android	Nicht verfügbar	13.03.2013 11:16	OK		
Android	Nicht verfügbar	12.12.2012 11:38	OK		
Android	Nicht verfügbar	13.11.2012 19:56	OK		
Android	Nicht verfügbar	15.07.2011 11:12	OK		
Android	Nicht verfügbar	11.07.2011 15:24	OK		
MotoAndroid	Nicht verfügbar	27.05.2011 17:45	OK		
1 ausgewählt von insgesamt 7					



2:34



Remote-Sicherheitsverwaltung

Einstellungen des Eingangsservers werden überprüft...

Der Server owa2010.uni-due.de erfordert die Erlaubnis
zur Remote-Steuerung einiger Sicherheitsfunktionen auf
Ihrem Telefon. Möchten Sie die Einrichtung dieses
Kontos abschließen?

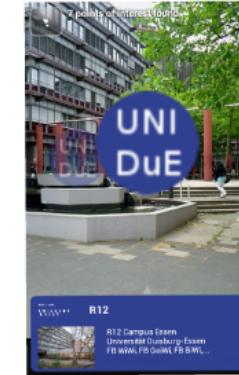
OK

Abbrechen

Abbrechen

Vorteile - Nutzen für die Hochschule:

- Kosten sparen (Hauptargument, Grund für den Hype [Computerwoche: Hype ebbt ab])
- schnelle Reaktion auf neue Geräte
- Freiheit der Forschung und Lehre
- fördert Erreichbarkeit



Nutzen für die Kunden:

- Keine zwei Landschaften pflegen
- Diversität Betriebssysteme
- Early Adopter haben alle Freiheiten
 - z.B. importierte Geräte aus China
- Freiheit in der Nutzung moderner Clouddienste
- Synergieeffekte durch eingebrachtes Know How
- fördert Homeoffice
- Kundenzufriedenheit
- ganz neue Szenarien möglich für m-Learning
 - Voting-Apps
 - Interaktion
 - Virtual Reality

Nachteile/Gefahren:

- 'bring your own disaster'
- Security nightmares
- Filesharing (Störerhaftung)
- Viren/Würmer
- Passwörter und Profile bei Dienstleistern wie Google und Apple
- Dienstliche Daten in der Cloud (Apple: iPhone Fotos, iCloud, Microsoft Skydrive)
- Datenschutz - Mischung dienstlicher und privater Profile/Daten
- Remote Wipe betrifft auch private Daten

- Ortsbezogene Dienste: Sie zahlen mit Ihren Daten (z.B. Bewegungsprofile sind möglich)
- Weitergabe Daten anderer Nutzer – Stichwort „WhatsApp“, Facebook, Google Kalender
- Weitergabe Adressbuch/Telefonbuch (iOS bis 4)
- Kalender E-Mail Kontakte
 - Synchronisation ohne cloud möglich?
 - Problem Google Kalender!
 - iPhone sync per Kabel?
- Biometrische Daten - iPhone 5S!
- TSM-Sicherung privater Daten?
- Gestohlene Geräte (remote lock and wipe)
- Defekte Geräte
- Jailbreak – „rooten“ (kann auch nützlich sein für BYOD, customized devices)
- Work life balance
- Läuft Vereinheitlichung entgegen



BACKUP UND WIEDERHERSTELLUNG

Meine Daten sichern

App-Daten, WLAN-Passwörter
und andere Einstellungen auf
Google-Servern sichern



Sicherungskonto

Das Sicherungskonto muss eingerichtet
werden.

Autom. Wiederherstellung

Stellen Sie nach der
Neuinstallation einer App
gesicherte Einstellungen und
Daten wieder her.



PERSÖNLICHE DATEN

Auf Werkszustand zurück

Löscht alle Daten auf dem Telefon



Standortzugriff

Zugriff auf meinen
StandortMeine Standortdaten dürfen
von Apps verwendet werden,

AN



Standortfreigabe

Ermöglicht dem Google-
Standortdienst, anonyme
Standortdaten zu erfassen. Einige
Daten werden möglicherweise auf
Ihrem Gerät gespeichert. Die
Erfassung erfolgt gegebenenfalls
auch dann, wenn gerade keine Apps
ausgeführt werden.

Ablehnen

Zustimmen





★★★★★ (76.787)

Kostenlos

**Yoke Messenger**

NHH DEVELOPER INC.

★★★★★ (1.021)

Kostenlos

**pMessenger**

HAMBEL-SOFTWARE

★★★★★ (7.220)

Kostenlos

**TalkBox Voice Messenger ...**

TALKBOX LIMITED

★★★★★ (16.393)

Kostenlos

IHRE NACHRICHTEN

SMS EMPFANGEN

Ermöglicht der App, SMS zu empfangen und zu verarbeiten. Das bedeutet, dass die App an Ihr Gerät gesendete Nachrichten überwachen und löschen kann, ohne sie Ihnen anzuseigen.

NETZKOMMUNIKATION

ZUGRIFF AUF ALLE NETZWERKE

Ermöglicht der App die Erstellung von Netzwerk-Sockets und die Verwendung benutzerdefinierter Netzwerkprotokolle. Der Browser und andere Apps bieten die Möglichkeit, Daten über das Internet zu versenden. Daher ist diese Berechtigung nicht erforderlich, um Daten über das Internet versenden zu können.

IHRE PERSONENBEZOGENEN DATEN

KONTAKTE LESEN

Ermöglicht der App, auf Ihrem Tablet gespeicherte Daten zu Ihren Kontakten einschließlich der Häufigkeit zu lesen, mit der Sie bestimmte Personen angerufen, an sie eine E-Mail gesendet oder auf andere Weise mit ihnen kommuniziert haben. Diese Berechtigung ermöglicht Apps das Speichern Ihrer Kontaktdaten und schädliche Apps können Kontaktdaten ohne Ihr Wissen weitergeben. Ermöglicht der App, auf Ihrem Telefon gespeicherte Daten zu Ihren Kontakten einschließlich der Häufigkeit zu lesen, mit der Sie bestimmte Personen angerufen, an sie eine E-Mail gesendet oder auf andere Weise mit ihnen kommuniziert haben. Diese Berechtigung ermöglicht Apps das Speichern Ihrer Kontaktdaten und schädliche Apps können Kontaktdaten ohne Ihr Wissen weitergeben.

MEINE KONTAKTE ÄNDERN

Ermöglicht der App, auf Ihrem Tablet gespeicherte Daten zu Ihren Kontakten einschließlich der Häufigkeit zu ändern, mit der Sie bestimmte Personen angerufen, an sie eine E-Mail gesendet oder auf andere Weise mit ihnen kommuniziert haben. Diese Berechtigung ermöglicht Apps das Löschen von Kontaktdaten. Ermöglicht der App, auf Ihrem Telefon gespeicherte Daten zu Ihren Kontakten einschließlich der Häufigkeit zu ändern, mit der Sie bestimmte Personen angerufen, an sie eine E-Mail gesendet oder auf andere Weise mit ihnen kommuniziert haben. Diese Berechtigung ermöglicht Apps das Löschen von Kontaktdaten.

TOP SECRET//SI//ORCON//NOFORN



Hotmail™



Google™



YouTube



(TS//SI//NF) PRISM Collection Details



Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)?

It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

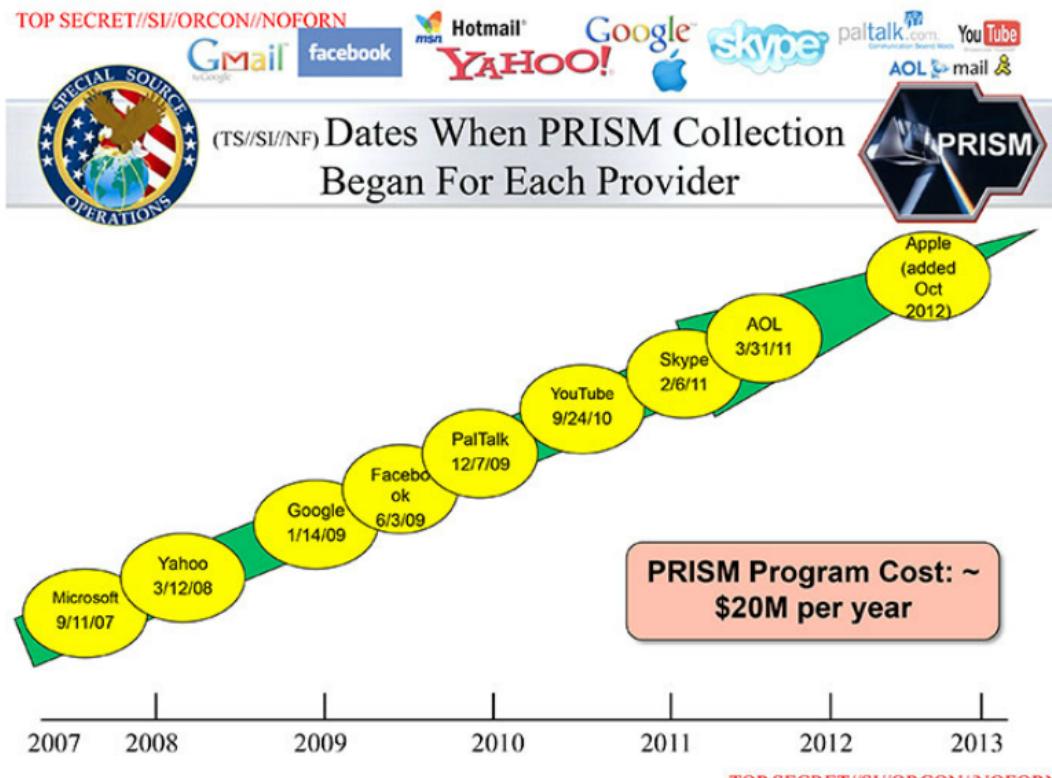
Complete list and details on PRISM web page:

Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

This image is a work of a U.S. military or Department of Defense employee, taken or made as part of that person's official duties. As a work of the U.S. federal government, the image is in the public domain.

Quelle: Wikipedia http://en.wikipedia.org/wiki/File:PRISM_Collection_Details.jpg



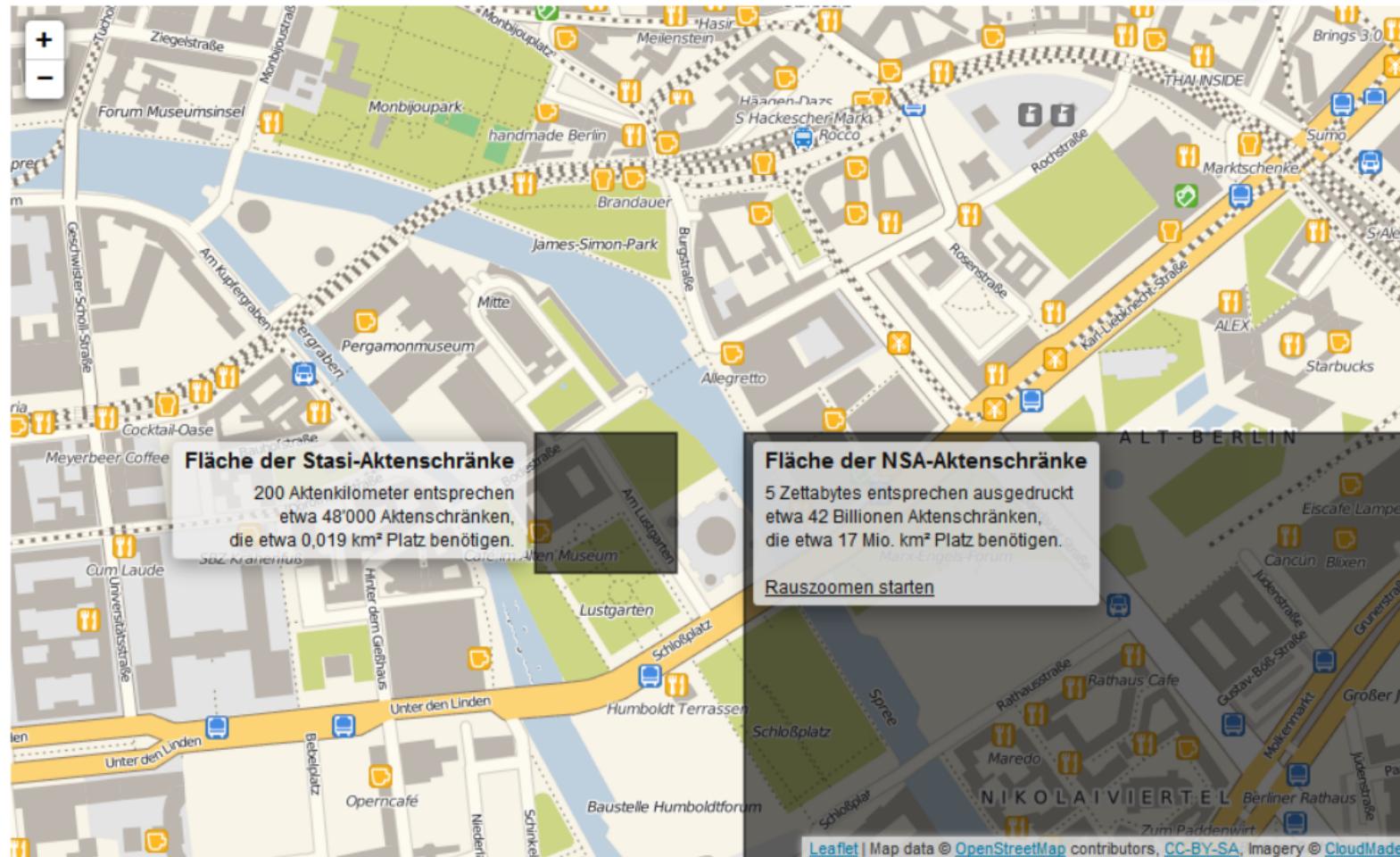
This image is a work of a U.S. military or Department of Defense employee, taken or made as part of that person's official duties. As a work of the U.S. federal government, the image is in the public domain.

Quelle: Wikipedia http://en.wikipedia.org/wiki/File:Prism_slide_5.jpg

Wieviel Platz würden die Aktenschränke der Stasi und der NSA verbrauchen - wenn die NSA ihre 5 Zettabytes ausdrucken würde?



Einbetten



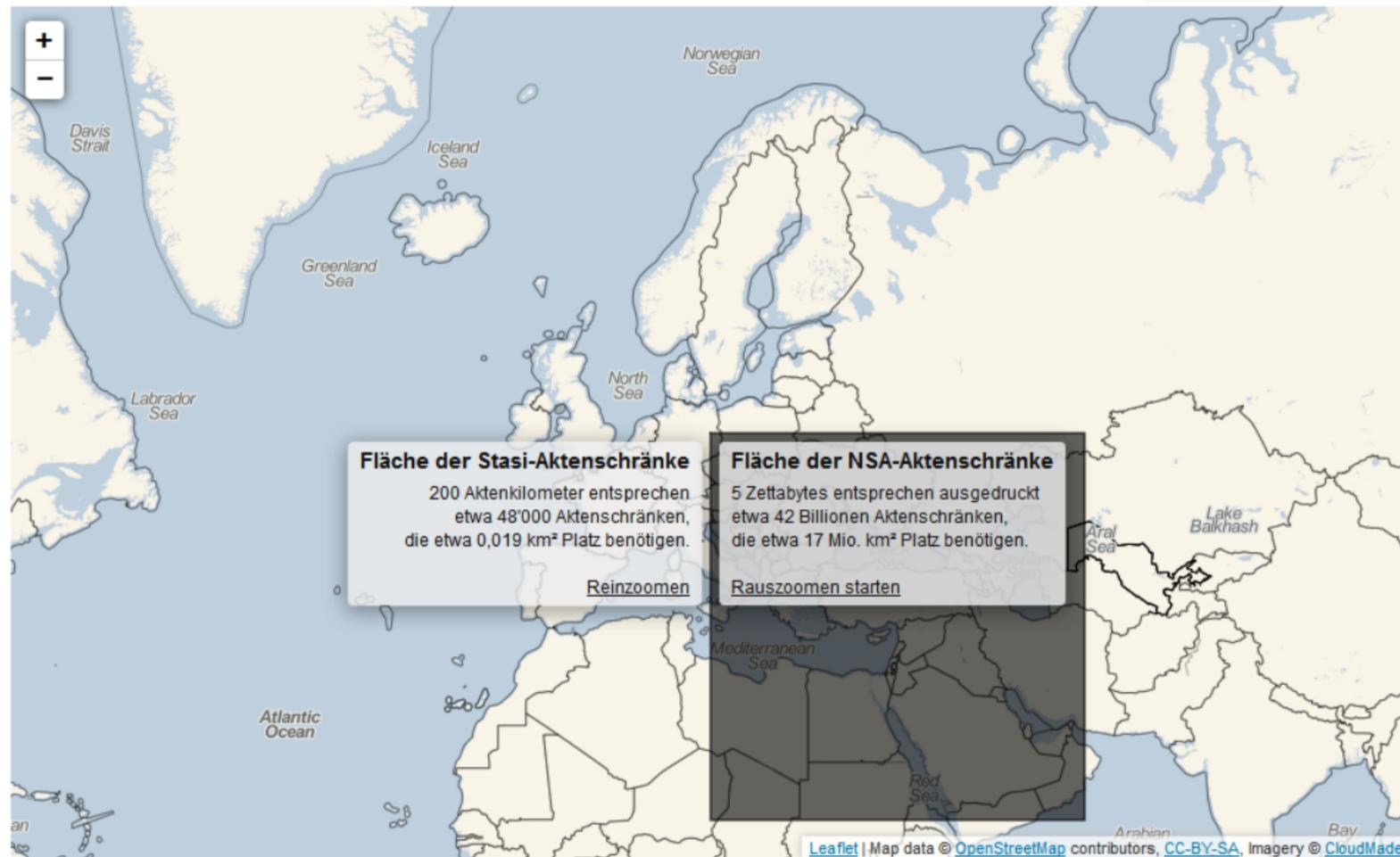
Realisiert von OpenDataCity. Anwendung steht unter CC-BY 3.0.

Options...

Wieviel Platz würden die Aktenschränke der Stasi und der NSA verbrauchen - wenn die NSA ihre 5 Zettabytes ausdrucken würde?

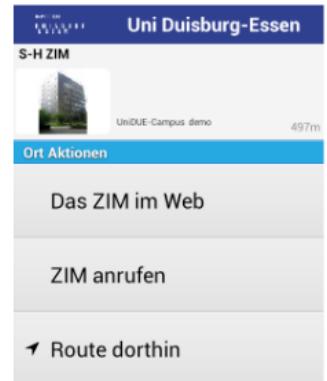


Einbetten



Realisiert von OpenDataCity. Anwendung steht unter CC-BY 3.0.

Rechtliche Rahmenbedingungen:



- Verletzung des Persönlichkeitsrechts (private Daten)
- Geheimhaltungspflicht aus Verträgen (dienstliche Daten)
- Auswirkungen auf Arbeitsverträge
- „privates“ Cloudcomputing von dienstlichen Daten ist unzulässig
(iCloud sichert komplettes Backup)
- Herausgabepflichten
(§257 HGB gelten auch für mobile Geschäftsunterlagen)
- Arbeitsrecht – Überschreitung der zulässigen Arbeitszeit (dienstlich und privat genutztes Gerät wird nicht ausgeschaltet) (Ordnungswidrigkeit 15000 € Bußgeld)
(für wissenschaftliche Mitarbeiter im Hochschulumfeld nicht realistisch)
- Mitbestimmungsrecht – Personalräte
- Haftungs- und Ersatzpflichten

Neue Anforderungen an das IDM durch Apps

- Authentifizierung, Autorisierung für Apps
- klassisch LDAP
- SSO für (Web-)Apps
 - plattformunabhängige Apps sind Web-Apps mit Wrappern, z.B. Phonegap
- Shibboleth mit OAuth2 Token
(RWTH Aachen, Bernd Decker, Rechen- und Kommunikationszentrum)
- CAS (<http://www.jasig.org/umobile>)
- UNI-Duisburg-Essen: Eigene Lösung mit Hashes und Proxy

Zusammenfassung

Die Frage ist nicht mehr wollen wir BYOD einführen! BYOD ist Realität!

Hochschulen profitieren bei BYOD von ihrer Erfahrung mit Studierenden!

Hochschulen betreiben traditionell offene und heterogene Systeme.

Herausforderungen im Datenschutz für mobile Systeme (von Datenschutzbeauftragten derzeit noch gar nicht im Fokus).

Es fehlen noch SSO-Lösungen für Smartphones (SAML, Shibboleth).

Die Benutzer müssen geschult und sensibilisiert werden!

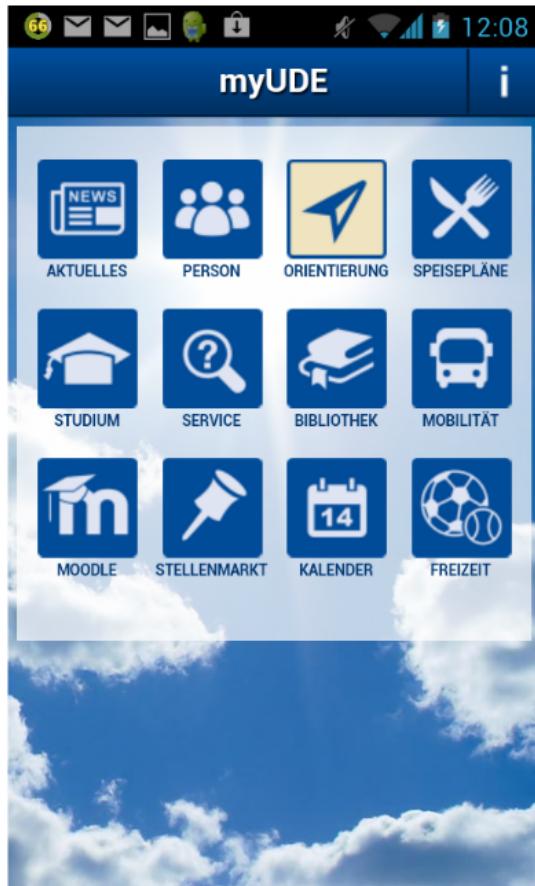


Die Rechenzentren müssen datenschutzkonforme Alternativen zu Clouddiensten anbieten

Die Konsequenzen der NSA-Affäre müssen für einen sicheren Betrieb bedacht werden.

Wie wirkt sich die NSA-Affäre auf Identitätsmanagement aus? Welche Anbietern kann vertraut werden?

Uni-Due Campus-App "myUDE":



<http://www.uni-due.de/myude/>



ZENTRUM FÜR INFORMATIONS- UND MEDIENDIENSTE

Bring Your Own Device - Auswirkungen
mobiler Endgeräte auf Identitymanagement und
Datenschutz

Dr.-Ing. Andreas Bischoff



Folien : <http://ude.de/byod>

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?

Kontakt: andreas.bischoff@uni-due.de

Ich bitte darum meine Kontaktdaten nicht in einer Cloud zu speichern! Der Weitergabe/Weiterleitung meiner Mails an Google-Mail stimme ich nicht zu!



Sep 23, 13 17:21	prezi_iso.txt	Page 1/3
Prezi exportiert Folien als Bilder. Daher fuer Suchmaschinen diese Texte:		
Bring Your Own Device - Auswirkungen mobiler Endgeräte auf Identitymanagement und Datenschutz		
Was ist "Bring your own device" BYOD?		
Intel erlaubte es im Jahre 2009 seinen Beschäftigten ihre privaten Gerät en am Arbeitsplatz zu nutzen Warum ist das ein Hype? Kostensparnis? - Nein! Erfolg mobiler Geräte wie Smartphones, Tablets, Netbooks, Notebooks (verdrängen PCs) Smartphones verdrängen herkömmliche Mobiltelefone in Deutschland Nutzer bringen private Geräte mit und nutzen Sie auch für dienstliche Daten (E-Mail) "It's not a question of if employees will bring their own mobile devices to work and connect to your systems. It's a matter of when." Malcolm Harkins, CISO Intel Bring Your Own Device - Auswirkungen mobiler Endgeräte auf Identitymanagement und Datenschutz		
Dr.-Ing. Andreas Bischoff		
Agenda		
Motivation Was ist das? Warum ist das (jetzt) ein Hype? BYOD an Hochschulen Voraussetzungen Nutzen - Vorteile - Dr. Jekyll Gefahren - Nachteile - Mr. Hyde Rechtliches Auswirkungen auf IDM Zusammenfassung - Tipps		
Mobiler Daten-Traffic = e-Funktion! Ausweg: neue Frequenzen (bis 10 GHz); Deregulierung mehr Mobilfunkstationen (Femtocells,Picocells)		
"It's not a question of if employees will bring their own mobile devices to work and connect to your systems. It's a matter of when." Malcolm Harkins, CISO Intel BYOD an Hochschulen		
Lange Tradition bei wissenschaftlichen Mitarbeitern und Professoren "freier" Umgang mit der Thematik an Hochschulen WLAN-Ausbau eduroam für Studierende und Mitarbeiter preiswerte Netbooks --> Studierende Preisverfall bei UMTS-Datenflatrates (2-10 monatlich) und Smartphones (Android-Smartphones unter 100) Technische Voraussetzungen seit 5 Jahren vorhanden, Kosten 2007: 60-100 pro Monat (24 Monate-Vertrag) Neue Szenarien über die mobile Nutzung des Webangebotes hinaus, mobile Learning, Kommunikationsdienste Klinikum iPhones		
Kosten sparen (Hauptargument, Grund für den Hype [Computerwoche: Hype eben ab]) schnelle Reaktion auf neue Geräte Freiheit der Forschung und Lehre förderst Erreichbarkeit		
Keine zwei Landschaften pflegen		

Sep 23, 13 17:21	prezi_iso.txt	Page 2/3
Diversität Betriebssysteme Early Adopter haben alle Freiheiten z.B. importierte Geräte aus China Freiheit in der Nutzung moderner Clouddienste Synergieeffekte durch eingebrachtes Know How förderst Homeoffice Kundenzufriedenheit ganz neue Szenarien möglich für m-Learning Voting-Apps Interaktion Virtual Reality		
Mobile Computing Notebooks -Netbook -Tablets Smartphones WLAN vs. UMTS, LTE (Kapazitätsgrenzen, Femtocell?) Offene Standards an der Hochschule (keine abgeschlossenen vereinheitlichten Welten)		
eduRoam In den eduroam-Netzen: Jeder in seinem Subnetz - keine Broadcasts Sicherheit Viren Scanner Trennung dienstlicher von privaten Daten z.B. Containerlösungen "Merkel-Phone" (Samsung Galaxy S2, S3 mit Mirokernel) Blackberry 10 mit Microkernel (QNX) gesicherter dienstlicher Bereich Transportverschlüsselung Storage-Verschlüsselung Remote Desktop Virtual Desktop Infrastructure (VDI) VPN für alle Plattformen Festplatten/Flash-Dateisystemverschlüsselung Webanwendungen/Virtual Desktop Infrastruktur		
Identitymanagement Verwaltungsmöglichkeiten externer Clients (Beispiel Exchange2010, Remote wipe) Benutzerhilfen know how Betriebssysteme Mobilplattformen - Benutzerberatung - FAQ früher: Early Adopter sorgten für Dokumente und konfigurierten selbst heute: Kunden verlangen die Konfiguration als Dienstleistung Dienstvereinbarungen		
Speicherung und Verarbeitung dienstlicher Daten auf privaten Geräten. Mobile Device Management Geräte sind oft nur für den Privatbetrieb gedacht, z.B. Android bis 4.2 nur ein Nutzerprofil z.B. iPad, IOS: E-Mail-Client nicht deaktivierbar, auch nicht kurzfristig durch falsches Passwort Softwareverteilung - Lizenzen BYOD policy (Benutzerordnung)		
'bring your own disaster' Security nightmares Filesharing (Störerhaftung) Viren/Würmer Passwörter und Profile bei Dienstleistern wie Google und Apple Dienstliche Daten in der Cloud (Apple: iPhone Fotos, iCloud, Microsoft Skydrive) Datenschutz - Mischung dienstlicher und privater Profile/Daten Remote Wipe betrifft auch private Daten		
Ortsbezogene Dienste: Sie zahlen mit Ihren Daten (z.B. Bewegungsprofile sind möglich) Weitergabe Daten anderer Nutzer Stichwort WhatsApp, Facebook, Google Kalender Weitergabe Adressbuch/Telefonbuch (iOS bis 4) Kalender E-Mail Kontakte Synchronisation ohne cloud möglich?		

Sep 23, 13 17:21

prezi_iso.txt

Page 3/3

Problem Google Kalender!
iPhone sync per Kabel?
Biometrische Daten - iPhone 5S!
TSM-Sicherung privater Daten?
Gestohlene Geräte (remote lock and wipe)
Defekte Geräte
Jailbreak rooten (kann auch nützlich sein für BYOD, customized devices)
Work life balance
Läuft Vereinheitlichung entgegen

Verletzung des Persönlichkeitsrechts (private Daten)
Geheimhaltungspflicht aus Verträgen (dienstliche Daten)
Auswirkungen auf Arbeitsverträge
privates Cloudcomputing von dienstlichen Daten ist unzulässig
(iCloud sichert komplettes Backup)

Herausgabepflichten
(\\$257 HGB gelten auch für mobile Geschäftsunterlagen)

Arbeitsrecht Überschreitung der zulässigen Arbeitszeit (dienstlich und privat genutztes Gerät wird nicht ausgeschaltet) (Ordnungswidrigkeit 15000 Bußgeld)

(für wissenschaftliche Mitarbeiter im Hochschulumfeld nicht realistisch)

Mitbestimmungsrecht Personalräte

Haftungs- und Ersatzpflichten
Die Frage ist nicht mehr wollen wir BYOD einführen! BYOD ist Realität!

Hochschulen profitieren bei BYOD von ihrer Erfahrung mit Studierenden!

Hochschulen betreiben traditionell offene und heterogene Systeme.

Herausforderungen im Datenschutz für mobile Systeme (von Datenschutzbeauftragten derzeit noch gar nicht im Fokus).

Es fehlen noch SSO-Lösungen für Smartphones (SAML, Shibboleth).

Die Benutzer müssen geschult und sensibilisiert werden!

Die Rechenzentren müssen datenschutzkonforme Alternativen zu Clouddiensten anbieten.

Die Konsequenzen der NSA-Affäre müssen für einen sicheren Betrieb bedacht werden.

Wie wirkt sich die NSA-Affäre auf Identitätsmanagement aus? Welche Anbieter kann vertraut werden?

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?

Kontakt: andreas.bischoff@uni-due.de
Folien : <http://ude.de/byod>
Dr.-Ing. Andreas Bischoff
Zentrum für Informations- und Mediendienste
Universität Duisburg-Essen
Herbsttreffen ZKI AK Verzeichnisdienste
Kaiserslautern 2013