Mobile Device Management (MDM) in Theorie und universitärer Praxis

Markus Krieger
Rechenzentrum Universität Würzburg

Mobile Devices

RECHENZENTRUM

- Smartphones / Tabletts (eigentlich auch Laptops)
- „Persönliche“ Geräte
- Viele Daten (Mails, Kontakte, PW, Dokumente, Bilder, ...)
- Leicht zu klauen/zu verlieren
- Kurzer Support / selten Bugfixes /schnell veraltet
- Vielzahl unsicherer Apps
- Nutzung über unsichere Infrastruktur
- Leichter Zugriff (USB-Kondom?)
- Spieltrieb der Nutzer
- Mischung privat / dienstlich

BYOD

RECHENZENTRUM

- Einführung Budgetüberprüfung
- Einbindung von Verantwortlichen in Workflow
- Erweiterung Anlagebuchhaltung um Garantieende
- Jedes Institut kann seinen IT-Bestand über die letzten 11 Jahre zurückverfolgen (z.B. Software-Download wiederholen)

Mobile Device Management

RECHENZENTRUM

- Gerät vs Container
- Inventarisierung
- Softwareverteilung
- Konfigurationsmanagement
- Implementieren von Policys
- Sicherheitseinstellungen
-

Mobile Device Management

RECHENZENTRUM

Typische Fähigkeiten

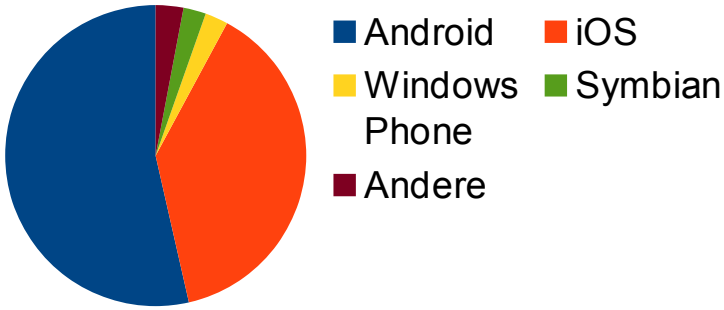
- App-Stores einschränken
- Kontrolle auf Jailbreak / Root
- Erfassen von OS-Typ / Version
- Ortung
- Remote Wipe der dienstlichen / aller Daten
- PIN erzwingen

- Problem: Möglichkeiten des MDM hängen von Features des Endgeräts ab!

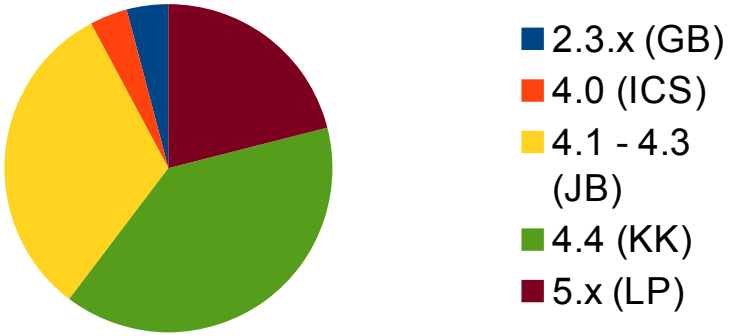
Problem: Vielfalt

RECHENZENTRUM

Marktanteile Smartphones/Tablets



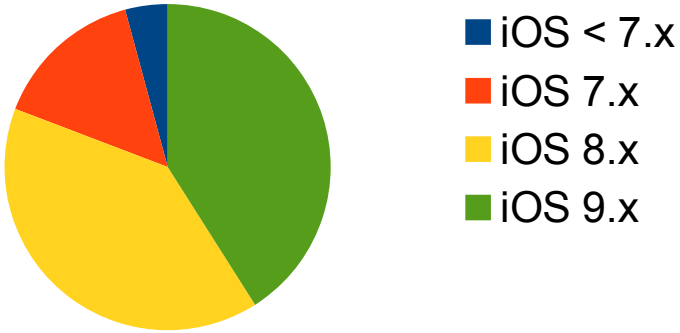
Verteilung Android Versionen



Clients im Uni-WLAN (Sept 2015)

- 18564 unique Clients
- 5440 „Apple“ (iOS + Mac)
- 2847 „Samsung“
- 2140 „unknown“
- 2134 „intel“
- 6003 auf 129 Hersteller verteilt

Verteilung iOS Versionen



Problem: Policy & Akzeptanz

RECHENZENTRUM

- B. Software-Download wiederholen)

Testballon gemeinsames MDM

RECHENZENTRUM

Ansatz

- Mandantenfähiges MDM
- ActiveSync/LDAP Anbindung an jeweilige Heimateinrichtung
- Gemeinsam erarbeiter Satz an Policy Templates
  - Durch Mandanten im eigenen Kontext anpassbar
- Nur dienstliche Endgeräte
- Minimale Baseline: Pin auf Geräten erzwingen
- Entlastung des Helpdesks: „Hilfe zur Selbsthilfe“
  - WLAN, Mail, VPN Profile verteilen
  - **Nutzer** kann sein Device remote löschen
  - Apps verteilen

Testballon gemeinsames MDM

RECHENZENTRUM

Umsetzung

- 2013 Installation „ZenWorks Mobile Management“ an der Uni Regensburg.
- Mandanten: Uni Regensburg, Uni Würzburg, OTH Amberg-Weiden
-
- Erweiterung Anlagebuchhaltung um Garantieende
- Jedes Institut kann seinen IT-Bestand über die letzten 11 Jahre zurückverfolgen (z.B. Software-Download wiederholen)

Produktiver Einsatz

RECHENZENTRUM

Zentralverwaltung der Uni Regensburg

- 10 iPads (dienstl. beschafft / dienstl. genutzt)
- Vorbereiten der iPads über Apple Configurator
  - Apps vorinstallieren
  - App Store, Touch ID, iTunes, iCloud deaktivieren
  - Device löschen nach 10 Passwortfehlversuchen
- MDM um WLAN + Mail Profile personalisiert auf dem Gerät einzurichten
- Datenhaltung per Netzlaufwerken / Novell Vibe
- „Befürchtung“ dass künftig auch Windows Phones Einzug halten

Fazit

RECHENZENTRUM

- Einführung Budgetüberprüfung
- Einbindung von Verantwortlichen in Workflow
- Erweiterung Anlagebuchhaltung um Garantieende
- Jedes Institut kann seinen IT-Bestand über die letzten 11 Jahre zurückverfolgen (z.B. Software-Download wiederholen)

WebShop

Beschaffung von Hardware, Software, etc. durch berechtigte Einrichtungen von Hochschulen usw.

Download-portal

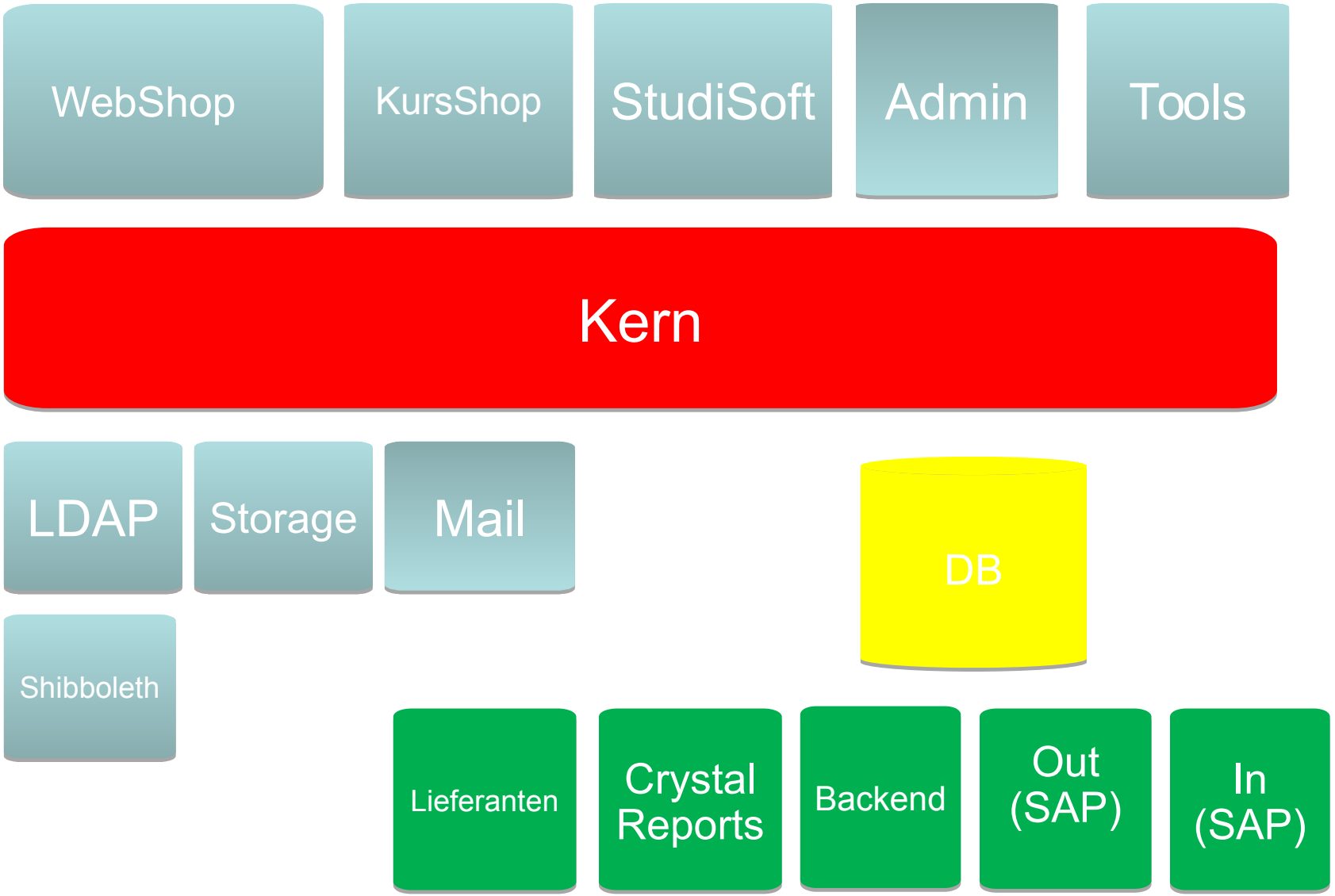
Verteilung von kostenloser und kostenpflichtiger Software für Studierende und Mitarbeiter (Home-use)

KursShop

Buchung und Bezahlung von Kursen durch Studierende, Mitarbeiter und Externen

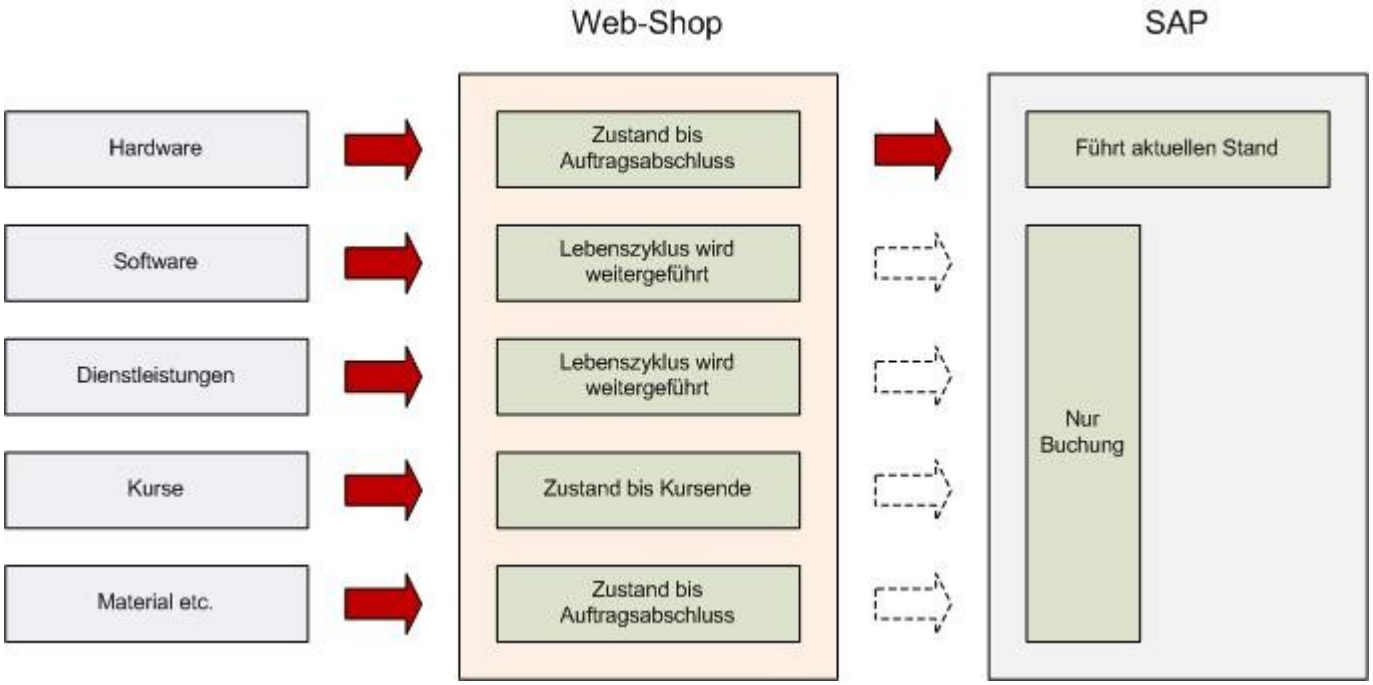
Dienstleistungen

Verrechnung von Print, Speicherplatz, Virtuellen Maschinen und weiteren Dienstleistungen


WebShop
KursShop
StudiSoft
Admin
Tools
Kern
LDAP
Storage
Mail
DB
Shibboleth
Lieferanten
Crystal Reports
Backend
Out (SAP)
In (SAP)


IT-Beschaffung der Hochschule
• Backend im Rechenzentrum
Sonstige Artikel
• Backend im Einkauf
Beschaffung anderer Hochschulen
• Backend: Eigene Tools
StudiSoft
• Administrationsoberfläche für zuständigen Admin

Datenzustand



Beispiele für Mehrwert

- Einführung Budgetüberprüfung
- Einbindung von Verantwortlichen in Workflow
- Erweiterung Anlagebuchhaltung um Garantieende
- Jedes Institut kann seinen IT-Bestand über die letzten 11 Jahre zurückverfolgen (z.B. Software-Download wiederholen)