"Bring Your Own Device" –

Sicher und mobil unterwegs mit Microsoft

Martin Wüthrich | itnetx gmbh

Ausganglage

- Clients heute
  - Full managed = Full controlled
  - Vorgeschriebene Hardware
  - Diverse Einschränkungen (Internet, Installationen, Funktionen…)
- Clients in «Zukunft» oder nicht schon heute?
  - Anwender haben eigene Vorlieben an Geräten (Operating System, Form, Grösse, Farbe…)
  - Anwender möchten überall arbeiten können
  - Anwender möchten alles «selber können»

Was bedeutet Bring your own device?

- Gerät gehört dem Benutzer
- NICHT standardisierte Hardware
- NICHT standardisiertes Operating System
- Gerät muss nicht durch die IT Abteilung
- Definierte Zugriffsmechanismen zu IT Systemen nötig

Umgang mit Mobilen Devices definieren

Massgebliche Punkte zur Findung der zu unterstützenden Geräte

- Relevanz der zur Verfügung gestellten Daten für mobile Geräte
- Die Sicherheitsfunktionen der mobilen Geräte
- Verbreitung der mobilen Geräte in der Zielgruppe
- Phone, Phablet, Tablet und Laptop

Weitere relevante Punkte

- BYOD ≠ CYOD (Choose your own Device)
- Wer ist für die Beschaffung zuständig?
- Wer ist für die Reparatur der Geräte zuständig?
- Verhalten des Benutzers bei Ausfall / Verlust des Geräts

Microsoft Enterprise Mobility Suite

- **Azure Active Directory Premium**

  Ermöglicht das Nutzen von Identitäten für Anmeldungen an Third Party und eigenen Web-Applikationen

- **Rights Management Services**

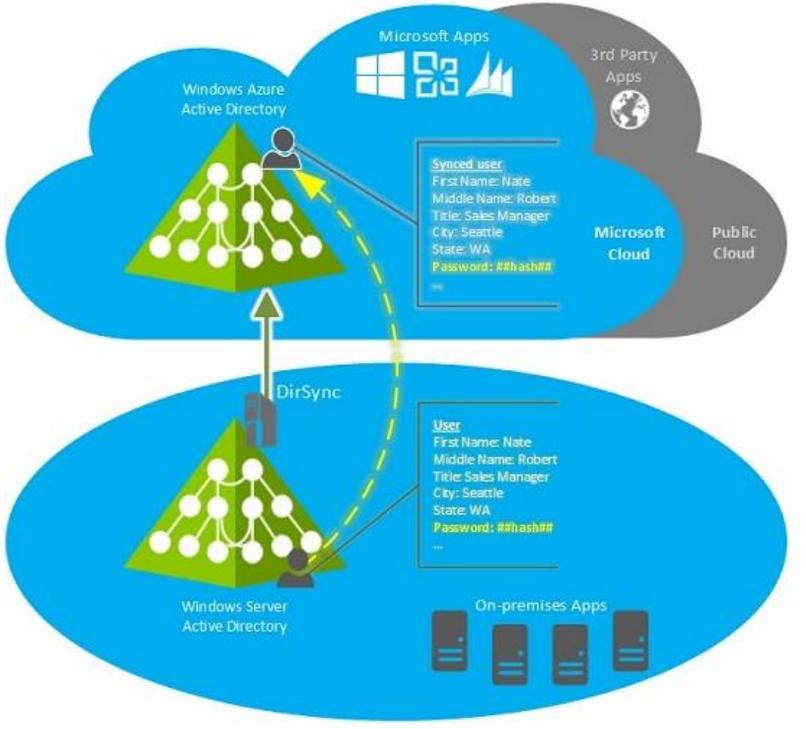
  Ermöglicht das Schützen von Daten, sei es auf mobilen oder stationären Geräten

- **Windows Intune**

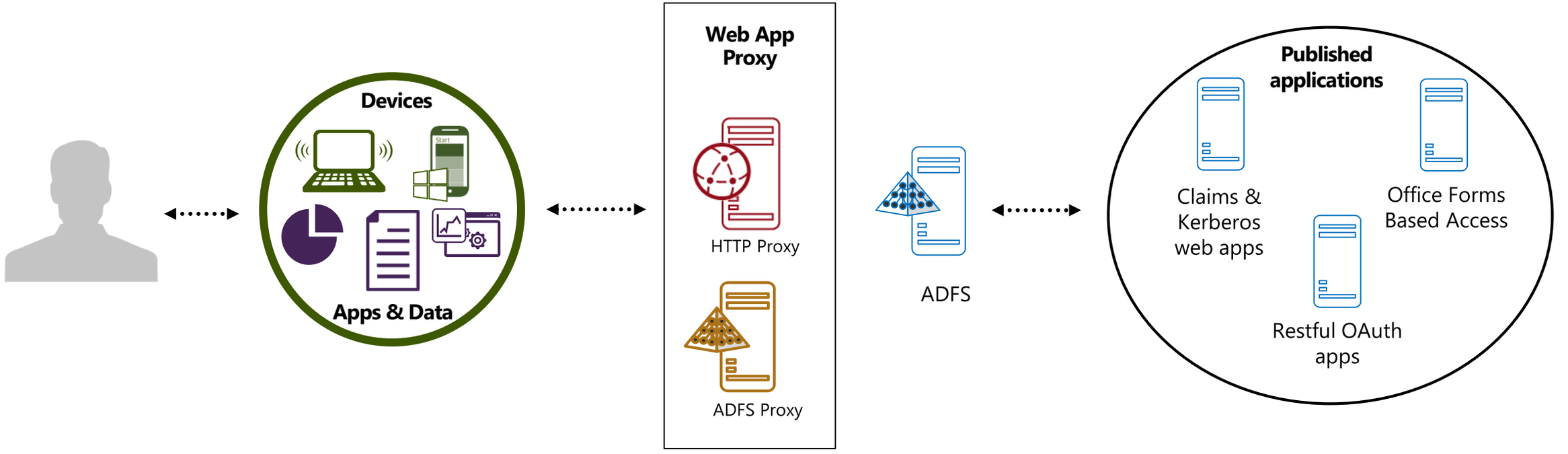
  Ermöglicht das Verwalten von Mobilen Devices in Verbindung mit System Center 2012 Configuration Manager

Azure SSO - Voraussetzungen

- On-Premise Active Directory
- Azure Active Directory Sync
- Passwort Synchronisation aktiviert
- Wenn kein PW Sync gewünscht -> ADFS



Conditional access control capabilities in Windows Server 2012 R2 AD



Users can access corporate data regardless of device or location.

Users are pre-authenticated securely at the edge before being allowed to access corporate resources from extranet.

IT can create business driven access policies based on user, device, authentication method & content being accessed

IT can centrally audit access policies and user access to help with compliance.

SSO für Cloud Dienste und Mobile Devices

itnetX

Demo

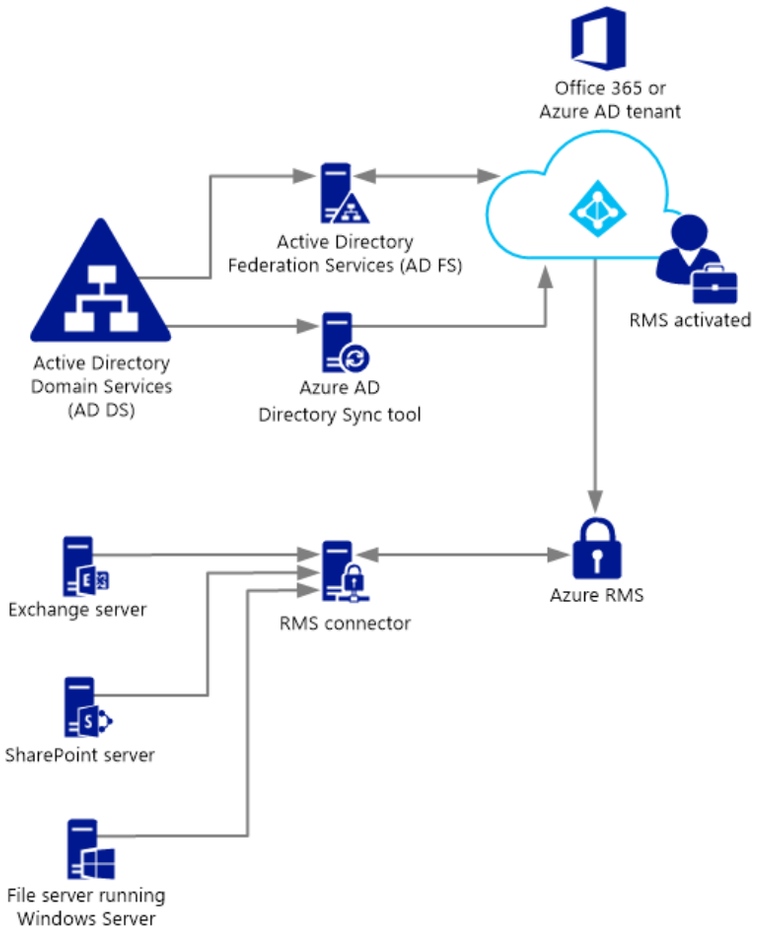
SSO für third party Webapplications am Beispiel von Twitter

itnetX

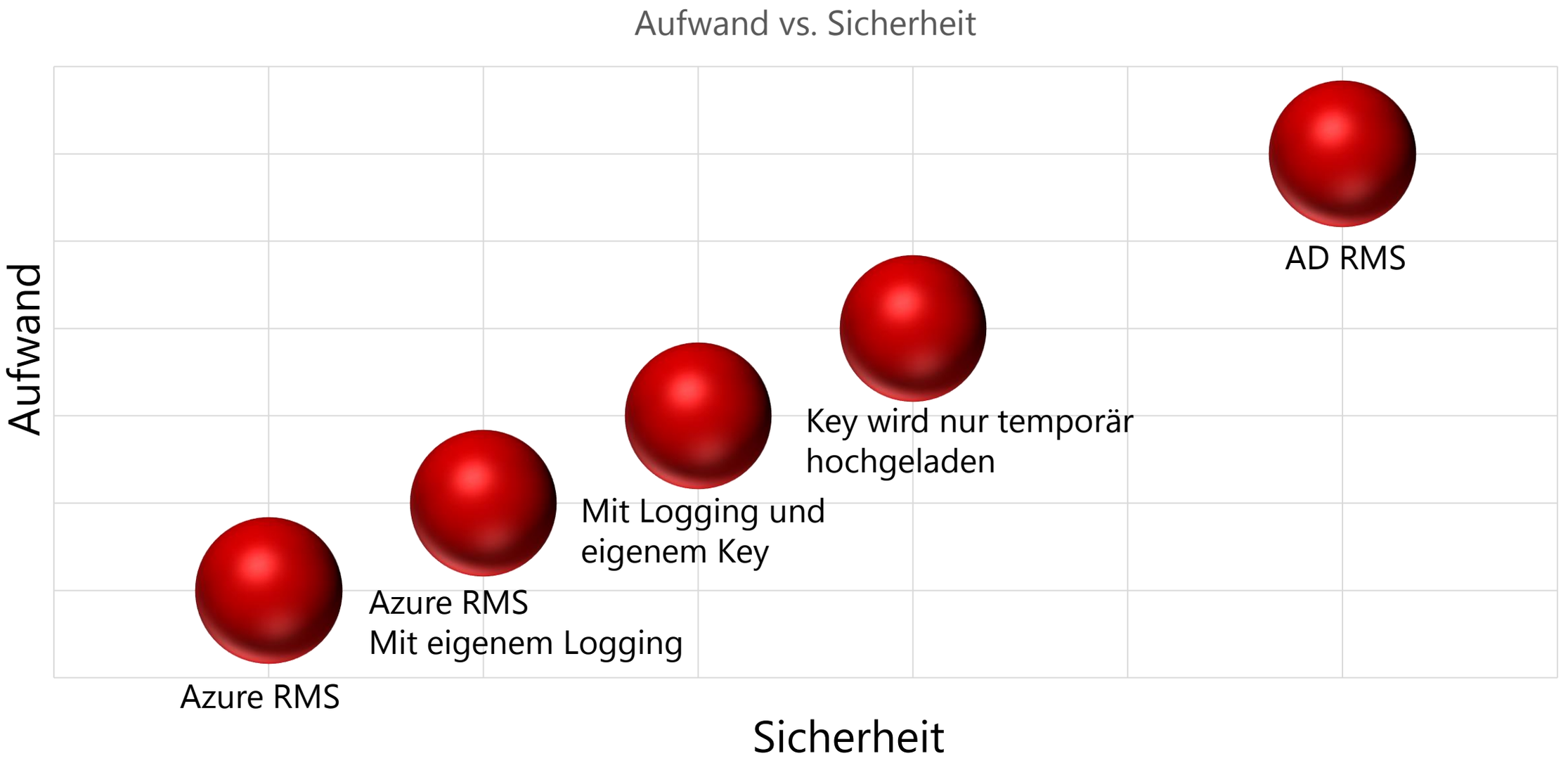
Demo

Azure Rights Management Service

- Einfache Integration
- Zugriffsrechte
  - Lesen
  - Kopieren
  - Verändern
  - Drucken
  - Weiterleiten (bei Mail)
  - Eigene können definiert werden



Azure RMS – Level of paranoia



Azure RMS - Create Policies

Sogenannte RMS Templates werden über das Azure Portal verwaltet

Demo

Konsumieren von Azure RMS geschützten Daten

Auf allen verbreiteten Geräten ist die Möglichkeit gegeben, geschützte Daten zu lesen

RMS Sharing App (https://portal.aadrm.com/home/download)

➡ Demo

Microsoft Intune für Mobile Device Management

- Integriert sich in bestehende SCCM 2012 Infrastrukturen
- Funktioniert ohne Agent
- Ist auf BYOD Szenarien ausgelegt
- Unterstützt durchgängig eine Identität

Microsoft Intune - Möglichkeiten

- Profile und Zertifikate verteilen

  Profiles: Exchange, WLAN, VPN

- Compliance Settings erzwingen

  Beispiel: Das löschen des Company Portals unterbinden

- Diverse Funktionen des Geräts steuern

  Kamera, Copy/Paste, Passwortzwang

- APPs auf Company Portal publizieren und «favorisieren»

Blog:
www.sccmfaq.ch

Twitter:
@hosebei

itnetx gmbh • bremgartenstrasse 37 • 3012 bern
phone +41 (0)31 802’05’05 • info@itnetx.ch • http://www.itnetx.ch