Citrix Day 2014
WES Konsolidierung NetScaler

06. November 2014

Chris Bässler
System Engineer

Ausgangslage

- Anforderungen zur Integration von Businessappliaktionen
- Anforderungen zur Einführung von Mobile Apps
- Keine Standardisierte Lösung (verschiedene ReverseProxies/WES)
- Kein zentraler Eingangspunkt
- Loadbalancing nur im eCommerce Bereich (DMZ)
- Ablösung "end of life" Komponenten (Cisco ACE, MS TMG)
- Zentrale Verwaltung der SSL-Zertifikate
- Big Fail bei Security Issues (z.B. SSL Heartbleed)

Projekt Ziele

BKW

- Servicedefinitionen ✓
- Plattformentscheid ✓
- Architektur NS Infrastruktur ✓
- Aufbau und Schulung ✓
- Konsolidierung bestehnder NS ✓
- Ablösung TMG
- Ablösung Reverse Proxies ✓
- Ablösung CISCO Loadbalancer ✓
- Vorkonfiguration SSO & WAF ✓

Plattformentscheid

Pro/Contra SDX

Pro:

- 5 VPXn Platinum Edition bereits pro SDX enthalten
- Zentrales Update / Deployment der VPXn direkt aus dem SDX
- Monitoring der tatsächlich genutzten Ressourcen
- Einsatz von SSL-Chips (reduzierte Last der CPUs)
- Betrieb von ca. 20 VPXn pro SDX (je nach SDX und Leistung der VPX)
- Physikalische und virtuelle Netzwerktrennung (SR-IOV Netzwerkkarten)
- Zentrales Backup und Versionsverwaltung aller VPXn über SDX
- Zukunftssicher durch Integration eigener/externer virtueller Appliancen

Contra:

- Neue Plattform, bisher noch nicht in Betrieb bei BKW
- Beschaffung neuer SDX Appliance bei >20 VPXn (je nach Leistung)
- Redundante Netzanbindung nur über LACP Channel (Thema Bonding activ-activ/activ-passiv)

Plattformentscheid

VPX auf VMWare / Pro und Contra

Pro:

- VMWare Plattform schon seit langem im Betrieb
- KnowHow im Betrieb und Engineering vorhanden
- Standard Hardware Einsatz (HP DL380 Gx)
- VPX Appliances verfügbar

Contra:

- Aufbau eingenständiger NS VMware Umgebung (DMZ/Intranet)
- Keine SSL Chips Unterstützung in VPX
- 2 Hersteller involviert bei Problemen (VMware & Citrix)
- Kein zentrales Patchen möglich
- Zusätzliche VMWare Lizenzen für neue Umgebung
- Hohe VPX Kosten

Plattformentscheid

VPX auf XenServer / Pro und Contra

Pro:

- Citrix Plattform schon durch Einsatz virtueller Arbeitsplätze (VDI/PDI)
- VPX schon in Betrieb (Intranet SSO, XenDesktop)
- Standard Hardware Einsatz (HP DL380 Gx)
- 1 Hersteller involviert, da alles aus einer Hand (Citrix)

Contra:

- Aufbau eingenständiger NS VMware Umgebung (DMZ/Intranet)
- Keine SSL Chips Unterstützung in VPX
- Falsche CPU/Memory Auslastungswerte über XenCenter
- Kein zentrales Patchen möglich
- Hohe VPX Kosten

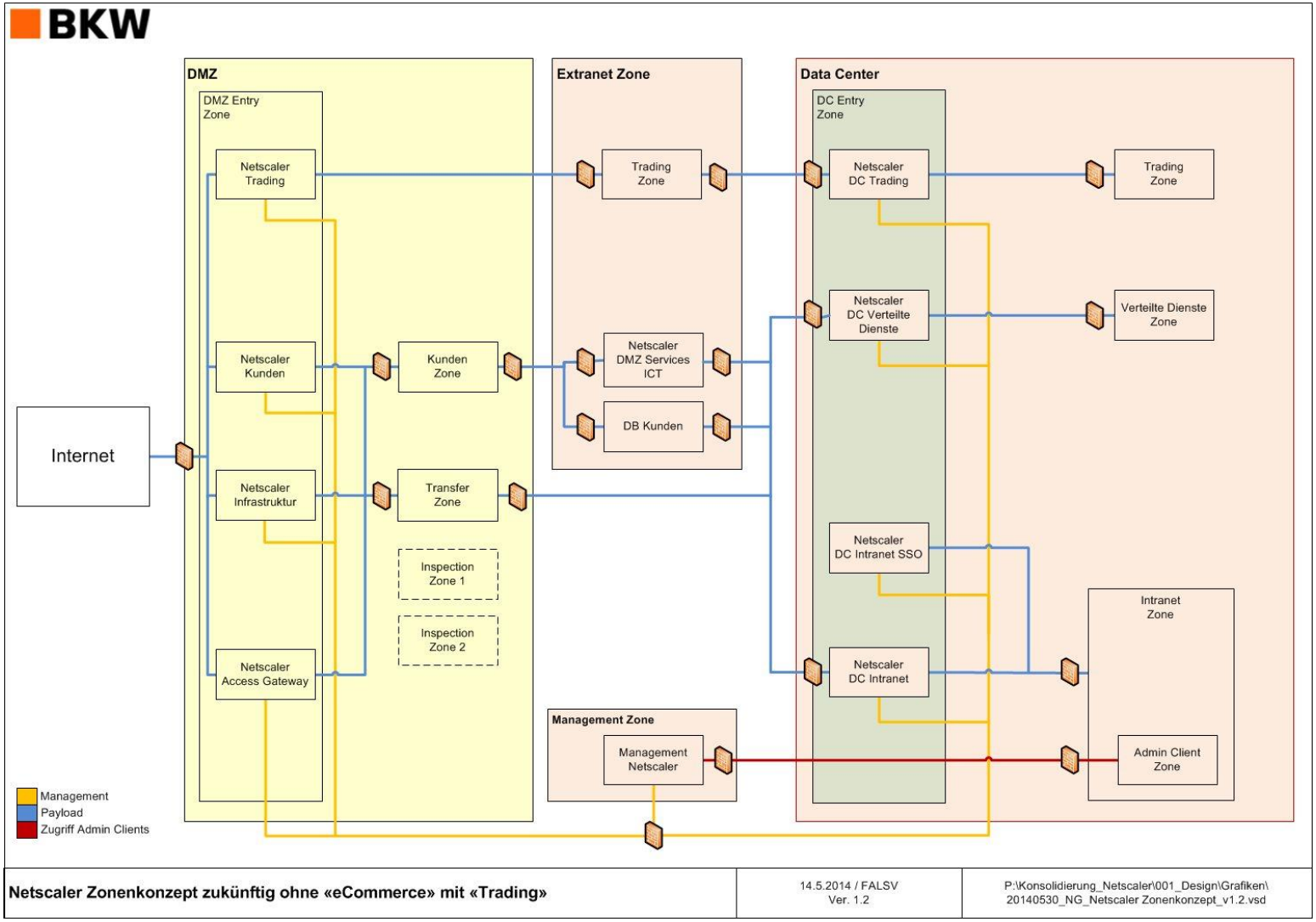
Architektur Konzept

Plattform

- 4 SDX Appliancen (Citrix SDX 11515)
- 2 x SDX Produktion und 2x SDX Test/Qualitätssicherung
- Aufbau Standortübergreifend (Bern - Mühleberg)
- 36 VPX (18 x P HA und 18 x Q/T HA)
- Aufbau "Entry Zone DMZ" und "Entry Zone Intranet"
- VLAN-Trennung zwischen T/Q und P (je /25)
- Aufbau Mangement Zone (für SDX und VPX)
- Umgestaltung BKW Netzwerkzonenkonzept

Architektur Konzept

Netzwerkzonen Zielbild (nach Abschluss Projekt)



Architektur Konzept

Plattform Betrieb / Engineering Teil 1

- Standardisierung
- ICT Security abgestimmte und genehmigte Lösung
- Betriebsteam betreibt die Plattform von der Hardware bis zur virtuellen Instance und Service
- Neue Instanzen & Services werden durch Engineering auf der Testumgebung aufgebaut, getestet und CLI Commands mittels Change beschrieben
- Engineering integriert die neue Lösung mit dem Betrieb zusammen auf der Q Umgebung
- Betrieb integriert und testet die Lösung selbständig auf der P Umgebung und passt die Dokumentation an

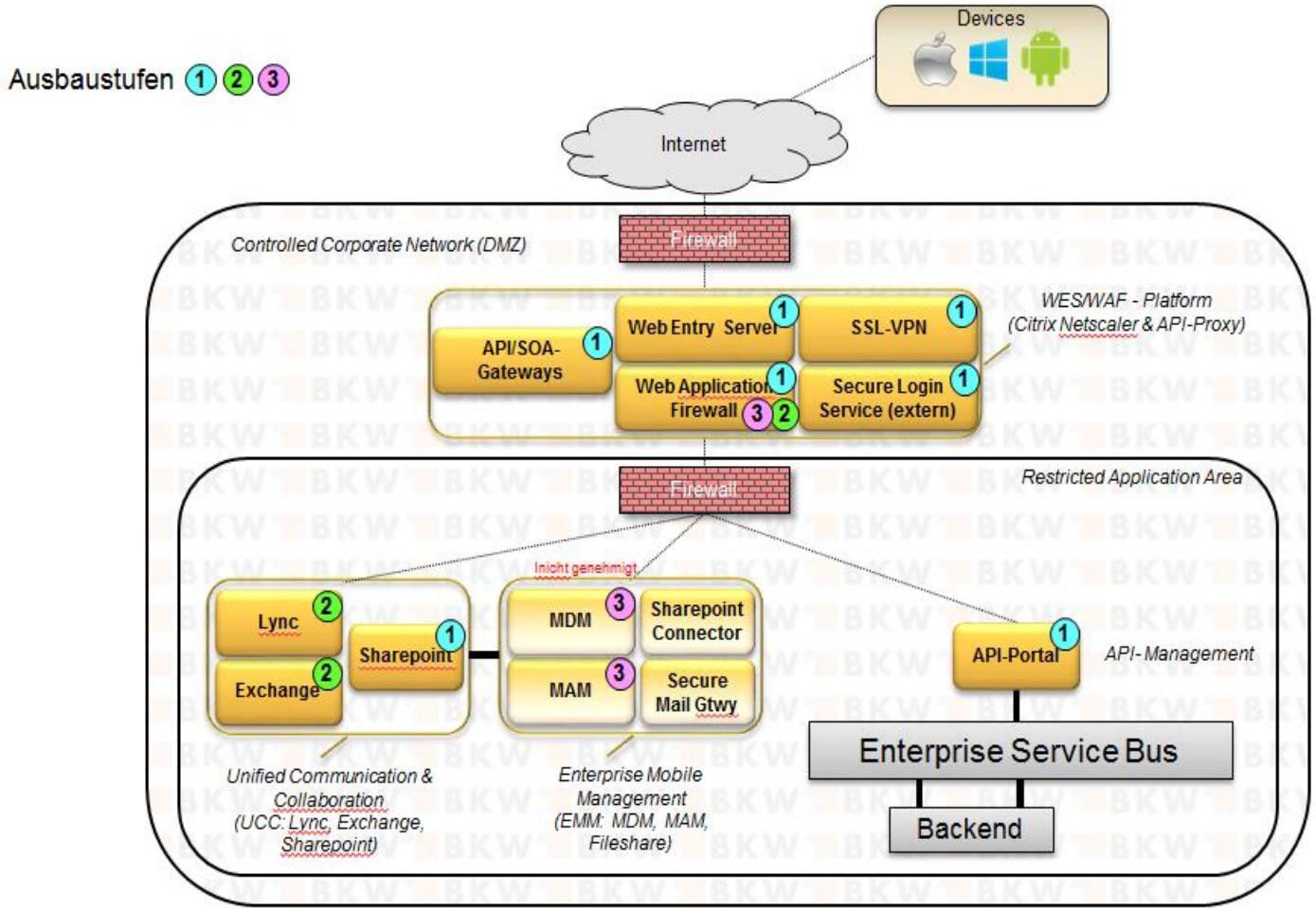
Architektur Konzept

Plattform Betrieb / Engineering Teil 2

BKW

Tätigkeit	Umgebung	IOC	IEN	Bemerkung
Monitoring • Engineering • Betrieb	T,Q,P T,Q,P	V V	M M	• Monitoring wird in Zusammenarbeit mit IEN integriert und getestet
Backup • Engineering • Betrieb	T,Q,P T,Q,P	V V	M M	• Backup wird in Zusammenarbeit mit IEN integriert und getestet
Restore	T,Q,P	M	V	• In Zusammenarbeit mit IEN
Lizenzmanagement	T,Q,P	?	?	•
Failover Tests	T,Q,P	V	I	• Pro Halbjahr 1 x Failover Test der VPX Appliances
Useradministration SDX/VPX	T,Q,P	V		• LDAP-Anmeldung mit AD-Gruppen
Release-/Patchmanagement	T,Q,P	M	V	• IEN prüft Patches und neue Releases und gibt diese mittels Change an IOC frei
Installation Patches/Releases	Q,P	V	I	• wird mittels Change auf Anforderung IEN durchgeführt • Ausnahme Installation aufgrund eines Citrix SRs • Q Durchführung bei Bedarf in Zusammenarbeit mit IEN
Installation Patches/Releases	T		V	• IEN installiert, prüft und validiert die neuen Patches/Releases • Übergabe und Drehbuch an IOC mittels Change
Aufbau neuer SDX	P	V	M	• In Zusammenarbeit mit IEN • Dokumentation durch IOC im BHB
Aufbau neuer SDX	T		V	• Erstellung Drehbuch
Aufbau neuer VPX	P	V		
Aufbau neuer VPX	Q	V	M	• In Zusammenarbeit mit IEN • Dokumentation durch IOC
Aufbau neuer VPX	T		V	
Bereitstellung neue VLAN SDX	P	V		
Bereitstellung neue VLAN SDX	T	M	V	• Durchführung IEN • Durchführung IOC bei Bedarf durch Change von IEN

Zielbild Architektur



Herzlichen Dank

Citrix Day 2014
Mobile@Work

06. November 2014

Marco Fernandez
System Engineer

Auftrag der Innovationsstudie

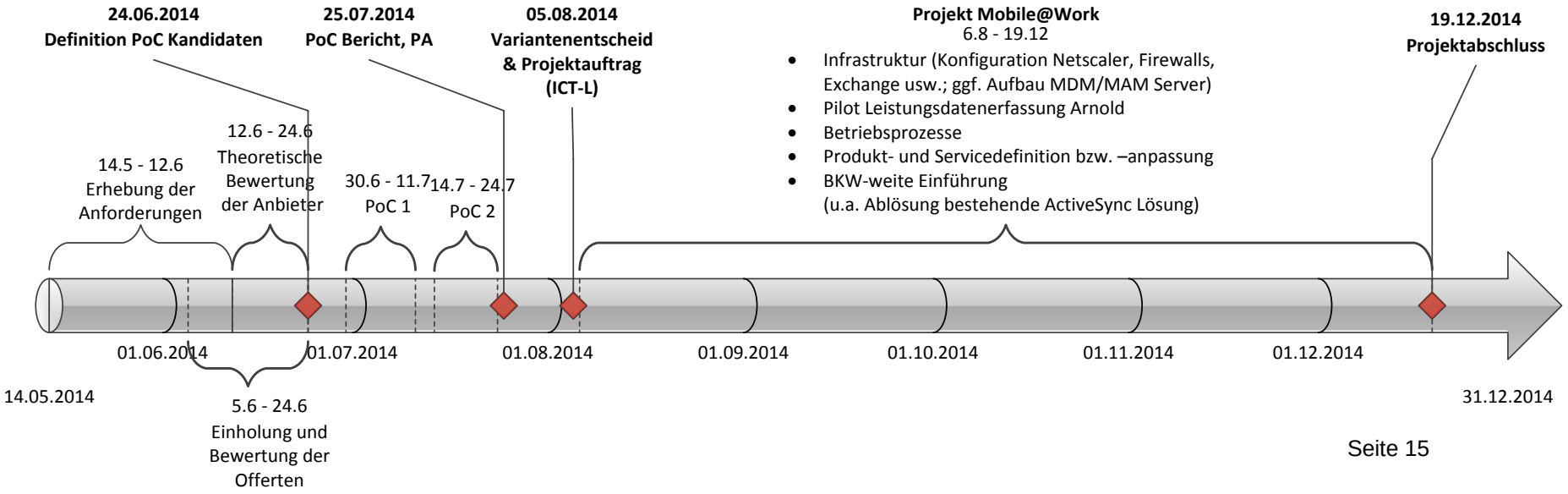
Auftrag der Innovationsstudie Mobile@Work:

Im Rahmen der Innovationsstudie Mobile@Work soll eine Lösung evaluiert werden, mit der Benutzer auf einem Mobile Device einen geschützten Zugang zu BKW Applikationen und zugehörigen Daten erhalten. Angestrebt wird insbesondere:

- einen Mehrwert für die Anwender (Funktionalität, Mobilität, Flexibilität)
- die Vereinfachung und Verbesserung von Business- und Anwender Prozessen
- ein effizienter Betrieb und eine effektive Servicebereitstellung und –Nutzung
- Inventarisierung (Corporate, BYOD)

Vorgehen

Innovationsstudie 14.05.2014 – 05.08.2014	1. Erhebung der Anforderungen 2. Theoretische Evaluation • Einholung von Offerten • Theoretische Bewertung der Anbieter 3. Durchführung Proof of Concepts 4. Variantenentscheid
Projekt Mobile@Work August – Dezember 2014	1. Projektauftrag 2. Aufbau Infrastruktur, ggf. Pilot Arnold 3. Betriebsprozesse 4. Produkt- und Servicedefinition bzw. -anpassung 5. Einführung



Auswahlverfahren für PoC

Beschränkung der Evaluation:

- Bewertung der Hersteller bei Gartner.
- Synergien mit bestehenden BKW-Infrastrukturen.
- Möglichkeit, die Lösung als externen Service zu beziehen.

➔ Betrachtete Lösungen:

- Citrix XenMobile
- VMware AirWatch
- MobileIron
- Microsoft Intune (Service)

PoC Kandidaten:

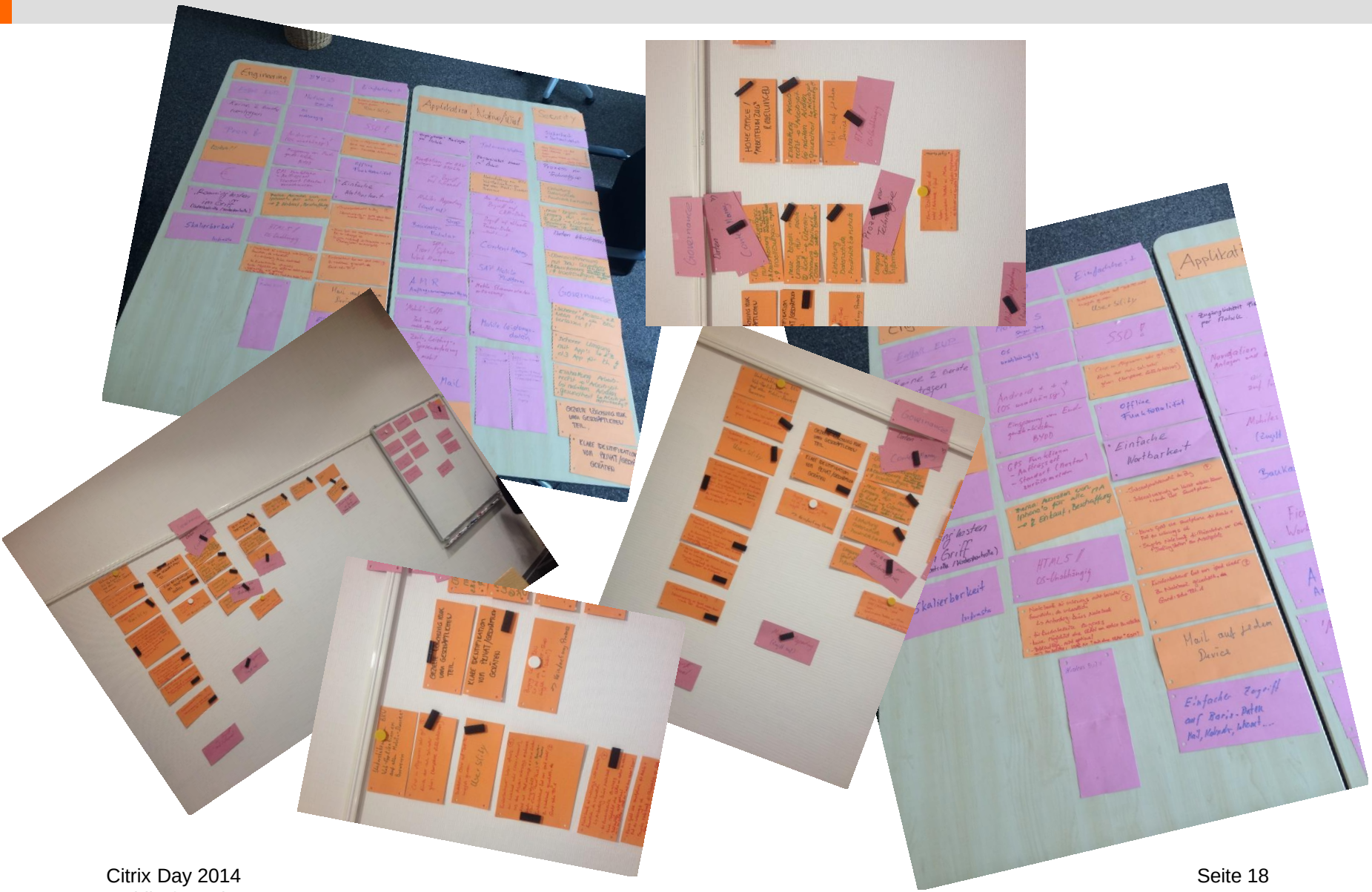
(1) Citrix **XenMobile** bietet erhebliche Synergien zu den laufenden Netscaler Aktivitäten und kann wegen des vorhandenen Know How relativ kurzfristig intern umgesetzt werden.

(2) MobileIron

(3) Microsoft **Intune** wird im Hinblick auf die Client Strategie 2016 geprüft.

Aufnahme der Anforderungen

Auswertung Teamarbeit



Ergebnisse 1/2

Mobile Device Management:
Alle Mobile Devices, die von der BKW ausgegeben wurden oder Zugriff auf BKW Ressourcen haben, werden mit einem Device Manager verwaltet.

Mobile Application Management:
Geschäftliche Daten oder Applikationen dürfen nur noch in einem geschützten Business Container betrieben und nicht mehr mit privaten Daten oder Apps durchmischt werden.

Ergebnisse 2/2

- Bestehende ActiveSync Lösung wird eigener E-Mail Client ersetzt.
- Zugriff auf Webseiten im Intranet / HTML 5 Content
- Zentralisierte Authorisierung und Authentisierung (SSO)
- VPN- Funktionalität
- Remote Wipe NUR Business Daten
- Intrgration Netscaler
- Bearbeiten von Office Dokumenten (Offline)
- Fotos hochladen
- BYOD

PoC 1: XenMobile Erkenntnisse

BKW

Positiv:

- ✓ Integration in die Netscaler Infrastruktur einfach umsetzbar
- ✓ Sämtliche Use Cases des PoC in kurzer Zeit umgesetzt
- ✓ Einfacher Enrollmentprozess
- ✓ Integrierte Lösung für Mobile Apps
- ✓ Zugriff auf XenDesktop und XenApp
- ✓ Übersichtliche Management Konsole
- ✓ Self Help Portal für Benutzer mit Funktionen selective und full Wipe, Lock, Locate
- ✓ Wrapping von iOS, Android und Windows Apps innert weniger Minuten
- ✓ Direkte Interaktion mit AD, d.h. just-in-time-Deaktivierung
- ✓ Worx Store als App integriert (Worx Home)

Negativ:

- – Separate Management Konsolen für XDM und XAM
- – ShareFile derzeit nur als Cloud Service verfügbar; künftig aber auch on-premise ☺
- – Windows Phone nur ab 8.1 und mit viel Aufwand unterstützt

PoC 2: MobileIron Erkenntnisse

Positiv:

- ✓ MobileIron bietet API für Zugriff auf GEO Location
- ✓ Usability der Apps im Business Container
- ✓ Self Help Portal mit den Funktionen Wipe und Locate
- ✓ Direkte SMS Anbindung
- ✓ Eine Konsole

Negativ:

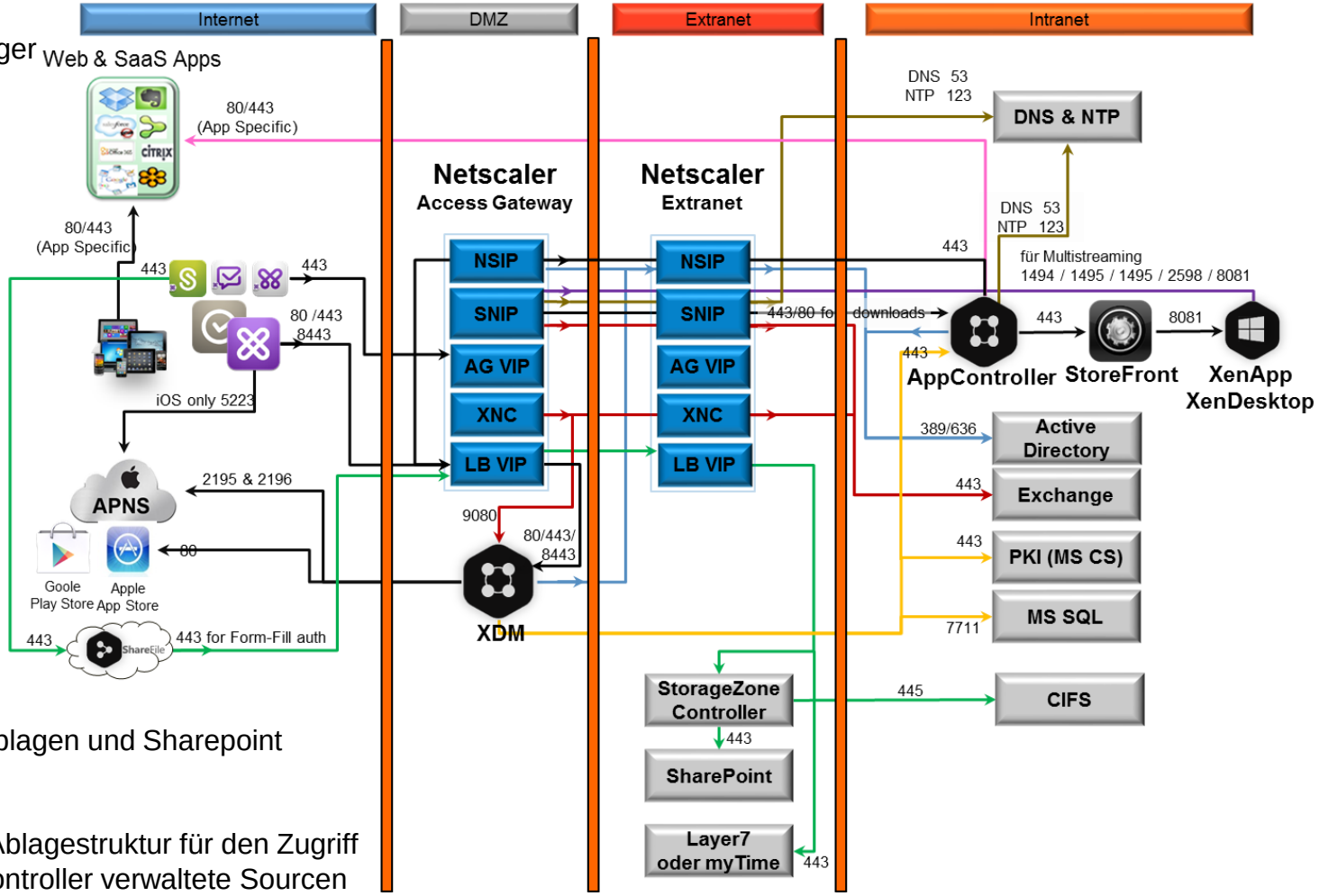
- AppStore nicht als App integriert
- Policy-Erstellung umständlich
- App Wraping nur durch MobileIron durchgeführt (Lange Durchlaufzeit)
- MAM unterstützt Windows Phone in der getesteten Version nicht
- Remote Wipe wurde erst nach mehreren Stunden ausgeführt
- Keine direkte Einbindung in die XenApp und in die XenDesktop Infrastruktur
- Integrierte SSO nur über Kerberos Constrained Delegation

Zielarchitektur XenMobile

BKW

XDM:
- XenMobile Device Manager
- Verwaltung Endgeräte

AppController (XAM):
- XenMobile Application Manager
- virtual Appliance
- Verwaltung mobile Apps



StorageZone Controller:
Zugriffssteuerung auf Fileablagen und Sharepoint

ShareFile:
- Web User Interface mit Ablagestruktur für den Zugriff auf vom StorageZone Controller verwaltete Sourcen

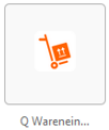
Optimierung der Business Prozesse

Zeit und Auftragserfassung für die Monteure der Firma Arnold (im Abacus)

Netzwerkelektriker, Instandhaltung, Versorgungsunterbrüche Push Messages

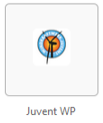
Zeiterfassung im SAP

Zentrale Kommunikations- Plattform der BKW (Intranet)



Bestätigen der Bestelleingänge im SAP mit SSO ist keine App sondern HTML 5 Webseite.

Das Fahrzeug kann reserviert werden und die Kilometer können direkt in die App aufgeschrieben werden.



Juvent WP Windpark ::: Windräder, Standort Auslastung des grössten Windkraftwerks der Schweiz

Sharepoint Zugriff::

- **Fotos Up and Download**
- **Topographische Pläne vom Auftraggeber (z.B.: SWISSCOM)**
- **Projektabläufe und Dokumentation**

Fragen?