SAP und Oracle einen Plan, welche neuen Funktionen und Technologien in das neue Oracle-Datenbank-Produktpaket für SAP eingebaut werden sollen. Die In-Memory-Datenbank-Option ist für viele SAP-Kunden sehr interessant und wichtig. Aus diesem Grund ist davon auszugehen, dass die In-Memory-Datenbank-Option unmittelbar nach Verfügbarkeit von Oracle 12.1.0.2 dem Zertifizierungsprozess zugeführt wird. Dass der SAP-Oracle-Kundenkreis sehr an einer Lösung interessiert ist, die einen signifikanten Schritt hinsichtlich höherer Performance erlaubt, ohne eine bestehende Umgebung vollständig „abreißen" und neu aufbauen zu müssen − mit all den bekannten technischen und finanziellen Risiken −, zeigen die vielen Gespräche, die wir bisher zu diesem Thema geführt haben.

Wie können DOAG-Mitglieder, die sich für diese Option interessieren, die Technologie intensiv und umfassend erlernen?

Stürner: Wenn die DOAG für ihre Mitglieder ein besonderes Seminar oder einen Workshop über dieses Produkt organisieren möchte, sind wir jederzeit bereit, die notwendigen Schritte einzuleiten. Wir können auch sogenannte „Test-Drives" durchführen; gerne auch als exklusive DOAG- Veranstaltung. Dieses spannende Thema wird uns die nächsten Jahre auf Trab halten und uns noch viel Freude bereiten.

Finger weg von meinem Telefon!

Steffo Weber, ORACLE Deutschland B.V. & Co. KG

Der Grund dafür, dass die meisten Unternehmen eine sehr restriktive Desktop-Richtlinie, aber keine klare Strategie für mobile Geräte haben, ist, dass iPhones, iPads & Co. genau das sind, was PCs niemals waren: persönlich und benutzerfreundlich. Die Standardstrategien im Umgang mit mobilen Geräten (VPN, Verbot mobiler Geräte, MDM etc.) machen diese Geräte unpersönlich oder die Bedienweise unfreundlich. Wesentlich effektiver ist es, nicht das Gerät zu managen, sondern die unternehmensbezogenen Daten und Dienste, auf die zugegriffen wird.

Aktuell konkurrieren verschiedene Ansätze (Mobile Application Management, Mobile Device Management, Containerization/Virtualization, Data Leakage Prevention, Mobile Access Management) zum Schutz von – ja, was denn eigentlich? – mobilen Geräten, mobilen Daten und Diensten für mobile Geräte untereinander. Sie werden hitzig diskutiert. Einer der interessantesten Kommentare hierzu lautet „I just came across another interesting statistic. According to a Juniper survey, the average mobile user owns 3 internet-connected devices. (...). But, and get this, 18% own 5! Can you imagine what it would be like for IT to manage these? To me, it's clear that IT should focus on managing THEIR data, and not any device."

Mobile Geräte sind – und das ist entscheidend – eben nicht lediglich ein neuer Gerätetyp, sondern benötigen ihre eigene, angepasste Infrastruktur. Sie repräsentieren einen Kulturwechsel, der sich schon seit Jahren vollzieht und zu einer immer stärkeren Ästhetisierung und Individualisierung führt. Dies betrifft auch die lange Zeit ästhetisch entkernten Bereiche wie Ökonomie und Bürowelt: Rein zweckorientierte beige PCs weichen smarten Tablets und die Software-Ergonomie ist Teil dieses Wechsels. Diese Entwicklung verlangt von Unternehmen ein grundsätzliches Umdenken im Hinblick auf folgende Aspekte:

- *Geändertes Nutzerverhalten und neue Nutzeransprüche*
  Nutzer zeigen bei mobilen Anwendungen weniger Bereitschaft, sich in die Tücken einer App einzuarbeiten, als bei Desktop-Anwendungen: Ladezeiten von über zwei Sekunden oder ein dreimaliger Absturz einer Anwendung führen bereits dazu, dass der Nutzer die App wieder löscht *[1, 2]*
- *Zugriff auf Business-Infrastruktur*
  Die Netz-Infrastruktur der meisten Unternehmen geht davon aus, dass das Unternehmen vollständige Kontrolle (Administratorrechte etc.) über das zugreifende Gerät hat. Das ist bei einem Smartphone nicht der Fall. Das Mantra lautet eben „bring your own device" und nicht „bring our own device".

Zwei Dinge sollte man genauer unter die Lupe nehmen: Welche unterschiedlichen Nutzertypen (intern, extern, Partner) greifen auf meine Daten zu und wo müssen die Daten geschützt werden – auf dem mobilen Gerät oder im Data Center?

Für Mitarbeiter und Partner: Sichere iOS-/Android-Container

Mitarbeiter und Partner verwenden typischerweise Apps (E-Mail, SharePoint etc.), die vom Unternehmen zwar bereitgestellt, aber nicht entwickelt werden. Dies ist ein Unterschied zu den Apps, die ein Unternehmen für Endkunden in Eigenregie entwickelt und hierbei alle Sicherheits-Features wie Datenverschlüsselung unter Kontrolle hat. Wie kann man also Daten, die von nicht selbst entwickelten Apps verarbeitet werden, so schützen, dass die mobile User Experience weiterhin gewährleistet ist?

Wenn der Privatheits-Charakter eines mobilen Geräts (mit dem wir Fotos und Memos aufnehmen, persönliche Nachrichten speichern) gewährleistet werden soll, greifen klassische Mobile-Device-Management-Lösungen (MDM) zu kurz. Sie sorgen lediglich dafür, dass Dritte das Gerät mit einer Managementsoftware verwalten. Hierbei spricht man nicht mehr von „bring your own device" (BYOD), sondern von „company owned, personally enabled" (COPE). COPE ist aufgrund von rechtlichen Grauzonen wie dem Löschen von persönlichen Fotos beim Geräte-Management umstritten. Eine Container-Lösung, bei der der Nutzer weiterhin vollständige Kontrolle über das Gerät hat, kann ein brauchbarer Kompromiss zwischen dem „Y" (your device) und den Sicherheitsinteressen eines Unternehmens sein:

- Die zu schützenden Unternehmensanwendungen (SAP-Clients, SharePoint-Apps, Mail-Client) werden hier in einem isolierten Container installiert. Daten (E-Mails, SharePoint-Dokumente) können diesen Container zumindest nicht unverschlüsselt verlassen.
- Eine Fernwartung wie das Löschen von Dokumenten ist problemlos möglich. Auf Daten außerhalb des Containers (wie Fotos, Musik) kann per Fernwartung nicht zugegriffen werden. Daten, die dem Unternehmen gehören und sich im Container befinden, lassen sich also durch das Unternehmen auf Knopfdruck löschen – private Fotos etc. nicht.
- Der Netz-Zugriff von Container-Apps erfolgt ausschließlich über die Protokolle Transport Layer Security (TLS) und Secure Sockets Layer (SSL). Der SSL-Endpunkt steht hierbei im Unternehmensnetz. Mit anderen Worten: Sämtliche Kommunikation läuft über ein Unternehmens-VPN (TLS-basiert).

Abbildung 1 zeigt die Funktionsweise einer Containerlösung (hier am Beispiel von Oracles Secure Container). Die Container-App (roter Block auf dem Smartphone) stellt für Unternehmens-Apps eine gesicherte Umgebung bereit. Die von den Apps auf dem Smartphone abgespeicherten Daten werden verschlüsselt, Copy & Paste in Anwendungen außerhalb des Containers ist nicht möglich. Drucken kann ebenfalls unterbunden werden. Der Container stellt eine Umgebung für Apps zur Verfügung, die

- sämtliche von der App gespeicherten Daten verschlüsselt
- Copy & Paste an Nicht-Container-Apps verhindert (auch nicht mit dem Share Button, über den ein an einer E-Mail hängendes PDF-Dokument an Dropbox weitergeleitet werden kann). An welche anderen Apps-Dokumente weitergeleitet werden kann, lässt sich in der Oracle-Lösung konfigurieren: Dropbox kann verboten, Ignyte beispielsweise erlaubt sein.

Damit eine App innerhalb des Containers laufen kann und die Mechanismen (Copy/Paste-Schutz etc.) des Containers wirksam werden, muss die App modifiziert sein. Dies kann automatisch erfolgen, die App

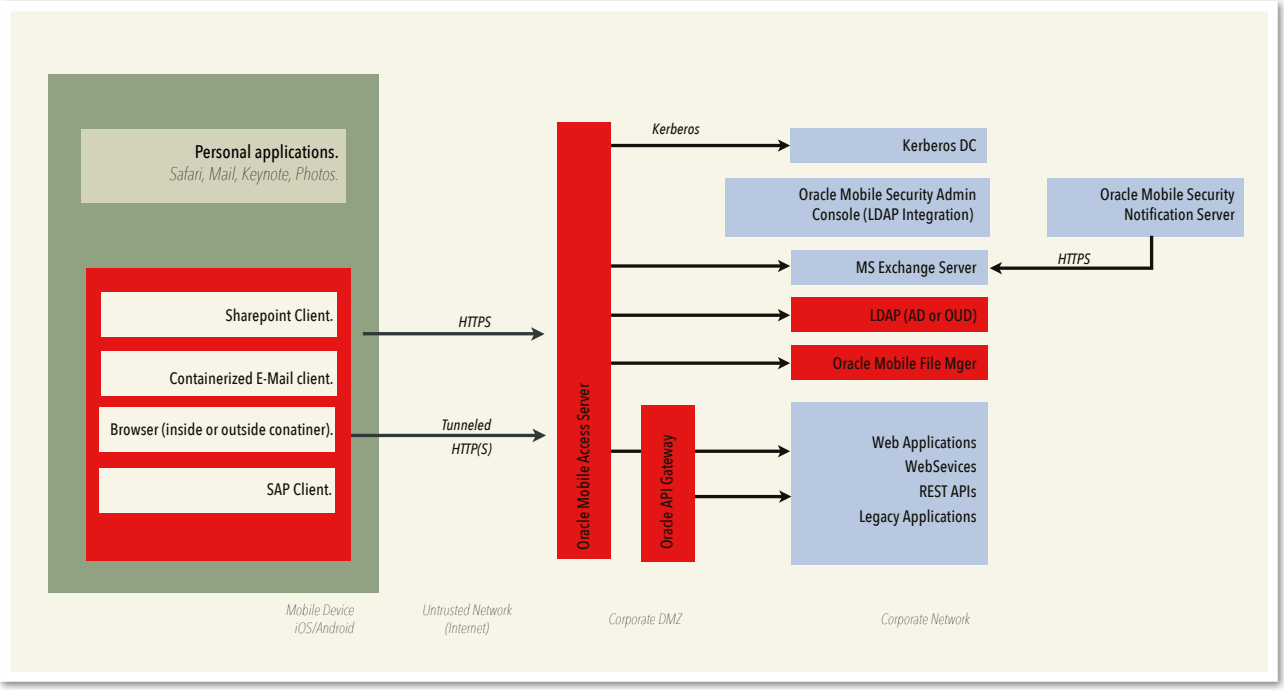

Abbildung 1: Funktionsweise einer Containerlösung

muss hierzu nicht im Quellcode vorliegen. Einzige Voraussetzung ist, dass die App unsigniert ist. Dies bedeutet zunächst, dass die aus dem Apple AppStore oder Google Playstore geladenen Apps nicht im Container lauffähig sind. Business-Apps hingegen (wie SAP Fiori Suite, Oracle Apps) können ohne Probleme eingesetzt werden, da viele Firmen (Colligo, Oracle, Nitrodesk, SAP etc.) ihren Kunden diese Apps unsigniert zur Verfügung stellen.

Tabelle 1 zeigt eine Gegenüberstellung von klassischen Mobile-Device-Management- und Container-Lösungen. Der Hauptunterschied: Es kann nur eine MDM- auf dem Gerät geben, aber mehrere Container-Lösungen. Mit anderen Worten: MDM ist ein Vendor Lock, Container hingegen nicht. * Hier kann man sich im Produkteinzelfall darüber streiten, ob MDM-Lösungen auch DLP-Lösungen sind. Ich finde in diesem Zusammenhang folgenden Kommentar (eines DLP-Herstellers) bemerkenswert: „Sixty-plus MDM vendors have hijacked the term "data loss prevention"-DLP- because data loss is a big problem for their customers. Customers want DLP solutions. No matter how often MDM vendors say they are, MDM isn't DLP". – Quelle: http://www.spydrsafe.com/why-mobile-device-management-doesnt-matter/#sthash.l5CBmESi.dpuf

	MDM	Container
Schutz von privaten Daten (Fotos, Kontakte etc.)	N	J
Verschlüsselung von Geschäftsdaten	N	J
Einführung rechtlich unbedenklich in DE	unklar	J
Lösung für Mitarbeiter und Kunden geeignet	N	J
App kann aus Apples Appstore oder Playstore übernommen werden	J	N
Digital Leakage Prevention, DLP	N*	J
Es können mehrere Lösungen auf einem Smartphone installiert sein (Vendor Lock)	N	J

Tabelle 1: Gegenüberstellung von MDM- und Container-Lösungen

Tabelle 2 zeigt die drei Typen von Anwendungen, die unterschieden werden können. Abgesehen von der Frage: „Laufen die für mein Unternehmen wichtigen Anwendungen im Container?", sind auch allgemeinere Aspekte zu klären, darunter:

- *Kommunikationspfade*
  Ein Container muss die Hintergrund-Dienste (Mail, SharePoint, Fusion Apps, SAP etc.) für die im Container laufenden Apps erreichbar machen. Hierzu wird typischerweise ein verschlüsselter Kanal (IPSEC, TLS/SSL) aufgebaut. Bei manchen Lösungen führt dieser Kanal immer über Cloud Services des Container-Herstellers, was bei der Oracle-Lösung nicht der Fall ist.
- *Unterstützte Betriebssysteme*
  Fast alle Hersteller unterstützen zurzeit iOS und Android, Windows Phone oder Blackberry haben eher Nischen-Charakter. Wichtig ist, den Enterprise- und nicht den Consumer-Markt zu berücksichtigen.
- *Einheitliches Identitätsmanagement*
  Kann die Identität des mobilen Nutzers so weit in das Unternehmensnetz propagiert werden, dass ein echtes Single Sign-on (in Windows-Umgebungen per Kerberos oder in Web-Umgebungen per SAML) möglich ist?
- *Silo-Lösung vs. integriert in die Unternehmensplattform*
  Beherrscht das Produkt einheitliches Enterprise Access Management oder ist es lediglich eine Remote-Access-Lösung?

Access Management sorgt für bessere User Experience, erhöhte Sicherheit und smartes Marketing

Die große Änderung, die die mobile Welt mit sich bringt, ist, dass sich der klassische Präsentations-Layer einer „n-Tier"-Architektur auf dem Smartphone befindet: Die App ist der Präsentations-Layer. Dies bedeutet, dass Maßnahmen wie Authentisierung das Vertrauensverhältnis zwischen Smartphone-Präsentations-Layer und Businesslogik (Service Layer) sicherstellen müssen *(siehe Abbildung 2)*.

Wird von einem per MDM verwalteten Gerät oder einer Container-App auf einen Dienst zugegriffen, so kann man das Vertrauensverhältnis als hergestellt betrachten. Was aber, wenn beliebige Nutzer – insbesondere solche, denen man keine MDM- oder Container-Lösung vorschreiben kann, – auf die Dienste zugreifen? In diesem Fall muss sich der Nutzer am Dienst authentisieren.

Unternehmen geben jedoch nicht nur eine App heraus, sondern oftmals mehrere. Für Mitarbeiter können das Apps wie „Reisekosten", „Zeiterfassung" oder „Urlaubsantrag" sein, für Endkunden eines Zeitschriftenverlags die unterschiedlichen Zeitschriften-Apps. Selbst Baumärkte haben mehrere Apps im Angebot. Um den Nutzer beim Aufruf der verschiedenen Apps nicht immer mit einem Anmeldedialog zu konfrontieren, bietet Oracle eine SSO-Lösung für Apps an. Hierbei handelt es sich um ein echtes SSO-Protokoll und

Signiert/Unsigniert	Wo erworben?	Container-fähig	Typische Nutzer
Signiert	Appstore / Playstore	N	Beliebig
Unsigniert	Direkt vom Hersteller	J	Partner, Mitarbeiter
Unsigniert	Eigenentwicklung	J	Partner, Mitarbeiter, Endkunde

Tabelle 2: Klassifikation von Apps

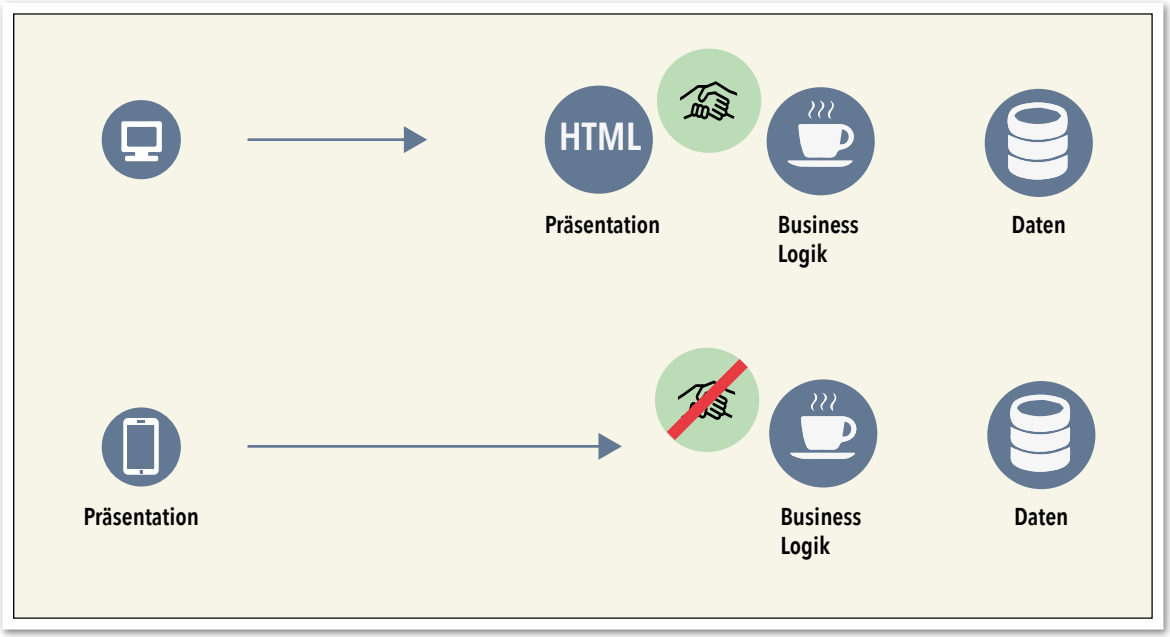

Abbildung 2: Geänderte Sicherheitslage gegenüber einer klassischen „3-Tier"-Architektur

nicht nur um das automatische Ausfüllen von Passwortfeldern. Die Vorteile einer SSO-Lösung für Apps sind:

- *Hintergrund-Dienste sind wirksam geschützt*
  Neben der Nutzer-Authentisierung kann auch die Geräte-Integrität (Jailbreak) überprüft werden. Geräte mit Jailbreak dürfen – je nach Richtlinie – nicht auf den Service-Layer (Business-Logik) zugreifen. Darüber hinaus ist eine Plausibilitätsprüfung beim Zugriff möglich: Erfolgt um 10:00 Uhr ein Zugriff mit Geolokation Hamburg und um 10:20 ein Zugriff aus Rom, so führt das System zusätzliche Sicherheitsabfragen (etwa Mädchenname der Mutter) durch.
- *Einfache Benutzung, gute User Experience*
  Die Design-Richtlinien von Apple empfehlen, dass Passwort-Abfragen möglichst selten (und möglichst spät) erfolgen. Beim SSO geschieht das nur einmal beim ersten relevanten Service.
- *Smartes Marketing*
  Der Herausgeber von sicherheitsunkritischen und kostenlos verteilten Apps kann von SSO profitieren: Die Baumarktkette bietet verschiedene Apps an, unter anderem eine App zur Ermittlung verschiedener Farbharmonien (ähnlich zu „kuler.adobe.com" oder

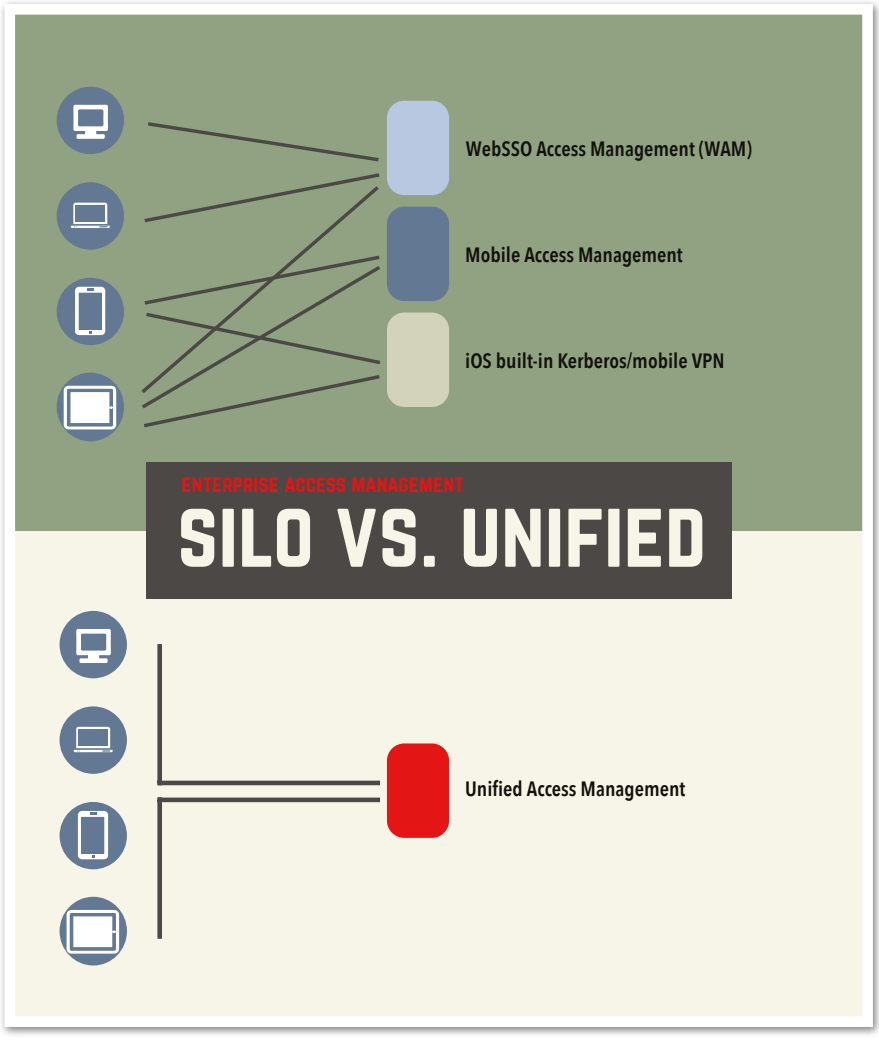

Abbildung 3: Access Management mit Identity Silos

Datenklasse	Eigner	Schutz von	Mechanismus	Nutzergruppe
Öffentlich	*	Dienst (REST WS)	Mobile Access Management	Beliebig (Kunden, Mitarbeiter)
Vertraulich	Smartphone Nutzer	Dienst (REST WS)	Mobile Access Management	Beliebig (Kunden, Mitarbeiter)
Vertraulich	Unternehmen	Dienst & Daten	Container	Partner & Mitarbeiter

Tabelle 3: Klassifikation von mobilen Zugriffen

„colourlovers.com") und eine andere zur Tapetenauswahl. Daten-Korrelationen der Art „Welcher Farbharmonie-Typ wählt welche Tapete" können aus Marketingsicht aufschlussreich sein. Der Schlüssel hierfür ist die (anonymisierte) App-übergreifende Nutzer-Identifikation.

Die nähere Funktionsweise eines App- und Browser-übergreifenden SSO ist in *[3]* beschrieben. Single Sign-on bietet also insbesondere bei mobilen Anwendungen neben der reinen Sicherheit auch Vorteile wie bessere User Experience und übergreifende Nutzer-Identifikation, die auch zu Marketingzwecken verwendet werden kann. User Experience und gerichtetes Marketing sind zudem aktuell stärkere Treiber als reine Sicherheitslösungen.

Fazit

Nutzer wollen Bequemlichkeit, Unternehmen ihre Daten schützen. Beides ist möglich, wenn man weiß, für welchen Nutzertypus die Lösung angeboten werden soll und wo die zu schützenden Daten liegen. Die architekturelle und produktspezifische Herausforderung wird darin bestehen, die unterschiedlichen Zugriffswege (VPN, Desktop Access, Mobile Access, Mobile Container) so zu vereinheitlichen, dass der Nutzer sich genau mit einer (und nur mit einer) Identität im (internen) Netz bewegt und seine Nutzungsmöglichkeiten größtenteils unabhängig vom verwendeten Gerät oder Kanal sind. Dies erst macht das Verwalten von Zugriffsregeln handhabbar *(siehe Abbildung 3)*. The Register *[4]* fasst dies in einem Artikel über den Mobile World Congress wie folgt zusammen: „This isn't just Mobile Device Management (MDM), this is Enterprise Mobility Management (EMM)".

Falls die üblichen Anmeldungspunkte wie VPN, Active Directory, Web Access Management (inkl. SAML) und App-Authentisierung (inkl. OAuth) die Nutzer-Identität nicht weiterleiten, muss sich der Nutzer mehrfach anmelden. Auch ein einheitliches LDAP-Verzeichnis löst dieses Problem nicht, Identitäten werden nicht propagiert (dazu gehört beispielsweise ein Weiterleiten der Art „Hier ist mein Kerberos-Ticket, bitte gibt mit ein SAML-Token dafür" oder „Hier ist ein SAML-Token, ich benötige ein OAuth Token". *Tabelle 3* grenzt die oben beschriebenen Mechanismen (Container, Mobile Access Management) bei der Verwendung von Services/Apps voneinander ab.

Referenzen

[1] Mobile Apps. What Consumers really want, offers2.compuware.com/rs/compuware/images/Mobile_App_Survey_Report.pdf

[2] mobilestatistics.com/mobile-news/the-rise-of-the-enterprise-tablet.aspx

[3] Weber, Steffo: Access Management 11g R2 für iOS und Cloud, DOAG News Nr. 1, 2013.

[4] http://www.theregister.co.uk/2014/02/24/mobile_world_congress_its_not_about_the_handsets_anymore

Steffo Weber
steffo.weber@oracle.com