Umsetzung Mobile Security

Michael Fischer
Oracle Deutschland
München

Schlüsselworte

Mobile Security, Sicherheitsklassen, Container, MAM, MDM, Single-Sign On, Starke Authentifizierung, 2-Faktor Authentifizierung, Verschlüsselung, OAuth, SAML, OpenID, Provisioning, Remote Wipe, Kontextbasierte Authorisierung, Device Fingerprint, TOTP (One Time Password), Android, Apple, Microsoft

Einleitung

Aus Sicht der **Unternehmen** ist es eines der Hauptziele gute Mitarbeiter zu aquirieren und zu halten. Häufig vergleichen dabei die (potentiellen) Mitarbeiter neben der Renommiertheit des Unternehmens auch deren Wettbewerbsfähigkeit hinsichtlich des Arbeitsplatzes. Hierzu zählen auch die Flexibilität bei der Arbeit an sich (work form Home, Nutzung der „Lieblingsgeräte“ und eines von überall erreichbaren Netzes). Lassen sich Unternehmen auf diese flexible Art der Arbeitsplatznutzung ein entsteht häufig eine Win-Win Situation. Der Mitarbeiter ist produktiver durch das angenehmere Arbeitsumfeld und auch ausserhalb der Anwesenheitszeiten erreichbar und er fühlt sich durch die eingeräumten Freiräume stärker wertgeschätzt.

Der Konkurrent ist nur einen Klick entfernt. Ein **Kunde** kann heute Angebote von Firmen mit minimalstem Aufwand vergleichen, so dass neben dem Preis, das Benutzererlebnis mehr kauf- oder bindungsentscheidend wird. Erkennbar ist das daran, dass sich online Shops oder Portale bemühen Informationen zielgerichteter (was wird wirklich gesucht) darzustellen und einfacher nutzbar zu machen (z.B. kaufen am Schluss ohne zusätzliche Hürden wie Porto, Zahlungsaufschläge, Anmeldungen). Bei vergleichbarem Portfolio muss der Mehrwert binnen kürzester Zeit sichtbar sein damit die Bindung nicht im frühen Stadium schon beendet wird. In einer App für ein Smartphone oder Tablet beispielsweise wird diese nach langen Wartezeiten oder Fehlversuchen prompt gelöscht und zum Wettbewerb gewechselt. Auch kommen neuartige Nutzungsszenarien hinzu wie im eHealth Umfeld mit dem Beobachten, Aggregieren und ggf. Auswerten von aktuellen Messgrössen unter Einbezug einer zentralen Stelle erfordern zusätzliche Kommunikationswege und Absicherungen.

Viele neue Initiativen in den Unternehmen werden aus den Fachbereichen und Marketing nicht nur initiiert, immer häufiger auch direkt und ohne Beteiligung der IT umgesetzt. Dies führt ohne übergeordnete Kontrolle zu einer Vielzahl von IT- und damit auch Sicherheitssilos, die langfristig teurer in Lizenzen und/oder Betriebskosten werden.

Eine **One-Fits-All Mobile Security Lösung** erscheint schon unter den o.a. Aspekten bedingt sinnvoll. Daher stellen wir exemplarisch ein abgestuftes Verfahren (im Folgenden als Sicherheitsklassen bezeichnet) zur Nutzung mit mobilen Devices vor sowie exemplarische Umsetzungen. Dabei liegt ein Augenmerk auf einer Integrationsmöglichkeit in ein Gesamtsystem, so dass auch Anforderungen wie zentrale Administrierung und Auswertung (inkl. Audit) Rechnung getragen wird.

Umsetzung Mobile Security

Zur Umsetzung wird im Folgenden zuerst unterschieden in die Anforderungen aus den Bereichen Kunden und Unternehmen um Sicherheitsklassen abzuleiten. In der Ausführung der Sicherheitsklassen wird Bezug darauf genommen inwieweit damit auch scheinbar andere Benutzerkreise (z.B. IoT Geräte) oder Anwendungsfälle (z.B. Cloud) abbildbar sind. Im Anschluss an die Definition wird die Umsetzung aufgezeigt und der Ort des Wirkens über eine einfache Architektur dargestellt.

Anforderungen

Die in der Einleitung aufgeführten Rahmenbedingungen bedeuten für Mobile Security aus **Kundensicht**:

Security darf sich nicht auf die Performance oder Nutzbarkeit von Geräten auswirken

Die Bedienung muss so intuitiv sein, dass diese nicht zum Abbruch führt

Schutzbedarfe müssen nachvollziehbar sein:

Zum Beispiel sind Unternehmensangebote wie Informationen oder Services transparent nutzbar, entweder ohne Login oder als angemeldeter z.B. facebook Nutzer über die sozialen Netzwerke die „sowieso“ genutzt werden.
Bei monitär sich auswirkenden Aktionen oder Übertragung/Nutzung persönlichen Daten (z.B. eHealth) je nach Sicherheitswunsch des Nutzers weitere intuitiv zu bedienende Authentifizierungen bzw. automatische Verschlüsselungen.

Aus **Unternehmenssicht** ergeben sich weitere Anforderungen

Es müssen attraktive und aktuellste Smart* unterstützt werden

Es muss zentral administrierbar sein

Die Schutzbedarfe müssen vermittelbar sein:

Beispielsweise gibt es unternehmenseigene stark in der Nutzung beschränkte Devices, die vollständig gemanagt werden, wie Kanzler- oder Vorstandsgeräte.
Mobilen Geräten wird der Zugang zu Unternehmensressourcen über einen sogenannten Container ermöglicht (sogenannte Mobile Application Mgmt / MAM). Dabei wird unternehmensseitig nur ein Teil des Geräts, der Container, gemanagt.
Zugang zu Unternehmensressourcen ermöglichen, die mit Hilfe des bestehenden Unternehmenszugriffssystems (Access Management) kontrolliert werden. Dabei spielt es keine Rolle ob dies aus einer nativen App heraus oder über den Browser erfolgt. Unternehmen stufen dabei den Einsatz der Sicherheitsklassen je nach Nutzergruppe ab, beispielsweise:

Abb. 1: Sicherheitsfunktionen angewandt von einem Unternehmen unterschieden nach Benutzergruppen

Sicherheitsklassen

Die Sicherheitsklassen decken die verschiedene Anforderungen ab. Diese werden aus zwei Perspektiven betrachtet, dem nutzenden Gerät bzw. dem Benutzer und der Infrastruktur, die die Services bereitstellt (im Folgenden „serverseitig“ genannt). Die Klassen sind aufeinander aufgebaut und enthalten zum Teil optionale Bausteine. Der Aufbau ist additiv gesehen, eine höhere Klasse enthält die Anforderungen der Niedrigeren.

Zur Strukturierung werden Bronze, Silber, und Gold als Klassen abgeleitet. Ist eine galvanische Trennung von Umgebungen gefordert, ist diese Aufteilung je Umgebung zu sehen, wobei ein Übergang zwischen den Umgebungen durch den Benutzer (z.B. mit Hilfe eines Smartphone Fotos) erfolgen kann, so dass rein diese Möglichkeit dazu führen kann die „andere“ Umgebung höher einstufen zu müssen.

Abb. 2: Sicherheitsklassen

Out of Scope:

Spezialthemen wie „Tokenisierung“ sind in der Aufstellung nicht enthalten. Dito Desktopvirtualisierungen oder VMs im Allgemeinen.
Basistechnologien wie SSL beim Anmelden werden vorausgesetzt.

„keine“:

Dieser Fall deckt den Benutzer ab, der eine Seite oder App als Informationsquelle nutzt. Benutzerseitig sind hier keine weiteren Anforderungen zu sehen. Serverseitig wird ein Basisschutz aus den bekannten Bausteinen wie Firewall usw. angenommen, um Angriffe auf die serverseitige Infrastruktur abzuwehren. Durch Vorgaben wie im Bundesdatenschutzgesetz (BDSG) sind in dieser Sicherheitsklasse keine personenbezogenen Daten im Spiel.

„Bronze“:

Diese Klasse sieht eine Anmeldung vor. Dem Benutzer ist es überlassen wie er sein Gerät sichert. Serverseitig sind diese Anmelde und ggf. personenbezogenen Daten durch geeignete Massnahmen wie Zugriffsbeschränkung der Administratoren, Protokollierung des Zugriffs und ggf. Verschlüsselung zu schützen. Um eine Anmeldung zu ermöglichen ist es sinnvoll ein Access Control System einzusetzen. Damit Single-Sign-On zwischen eigenen und fremden Angeboten möglich wird wird empfohlen auch die gängigen Standards wie OAuth, SAML, OpenID Connect zu unterstützen.
Sollen Daten zu Test- oder Auswertezwecken ohne explizite Freigabe des betroffenen Nutzers verwendet werden empfiehlt sich der Einsatz einer Maskierung beim Datenauszug bzw. Übertrag.

„Silber“:

Bei kritischen Daten wie im Onlinebanking bei Transaktionen oder im Falle von Gesundheitsdaten bei remote Überwachung von kritischen Patienten ist es sinnvoll diese stärker zu schützen. Hier ist nebn der Verschlüsselung eine Mehrfaktor Authentifizierung zu sehen ebenso wie One Time Token (z.B. per SMS) um die Wahrscheinlichkeit dass der angenommene Benutzer auch wirklich der angemeldete Benutzer ist zu erhöhen. Serverseitig ist sicherzustellen dass der Administrator keinen Zugriff auf die Daten oder Transaktionen bekommt, auch nicht im Backup o.ä.
optional: Je nach Schutzwunsch des Benutzers kann auch eine sichere Ablaufumgebung wie bei HBCI gewählt werden. Je nach Schutzwunsch des Unternehmens kann auch eine sichere Ablaufumgebung (MDM/MAM) im Falle für Smartphones/Tablets vorgegeben werden.

„Gold“

Die höchste Klasse wartet mit Funktionen auf um situativ zu reagieren. Kontextabhängig wird dabei die Authorisierung geprüft, um im Bedarfsfall weitere Authentifizierungsschritte des Benutzers einzufordern oder die Aktion/Transaktion abzubrechen. Auch können dynamisch Funktionen eingeschränkt oder Daten gefiltert werden. Kontextabhängig ist dabei der (wechselnde) Aufrufort des Benutzers, das Gerät (erkennbar an einem digitalen Fingerprint), der bisher durchgeführten Transaktionen etc.
Neben dem situativen/kontextbasiertem erfolgt eine systemübergreifende Überwachung der Accesslogs. Diese werden korreliert um entsprechende Aktionen abzuleiten (z.B. beim Zugriffsversuch über mehrere Kanäle den account sperren).
Über eine zentrale Administration können Devices auch remote gelöscht werden.

Im Überblick stellt sich das wie folgt dar:

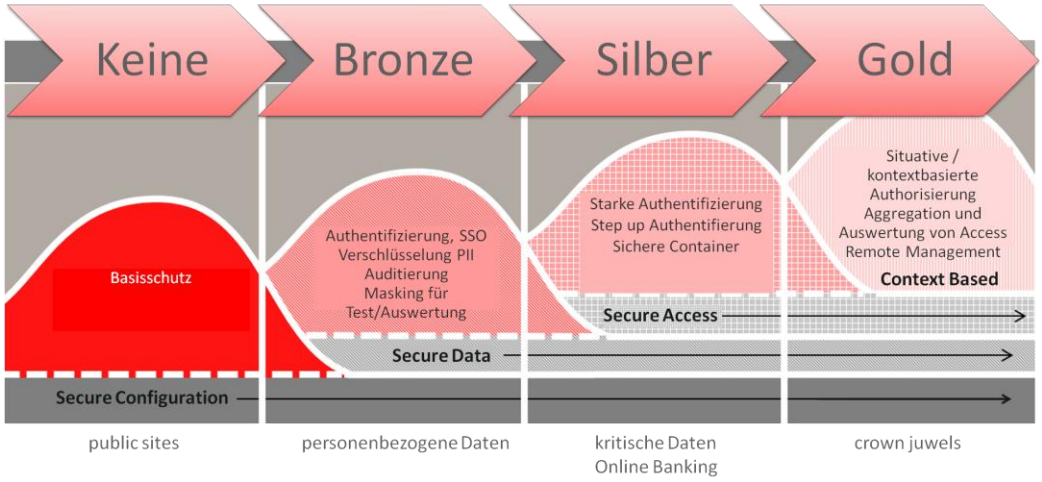

Abb. 3: Sicherheitsklassen und deren Grundfunktionen

Eine einfache Verteilung auf das Gerät des Benutzers und die Serviceseite sieht dabei so aus:

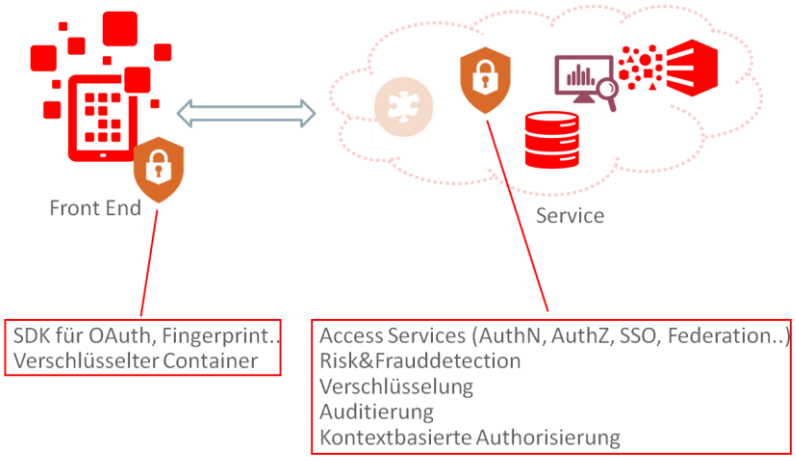

Abb. 4: Verteilung der Sicherheitsfunktionen

Umsetzung

Die Umsetzung erlaubt den Einsatz verschiedenster Technologien und Hersteller. Für eine Umsetzung mit Oracle sind die Produktgruppen unter den Schutzklassen aufgeführt.

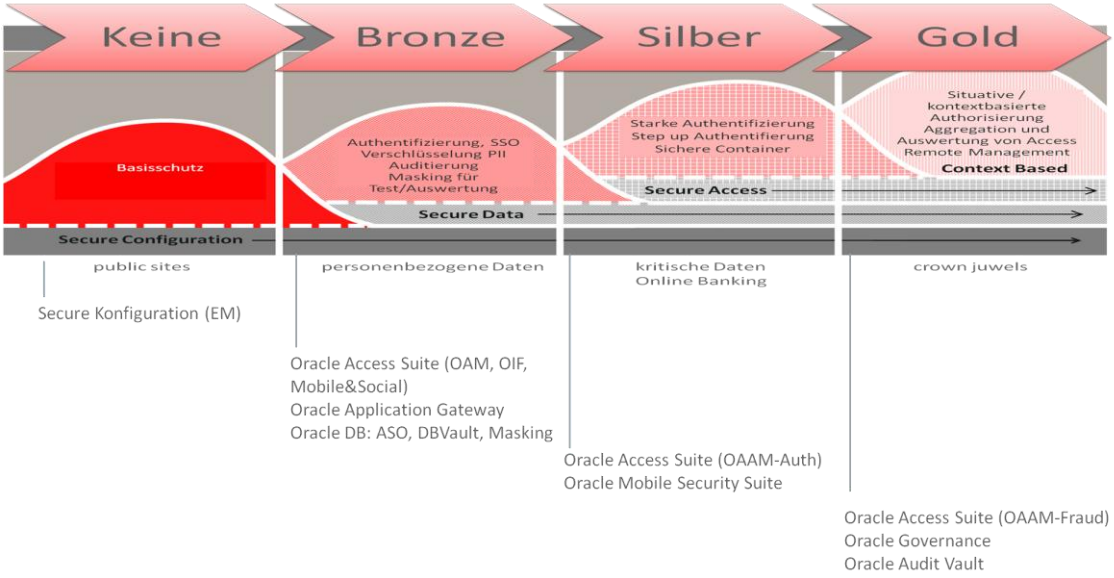

Abb. 5: Umsetzung Sicherheitsklassen mit Oracle

Die folgende Abbildung zeigt eine Umsetzung aller Sicherheitsklassen mit Oracle Komponenten in einer logischen Achitektur. Hierbei sind der Übersichtlichkeit halber die Management und Monitoringkomponenten ausgeblendet genaus wie die Integration mit Cloud und Social Services, die natürlich gegeben ist.

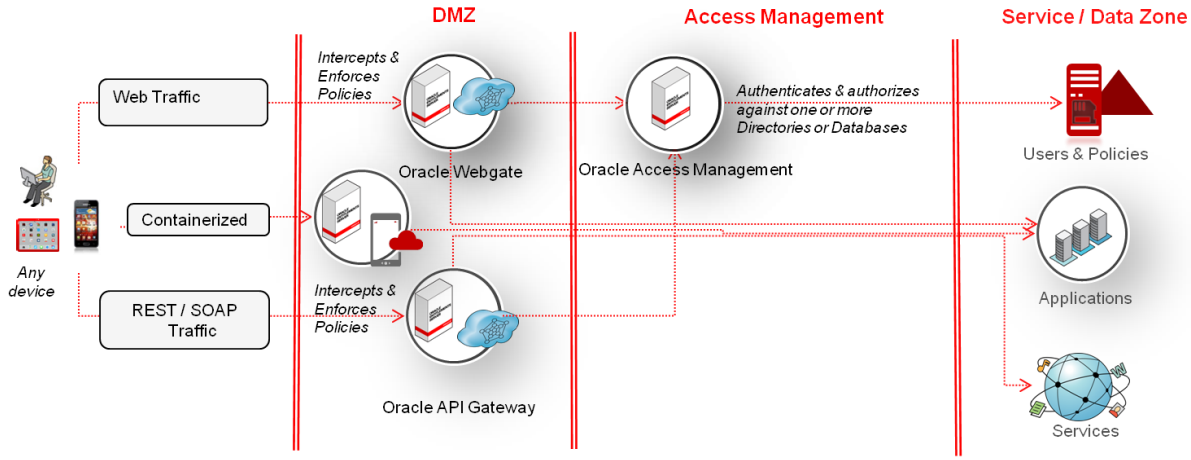

Abb. 6: Sicherheitsklassen in einer Oracle Architekur vereint

Bei einer Umsetzung mit Oracle kommen die Vorteile einer Vorintegration zum Tragen. Durch die Unterstützung von Standards an den jeweiligen Schnittstellen lassen sich die Komponenten herstellerübergreifend mischen als auch über verschiedene Rechenzentren / Cloud verteilt betreiben/integrieren.

Fazit

Mobile, Social, Cloud und eine informationszentrische Sicht ändern bestehende Geschäftabläufe und –strukturen nachhaltig. Security und Identity Management sind wichtige Begleiter dieser Trends und gehören gleich zu Beginn einer neuen Initiative mit auf die Agenda. Aber die eine Technik, die alles transparent und non-invasiv absichert gibt es so nicht. Bestehende Regeln und Identitätsspeicher wieder zu verwenden und neue Silos zu vermeiden ist sinnvoll und möglich. Kontextbasierte Entscheidungen (Ort, Gerät, Zeit, Historie) und feingranulare Steuerung auf den Zugriff von Dokumenten und Daten sowie die verschlüsselte Ablage und Übertragung von Daten auf mobile Endgeräte gehören dabei ebenso betrachtet wie die Integration in soziale Netzwerke.

Diese Anforderungen lassen sich gruppiert in verschiedene aufeinander aufbauende Sicherheitsklassen abbilden. Oracle hat Komponenten oder Technologien im Portfolio die diese Anforderungen umsetzen können. Viele Kunden nutzen erfolgreich den Oracle Ansatz für die Umsetzung der Sicherheitsklassen. Die folgende Abbildung nennt einige davon, unterschieden in die jeweilige Einsatzart:

Abb. 7: Kunden die Oracle verwenden, um Sicherheitsklassen umzusetzen

Weitere Informationen finden Sie im Internet unter www.oracle.com/identity.

Kontaktadresse:

Michael Fischer

ORACLE Deutschland B.V. & Co. KG

Riesstr. 25

80992 München

Telefon: +49 (0)172 8323654

E-Mail michael.fischer@oracle.com

Internet: www.oracle.de