Bring Your Own Device

Privates im DESY-Netzwerk

Carsten Porthun (D4)
Technisches Seminar
Zeuthen, 26.11.2013

HELMHOLTZ GEMEINSCHAFT

DESY

Agenda

- Einführung
- Rechtliche Aspekte
  - Eigentum
  - Pflichten und Verantwortung
  - Haftung und Lizenzfragen
- Nutzung von Webdiensten
  - Beispiel Email- und Kalenderdiente
  - Beispiel soziale Netzwerke
- Zusammenfassung
- Fragen und Diskussion

DESY

Einführung

Einführung – „Devices“

Hardware	Software	Webdienste
Laptops / VPN-Desktops	OS - Lizenzen	Mail / Kalender
Smartphones / Tablets	OEM-Installationen	Speicherdienste
Netzwerke	Freeware	Software as a Service
Speichermedien	…	Soziale Netzwerke
…		…

Problematik: Früher

Problematik: Heute

Einführung - Gefahren

- Vertrauliche / dienstliche Daten auf externen Servern
  - Verstöße gegen gesetzliche Vorgaben
  - Unbefugter Zugriff auf vertrauliche Informationen
- Beeinträchtigung des IT-Sicherheits-Niveaus
  - Keine zentrale Administration
  - Einspielen von Sicherheitspatches?
  - Einhaltung von Policies?

Einführung - Beschaffungskriterien

DESY

- Kosten für Beschaffung und Wartung
- Garantie und Gewährleistung
- Integration in bestehende Infrastruktur
- Zentrale Administration
- Kompatibilität mit bestehenden Anwendungen

Privat

- Kosten
- Lifestyle
- Einfache Handhabung und Konfiguration
- Integration in private Umgebung – ggf. Anpassung der Infrastruktur
- Digitale Medien und Kommunikation

Rechtliche Aspekte

- Eigentum
- Pflichten und Verantwortung
- Haftung und Lizenzfragen

Eigentum

- Wem gehört die Hardware?
  - Eigenes Gerät
  - Leasing-Gerät
  - „Familiengerät“
- Wem gehören Daten? Wer darf darauf zugreifen?
  - Dienstliche Daten gehören dem Arbeitgeber
  - Private Daten sind privat.
  - AGBs von Webdiensten – Nutzungsrechte?
  - Vermischung privater und dienstlicher Daten
- Wem gehören Accounts und Programme
  - Problematik von AppStores
  - Vermischung privater Accounts mit eventuell dienstlich gekauften Apps

Verantwortung und Pflichten

- Datenverantwortung
  - Für dienstliche Daten beim Arbeitgeber – Gesetzliche Verpflichtungen
- Gesetzliche Anforderungen
  - Aufbewahrungspflichten
  - Schutz personenbezogener Daten
- Klassifikation der Vertraulichkeit
  - Weltweit
  - Nur intern
  - Vertraulich
  - Streng vertraulich

Haftung und Lizenzfragen

- Verstöße gegen rechtliche Anforderungen
  - Beispiel: „Auftragsdatenverarbeitung“ bei Übertragung personenbezogener Daten an Dienstanbieter
- Hardwareverlust
- Hardwaredefekt
- Lizenzverstöße
  - Nutzung von „privaten“ Lizenzen im dienstlichen Umfeld
  - Nutzung von DESY-Lizenzen im privaten Umfeld
  - Dienstliche Nutzung von Freeware, die nur für privaten Gebrauch „frei“ ist

MS Office 2010 EULA

12. HOME AND STUDENT-SOFTWARE.
Bei als „Home and Student“-Version gekennzeichneter Software sind Sie berechtigt, eine Kopie der Software auf bis zu drei lizenzierten Geräten in Ihrem Haushalt zur Verwendung durch Personen, die dort ihren Hauptwohnsitz haben, zu installieren. Die Software darf **nicht für kommerzielle, gemeinnützige oder Einnahmen erwirtschaftende Aktivitäten** verwendet werden.

Merke …

- Daten verbleiben nach Möglichkeit auf DESY-Servern
  - Nutzung von Remote-Zugängen (Terminal- / Workgroupserver)
  - Email
  - Dienstliche Daten nur in begründeten Ausnahmen auf private Hardware
  - Löschen nicht benötigter Daten auf privater Hardware (überschreiben)
- DESY Regeln gelten auch für private Hardware
  - RSR Statement 2002/01 (Passwort-Policy)
  - RSR Statement 2003/01 (Systeme in internen Netzen)
  - RSR Statement 2006/01 (Remote Zugänge)

(https://rechnersicherheit.desy.de/statements)

Merke weiter …

- Speicherverschlüsselung auf Endgeräten
- Nutzung verschlüsselter Protokolle
- Zugriffssperren (PIN / Passwort)
- Trennung privater und dienstlicher Nutzung durch unterschiedliche Accounts
- Verluste melden und entsprechend handeln (Passwörter)
  (https://rechnersicherheit.desy.de/index_ger.html -> Hardwareverlust)
- (Remote Wipen)

Nutzung von Webdiensten

- Beispiel Email- und Kalenderdiente
- Beispiel soziale Netzwerke

Beispiel Weiterleitung von Emails; Kalender

> Privates Postfach als Sammeladresse für Emails

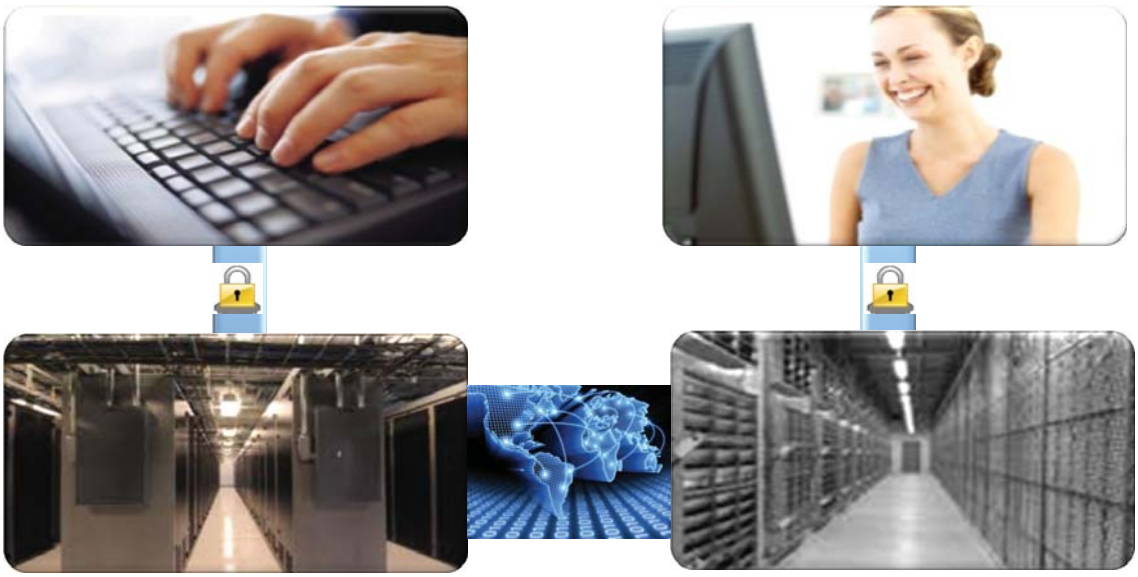
- Automatische Weiterleitung eingehender Emails
- Antwort mit Absender-Adresse des privaten Postfachs
- Dienste bieten teilweise andere Absenderadressen an

> Pflege von Kalendereinträgen in einem privaten Kalender

- Teilen der Information mit Familienmitgliedern
- Synchronisieren dienstlicher mit privaten Kalendern

E-Mail und Kalender

Email



Zu beachten: Versender

- Was soll per Mail übertragen werden?
  - Vertrauliche Informationen
  - Personenbezogene Daten
  - Anhänge
  - Disclaimer
- Wen soll die Information erreichen?
  - Empfängerauswahl
  - Adresslisten, Cc oder besser Bcc?

Zu beachten: Empfänger

- Von wem stammt die Mail?
  - Identität prüfen
- Für wen ist die Information bestimmt?
  - Weiterleitungen
  - Berechtigungen von Postfach und Kalender
- Wohin
  - Automatische Weiterleitungen an Postfächer / Kalender bei externen Providern?
  - Regelbasierte Weiterleitung in Abwesenheit?
  - Mobile Endgeräte

Merke

- **Keine** dienstlichen Mails an **private Postfächer**
- **Keine** dienstlichen Termine in **private Kalender**

- Keine **personenbezogenen** oder **vertraulichen** Daten in Emails
- Freigaben **mit Bedacht** wählen
- **Filesystem** anstelle von Attachments
- **Adresslisten, Bcc** besser als Cc
- **Keine** automatischen **Weiterleitungen** in Abwesenheiten
- (Disclaimer sind ohne Bedeutung)

Tipps

- Einbindung externen (privater) Kalender anstelle von Weiterleitungen
- mobiler Endgeräte:
  - PIN / Passwort
  - Speicherverschlüsselung
  - (Remote Wipen)

- Funktionsadressen nutzen
  (http://rechnersicherheit.desy.de/regeln_und_empfehlungen/vertretungen___accounts_fuer_rollen/index_ger.html)
- Übergabe beim Ausscheiden
- Vertraulichkeitsvermerk im Betreff

Beispiel: Soziale Netze

Beispiel: WhatsApp

0123/1234567

0111/1212123
0122/1313167
0114/8765432
…..

Regelmäßige Übertragung aller Telefonnummern aus den Kontaktdaten!

Privates Whatsapp und dienstliches Telefonbuch!

….
0123/1234567
0111/1212123
….
0122/1313167
0114/8765432
0125/1313167
0114/9876543
….

0111/1212123

0123/1234567
0125/1313167
0114/9876543
…..

Bildquellen:
en.wikipedia.org/wiki/LG_Optimus_2X

WhatsApp: Probleme

- Übertragung personenbezogener Daten an Dritte
  - Formal: Auftragsdatenverarbeitung nach BDSG
  - Liegt eine Einwilligung der Betroffenen vor?
  - Erfüllt Dienstanbieter alle Anforderungen des BDSG, sind diese geprüft worden?
- Regelmäßiges Übertragen des Kontakt-Profils
- Lange Zeit unverschlüsselt übertragen
  - Sicherheitsbewusstsein des Anbieters lässt zu wünschen übrig
- Sicherheitseinstellungen der App – Was wenn die App gehackt wird?

WhatsApp? - What´s Wrong ? I

- **Ihre Konten**
  Informationen zur Authentifizierung eines Kontos verwenden
  (Ermöglicht der App, Authentifizierungs-Tokens anzufordern)

  Kontoliste verwalten
  (Ermöglicht der App, Konten hinzuzufügen und zu entfernen oder deren Passwörter zu löschen)

  Als Kontoauthentifizierer fungieren
  (Ermöglicht der App, die Kontoauthentifizierungsfunktionen des Konto-Managers zu verwenden, einschließlich der Funktionen zum Erstellen von Konten sowie zum Abrufen und Festlegen der entsprechenden Passwörter)

  Bekannte Konten suchen
  (Ermöglicht der App, eine Liste der dem Tablet bekannten Konten abzurufen. Ermöglicht der App, eine Liste der dem Telefon bekannten Konten abzurufen.)
- **Kostenpflichtige Dienste**
  SMS senden
  (Ermöglicht der App das Senden von SMS. Bei schädlichen Apps können Kosten entstehen, wenn Nachrichten ohne Ihre Zustimmung versendet werden.)

  Telefonnummern direkt anrufen
  (Ermöglicht der App, Rufnummern ohne Ihr Eingreifen zu wählen. Schädliche Apps können so für unerwartete Telefonate auf Ihrer Telefonrechnung sorgen. Das Wählen von Notrufnummern ist allerdings nicht möglich.)
- **Hardware-Steuerelemente**
  Audio aufnehmen
  (Ermöglicht der App, auf den Pfad für Audioaufzeichnungen zuzugreifen)

  Vibrationsalarm steuern
  (Ermöglicht der App, den Vibrationsalarm zu steuern)

  Netzwerkstatus anzeigen
  (Ermöglicht der App, den Status aller Netzwerke einzusehen)

  WLAN-Status anzeigen
  (Ermöglicht der App, die Informationen zum WLAN-Status einzusehen)

WhatsApp? - What´s Wrong ? II

- **Standort**
  Ungefährer (netzwerkbasierter) Standort
  (Ermöglicht Zugriff auf Quellen mit ungefähren Standortbestimmungen wie die Datenbank des Mobilfunknetzes, um den ungefähren Standort des Tablets zu bestimmen (falls verfügbar). Schädliche Apps können so herausfinden, wo Sie sich ungefähr befinden. Ermöglicht Zugriff auf Quellen mit ungefähren Standortbestimmungen wie die Datenbank des Mobilfunknetzes, um den ungefähren Standort des Telefons zu bestimmen (falls verfügbar). Schädliche Apps können so herausfinden, wo Sie sich ungefähr befinden.)

  Genauer (GPS-) Standort
  (Ermöglicht Zugriff auf genaue Standortquellen wie GPS auf dem Tablet (falls verfügbar). Schädliche Apps können damit bestimmen, wo Sie sich befinden, und Ihren Akku zusätzlich belasten. Ermöglicht Zugriff auf genaue Standortquellen wie GPS auf dem Telefon (falls verfügbar). Schädliche Apps können damit bestimmen, wo Sie sich befinden, und Ihren Akku zusätzlich belasten.)
- **Ihre Nachrichten**
  SMS empfangen
  (Ermöglicht der App, SMS zu empfangen und zu verarbeiten. Schädliche Apps können so Ihre Nachrichten überwachen oder löschen, bevor sie angezeigt werden.)
- **Netzkommunikation**
  Uneingeschränkter Internetzugriff
  (Ermöglicht der App, Netzwerk-Sockets einzurichten)

  Daten aus dem Internet abrufen
  (Ermöglicht Apps, von dem App-Dienst gesendete Cloud-an-Gerät-Nachrichten zu akzeptieren. Bei der Verwendung dieses Dienstes werden Daten übermittelt. Schädliche Apps können zu übermäßigem Datenverbrauch führen.)
- **Ihre persönlichen Daten**
  Kontaktdaten lesen
  (Ermöglicht der App, alle auf Ihrem Tablet gespeicherten Kontaktdaten (Adressen) zu lesen. Schädliche Apps können so Ihre Daten an andere senden. Ermöglicht der App, alle auf Ihrem Telefon gespeicherten Kontaktdaten (Adressen) zu lesen. Schädliche Apps können so Ihre Daten an andere senden.)

  Kontaktdaten schreiben
  (Ermöglicht der App, die auf Ihrem Tablet gespeicherten Kontaktdaten (Adressen) zu ändern. Schädliche Apps können so Ihre Kontaktdaten löschen oder ändern. Ermöglicht der App, die auf Ihrem Telefon gespeicherten Kontaktdaten (Adressen) zu ändern. Schädliche Apps können so Ihre Kontaktdaten löschen oder ändern.)
- **Telefonanrufe**
  Telefonstatus lesen und identifizieren
  (Ermöglicht der App, auf die Telefonfunktionen des Geräts zuzugreifen. Eine App mit dieser Berechtigung kann unter anderem die Telefon- und Seriennummer dieses Telefons ermitteln und feststellen, ob ein Anruf aktiv ist oder mit welcher Nummer der Anrufer verbunden ist.)
- **Speicher**
  Inhalt des USB-Speichers und der SD-Karte ändern/löschen
  (Ermöglicht der App das Schreiben in den USB-Speicher und auf die SD-Karte)

WhatsApp? - What´s Wrong ? III

- **System-Tools**
  Standby-Modus des Tablets deaktivieren Standby-Modus des Telefons deaktivieren
  (Ermöglicht der App, den Standby-Modus des Tablets zu deaktivieren. Ermöglicht der App, den Standby-Modus des Telefons zu deaktivieren.)

  Allgemeine Systemeinstellungen ändern
  (Ermöglicht der App, die Einstellungsdaten des Systems zu ändern. Schädliche Apps können so die Systemkonfiguration beschädigen.)

  Synchronisierungseinstellungen erstellen
  (Ermöglicht einer App, die Synchronisierungseinstellungen zu ändern, etwa um festzulegen, ob die Synchronisierung für Kontakte aktiviert ist)

  Aktive Apps abrufen
  (Ermöglicht der App, Informationen zu aktuellen und kürzlich ausgeführten Aufgaben abzurufen. Schädliche Apps können so geheime Informationen zu anderen Apps erhalten.)

  Automatisch nach dem Booten starten
  (Ermöglicht der App, sich selbst zu starten, sobald das System gebootet wurde. Dadurch kann es länger dauern, bis das Tablet gestartet wird, und durch die ständige Aktivität der App wird die gesamte Leistung des Tablets beeinträchtigt. Ermöglicht der App, sich selbst zu starten, sobald das System gebootet wurde. Dadurch kann es länger dauern, bis das Telefon gestartet wird, und durch die ständige Aktivität der App wird die gesamte Leistung des Telefons beeinträchtigt.)

  Synchronisierungsstatistiken lesen
  (Ermöglicht der App, die Synchronisierungsstatistiken zu lesen, etwa den Verlauf der bereits durchgeführten Synchronisierungen)

  Synchronisierungseinstellungen lesen
  (Ermöglicht einer App, die Synchronisierungseinstellungen zu lesen, etwa um festzustellen, ob die Synchronisierung für Kontakte aktiviert ist)
- **Standard**
  Sicherheitseinstellungen für das System ändern
  (Ermöglicht der App, die Sicherheitseinstellungsdaten des Systems zu ändern. Nicht für normale Apps vorgesehen.)

  Rechnungsdienst von Market
  (Nutzer können mit dieser App Artikel über Market kaufen.)

  In Ihren Profildaten lesen
  (Ermöglicht der App, auf Ihrem Gerät gespeicherte persönliche Profildaten zu lesen, darunter Ihren Namen und Ihre Kontaktdaten. Die App kann Sie somit identifizieren und Ihre Profildaten an andere senden.)

Zusammenfassung

Zusammenfassung

- Nutzung privater Hard- und Software sowie von Webdiensten bringt Probleme mit sich, die es zu beachten gilt.
- Dienstliche Daten, Emails und Kalendereinträge gehören nicht auf private Geräte oder Server von Webdiensten.
- Bei Nutzung privater Hardware für dienstliche Zwecke oder in DESY Netzen sind die DESY-Sicherheitsregeln zu beachten.
- Nutzungsbedingungen von Software sind zu beachten.
- Nutzung von Webdiensten ist problematisch.
- Es sind ausreichend Vorkehrungen zu treffen, dass keine internen oder vertrauliche Informationen in falsche Hände gelangen.
- Prüfen der AGBs von Webdiensten.
- Nicht alles was einfach und bequem zu nutzen ist, ist auch sicher.

Fragen und Diskussion