UNITED SECURITY PROVIDERS

MOBILE DEVICE SECURITY

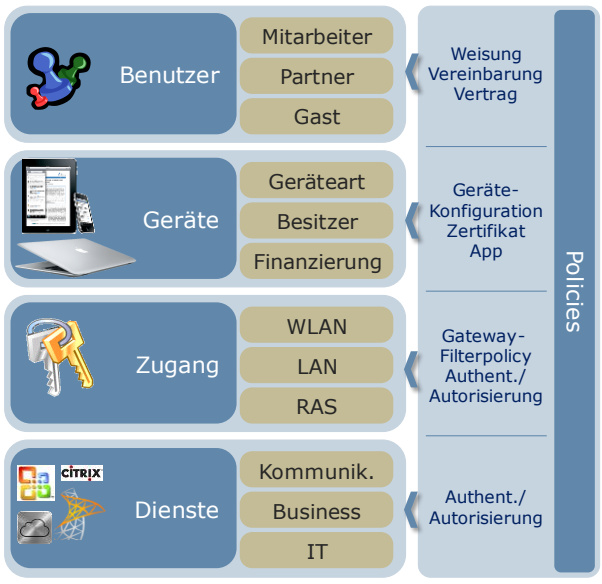
BYOD

Sicherer und produktiver Einsatz von Smartphones und Tablets im Unternehmen

Die Einführung von Bring Your Own Device (BYOD) im Unternehmen ist eine komplexe Aufgabe. Neue Anforderungen auf technischer, organisatorischer und rechtlicher Seite erfordern eine enge Zusammenarbeit unterschiedlicher Bereiche im Unternehmen. Entsprechend ist ein durchdachtes Vorgehen von Beginn weg ein zentraler Erfolgsfaktor. United Security Providers lenkt die Aufmerksamkeit auf die wichtigen Aspekte und sorgt mit einem praxisbewährten Vorgehen für eine erfolgreiche Umsetzung – von der Strategie bis hin zum Betrieb.

DIE AUSGANGSLAGE

Die Mitarbeiter sorgen mit ihrem Wunsch nach Wahlfreiheit bei der Beschaffung ihres Arbeitsmittels für einen regelrechten Kulturwechsel. Die neuen Rahmenbedingungen werfen viele Fragen auf und führen in vielen Unternehmen zu heftigen Diskussionen über Sicherheit und Effizienz bei der Arbeit. Neue Mittel und Medien lassen sich kaum noch aus dem Unternehmensalltag verbannen. Eine kontrollierte Einführung birgt weit geringere Risiken, als dem Mitarbeiter die Wahl der Mittel und Wege zu überlassen um interne Daten auf seinem privaten Smartphone oder Tablet zu bearbeiten. Doch mit der Nutzung privater Geräte im geschäftlichen Umfeld wird nicht nur die IT-Architektur vor neue Herausforderungen gestellt. Auch auf rechtlicher Seite tauchen neue Aspekte auf, die adressiert werden müssen.



Die fünf strategischen Dimensionen im Thema BYOD

DAS RICHTIGE MASS

Häufig steht im Zentrum der Diskussion, welche Geräte für den Zugriff auf unternehmensinterne Daten zugelassen werden sollen. Doch dies ist nur ein Aspekt, den es zu bestimmen gilt. Insgesamt sind fünf strategische Dimensionen zu definieren: Benutzer, Geräte, Zugang, Dienste und Policies. Diese weisen gegenseitige Abhängigkeiten auf, die eine isolierte Betrachtung der einzelnen Dimensionen praktisch unmöglich machen. Ziel ist es, beim Verändern einer Dimension die Auswirkungen auf alle anderen Dimension sofort erkennen zu können um so zu einer realisierbaren Gesamtlösung zu gelangen. Im Zuge der Festlegung der fünf Dimensionen kristallisieren sich die für das Unternehmen relevanten Geschäftsfälle fast von alleine heraus. Das richtige Mass ist dann erreicht, wenn sowohl das Unternehmen als auch die Mitarbeiter einen spürbaren Nutzen aus dem Einsatz der mobilen Geräte ziehen können.

KOSTEN SPAREN MIT BYOD

Dem Mitarbeiter die Beschaffung und den Betrieb der Arbeitsmittel wie Smartphones und Tablets oder gar Laptops zu überlassen, verspricht auf den ersten Blick willkommene Kosteneinsparungen. Die durch die Typenvielfalt entstehenden Supportkosten und Ineffizienzen können diese Einsparungen aber schnell wieder wettmachen. Eine positive Bilanz zu schaffen, bedarf einer genauen Betrachtung der verschiedenen Finanzierungsmodelle. Je nach Unternehmen und Belegschaft sind Aspekte wie Typenvielfalt und Kostenaufteilung unterschiedlich zu bewerten. Um die effiziente Nutzung der Lösung zu gewährleisten, empfiehlt es sich, rechtzeitig eine leistungsfähige Supportorganisation bereit zu stellen.

UNITED SECURITY PROVIDERS

MOBILE DEVICE SECURITY

BYOD

SICHERHEIT DURCH INTEGRATION

Der Einsatz von Smartphones und Tablets bildet eine neue Komponente in der IT-Infrastruktur von Unternehmen. Die bekanntermassen risikobehafteten Geräte müssen analog zur bereits vorhandenen Infrastruktur wie Laptops in das Sicherheitsdispositiv am Perimeter integriert werden. Zentrale Komponente dafür ist ein Mobile Device Management System (MDM), das die Verwaltung der mobilen Neulinge übernimmt. Das MDM setzt eine Policy auf dem mobilen Gerät durch, welche die bestehenden Freiheiten einschränkt. Damit steht die notwendige Sicherheitsfunktionalität zur Verfügung, wenn mit dem Gerät auf Unternehmensdaten zugegriffen wird.

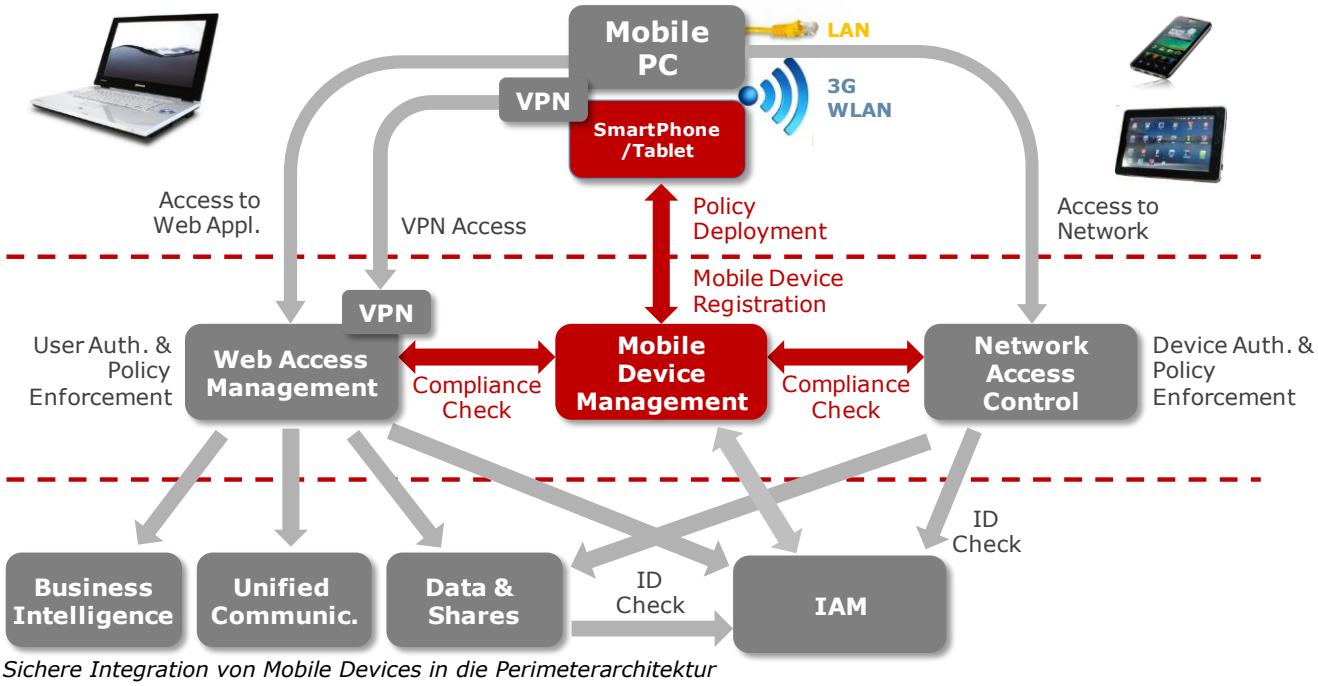
Der Sicherheitsgewinn entsteht jedoch erst dann, wenn die aus dem MDM stammenden Informationen über den Zustand des mobilen Gerätes im Perimeter für den Zugangsentscheid ins Unternehmensnetz genutzt werden können.

UNSER ANGEBOT

United Security Providers führt mit seinen Spezialisten in folgenden Schritten durch das Vorhaben:

- Erstellen einer passenden BYOD-Strategie basierend auf den fünf strategischen Dimensionen
- Erarbeiten der wichtigsten Anwendungsfälle
- Erstellen der rechtlich relevanten Weisungen und Vereinbarungen
- Erstellen eines Umsetzungskonzeptes
- Stufenweiser Aufbau und Einführen der Lösung sowie Betriebsunterstützung

Die einzelnen Schritte können je nach Umfang und Mitarbeiter durch den Kunden selbst erarbeitet werden. United Security Providers führt auf Anfrage vorbereitende Workshops durch.



Sichere Integration von Mobile Devices in die Perimeterarchitektur

NETWORK ACCESS CONTROL UND WEB ACCESS MANAGEMENT VERVOLLSTÄNDIGEN DIE BYOD-LÖSUNG.

Das MDM liefert Informationen über den Zustand des mobilen Gerätes an das USP Network Authentication System™, wo entschieden wird, ob und in welches Netzwerk der Zugriff erfolgen kann.

In Ergänzung dazu liefert das MDM Informationen an den USP Secure Entry Server™. Anhand dieser Information kann automatisiert entschieden werden, ob und auf welche Web Anwendungen zugegriffen werden darf.

United Security Providers AG
Stauffacherstrasse 65/15·CH-3014 Bern
Tel +41 31 959 02 02·Fax +41 31 959 02 59

Förrlibuckstrasse 70 CH-8005 Zürich
Tel +41 44 496 61 11·Fax +41 44 496 61 99

info@united-security-providers.ch
www.united-security-providers.ch