HOB GmbH & Co. KG
Schwadermühlstr. 3
90556 Cadolzburg

Tel: +49 9103 715 3715
Fax: +49 9103 715 3271
E-Mail: marketing@hob.de
Internet: www.hob.de

WhitePaper

HOBLink Mobile -

Mit Smartphone und Tablet auf E-Mails, Kalender, Kontakte und Notizen im Unternehmensnetzwerk zugreifen.

April 2014

Your knowledge.

Your people.

Your future.

Abstract

HOBLink Mobile ist eine Lösung von HOB, die es Mitarbeitern erlaubt, mit einem Smartphone oder Tablet per Fernzugriff auf E-Mails, Kalender, Kontakte und Notizen aus dem Unternehmensnetzwerk zuzugreifen.

Dieses Whitepaper zeigt Probleme auf, die beim Fernzugriff auf Unternehmensdaten mit einem mobilen Endgerät entstehen können und erläutert, wie diese mit HOBLink Mobile beseitigt werden können.

Einleitung

Probleme beim geschäftlichen Einsatz von mobilen Geräten

In der dynamischen Welt von heute gewinnt mobiles Arbeiten immer mehr an Bedeutung. Die Möglichkeit, zu jeder Zeit und von jedem Ort aus arbeiten zu können, hat sowohl für Mitarbeiter als auch für Unternehmen Vorteile. Mitarbeiter können ihre Arbeitszeiten flexibel gestalten, was sich positiv auf die Work-Life Balance auswirkt. Unternehmen profitieren wiederum von der erhöhten Produktivität und Zufriedenheit ihrer mobilen Arbeitnehmer.

Die Beliebtheit von mobilen Arbeitsplätzen spiegelt sich auch in aktuellen Studien wider. Eine Studie aus 2013 besagt, dass 32 Prozent der deutschen Arbeitnehmer regelmäßig von unterwegs auf Unternehmensdaten zugreifen.[1] Dabei ist insbesondere der Zugriff auf E-Mails und Kalender beliebt (28% der Befragten). Eine weitere Umfrage aus 2012 fand heraus, dass 92% der befragten Unternehmen geplant hatten, bis Ende 2013 mobiles Arbeiten weiter zu fördern bzw. einzuführen.[2] Aus einer HOB Umfrage unter 250 CTOs und CIOs von 2013 geht hervor, dass 72% der Befragten erwarten, dass die Anzahl an Mitarbeitern, die Möglichkeiten für den Fernzugriff auf Unternehmensdaten benötigen, in den nächsten 12 Monaten deutlich steigen wird.[3]

Im Rahmen von mobilen Arbeitsplätzen gewinnen insbesondere mobile Endgeräte wie Smartphones oder Tablets an Bedeutung. Die anhaltende Konsumerisierung der IT führt dazu, dass mehr und mehr Arbeitnehmer sich wünschen, ihr privates Smartphone auch beruflich nutzen zu können – Stichwort Bring Your Own Device (BYOD).

Die Umfrage von HOB zeigt, dass 54% der Befragten Entscheidungsträger glauben, dass ihre Mitarbeiter unter anderem private Mobilgeräte benutzen, um auf Unternehmensserver zuzugreifen. Aus einer anderen Studie von 2012 geht hervor, dass mittlerweile 43% der befragten ITK-Unternehmen es erlauben, private Mobilgeräte geschäftlich zu nutzen. Allerdings haben nur 60% dieser Unternehmen spezielle Regeln für die Nutzung privater Mobilgeräte aufgestellt. 53% der befragten Unternehmen lehnen private Endgeräte am Arbeitsplatz komplett ab, weil sie einen erhöhten Wartungsaufwand und Sicherheitsrisiken fürchten.[4] Zudem können bei der beruflichen Nutzung von privaten Endgeräten datenschutzrechtliche Probleme auftreten.

Für Unternehmen lassen sich bei der Nutzung von Mobilgeräten somit drei grundliegende Problemfelder erkennen, die es für die erfolgreiche Implementierung von mobilen Arbeitsplätzen zu beachten gilt:

Sicherheitsrisiken

Durch den Zugriff von Mobilgeräten auf Unternehmensserver verlassen unternehmenskritische Daten das sichere Unternehmensnetzwerk, wodurch Sicherheitslücken entstehen können. Der Verlust eines Mobilgeräts führt gleichzeitig zum Verlust der gespeicherten Unternehmensdaten oder -kontakte. Des Weiteren können insbesondere private, ungeschützte Mobilgeräte leicht von Hackern angegriffen werden, die es auf Unternehmensdaten abgesehen haben.

Datenschutzrechtliche Probleme

Bei der beruflichen Nutzung eines privaten Mobilgerätes kommt es zu einer Mischung privater und geschäftlicher Daten. Dies ist aus Datenschutzgründen bedenklich, da das Gesetz (§ 9 Bundesdatenschutzgesetz) extrem hohe Anforderungen an die Verarbeitung und Speicherung von personenbezogenen Unternehmensdaten stellt, die bei der privaten Nutzung eines Smartphones kaum zu erfüllen sind. Gleichzeitig müssen aber auch private Daten vor Einflüssen des Unternehmens geschützt werden.

Administrationsaufwand

Für IT-Administratoren entsteht ein erhöhter Administrationsaufwand. Neben dem Arbeitsplatz im Unternehmen muss zusätzlich der mobile Arbeitsplatz in Form eines Mobilgeräts administriert werden. Womöglich muss hierfür jedes Gerät einzeln in die Hand genommen werden.

Mit HOBLink Mobile ist es Unternehmen möglich die soeben genannten Probleme zu beseitigen und von den Vorteilen mobiler Arbeitsplätze zu profitieren. Wie HOBLink Mobile dies ermöglicht, soll nachfolgend genauer erläutert werden. Dazu wird zunächst auf die Funktionsweise von HOBLink Mobile eingegangen und anschließend erläutert, wie diese konkret dazu beiträgt, die genannten Probleme zu lösen.

HOBLink Mobile

Architektur und Funktionsweise

Die HOBLink Mobile Lösung besteht aus zwei Komponenten, die miteinander kommunizieren und somit den sicheren Zugriff auf Unternehmensdaten gewährleisten: Die HOBLink Mobile App und der HOBCOM Universal (HCU) Server.

Die *HOBLink Mobile App* kann für Apple iOS und Android Geräte aus dem entsprechenden App Store kostenfrei heruntergeladen werden und wird auf dem Clientgerät installiert. Nach Öffnen der App müssen nur noch Benutzername, Passwort und Servername eingegeben werden, um eine Verbindung zum HCU Server herzustellen. Nach erfolgreicher Authentifizierung am Server wird dem Anwender eine Liste der für ihn freigeschalteten Anwendungen (E-Mail, Kalender, Kontakte, Notizen) angezeigt, aus denen er sich für eine entscheiden kann. Selbstverständlich ist es auch möglich, nacheinander verschiedene Anwendungen auszuführen.

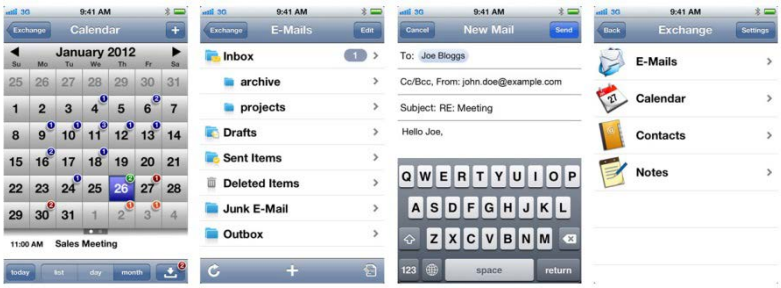

Abbildung 1: Screenshots von HOBLink Mobile App

Der *HCU Server* befindet sich in der DMZ oder im LAN des Unternehmens und untersteht somit den Sicherheitsvorkehrungen des Unternehmens. Der HCU Server nimmt Clientanfragen entgegen und übermittelt diese an den Exchange Server, auf dem sich E-Mails, Kontakte, Notizen und Kalenderinformationen befinden. Die Antwort des Exchange Servers wird dann wiederum an den Client übertragen. Aus Sicherheitsgründen und für eine optimierte Bandbreitenausnutzung werden hierbei nur Daten an das Mobilgerät geschickt, die gerade für die Anzeige benötigt werden. Solange HOBLink Mobile aktiv ist werden diese Daten in den Hauptspeicher geladen. Wird die Anwendung beendet, verbleiben keine Daten auf dem Endgerät. Somit besteht keine Gefahr, dass wertvolle Unternehmensdaten von dem Mobilgerät entwendet werden.

Die Kommunikation zwischen der HOBLink Mobile App und dem HCU Server kann entweder direkt mit dem Unternehmensserver oder über den HOB WebSecureProxy (WSP) erfolgen.

Bei der direkten Kommunikation wird diese mit AES (128 bit) verschlüsselt. Zur Authentifizierung steht die Kombination aus Username und Passwort zur Verfügung. Eine grafische Übersicht über die direkte Kommunikation bietet Abbildung 2.

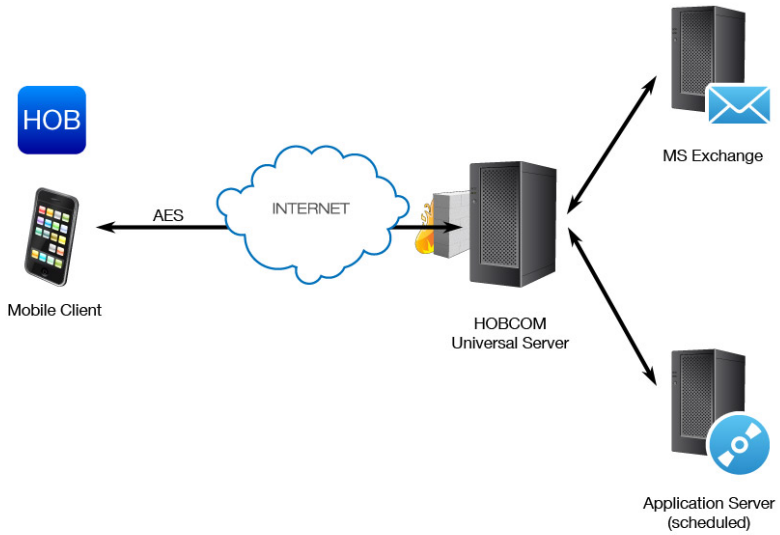

Abbildung 2: Direkte Kommunikation zwischen App und HCU Server

Bei der indirekten Kommunikation über den HOB WSP erfolgt die Kommunikation mit SLL Verschlüsselung (siehe Abbildung 3). Darüberhinaus stehen erweiterte Authentifizierungsmöglichkeiten wie Zertifikate, RADIUS oder One-Time Passwort Tokens zur Verfügung.

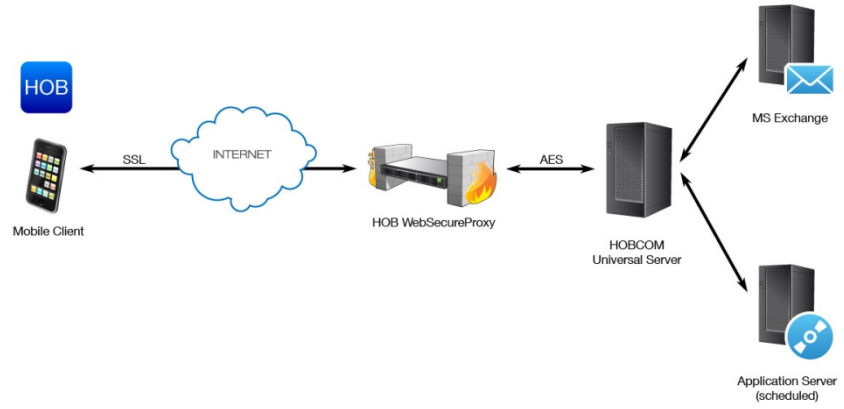

Abbildung 3: Indirekte Kommunikation zwischen App und HCU Server

Problemlösung mit HOBLink Mobile

Aufgrund der Architektur und Funktionsweise von HOBLink Mobile können die zu Anfangs erwähnten Probleme leicht gelöst werden, so dass Sie und ihr Unternehmen von den vollen Potentialen mobiler Arbeitsplätze profitieren können.

Sicherheitsrisiken

Die von vielen Unternehmen befürchteten Sicherheitsrisiken, die sich aus dem mobilen Zugriff auf Unternehmensdaten ergeben können, werden durch den Einsatz von HOBLink Mobile beseitigt. Da bei der Benutzung zu keiner Zeit Daten auf dem Mobilgerät gespeichert werden, können diese selbst bei einem Verlust oder Diebstahl des Mobilgeräts nicht verloren gehen. Dank der Verschlüsselung der Kommunikation mit AES bzw. SSL ist HOBLink Mobile auch vor ungewollten Abhörattacken geschützt. Die verschiedenen Authentifizierungsmöglichkeiten stellen außerdem sicher, dass nur Personen Zugriff auf E-Mails, Kalender, Kontakte und Notizen erhalten, die dazu berechtigt sind.

Datenschutzrechtliche Probleme

Auch die strikte Trennung von privaten und geschäftlichen Daten ist mit HOBLink Mobile gewährleistet. Dank des Sandboxkonzepts von HOBLink Mobile bleiben geschäftliche Daten von privaten stets getrennt. Der Zugriff auf Unternehmensdaten erfolgt sozusagen isoliert vom restlichen, privaten Betrieb des Mobilgeräts. Unternehmen können somit sicherstellen, dass es zu keiner Vermischung von privaten und geschäftlichen Daten kommt und es keine Konflikte mit Datenschutzbestimmungen gibt. Anwender brauchen wiederum keine Angst zu haben geschäftliche Daten aus Versehen zu verlieren oder zu löschen. So bleibt das Mobilgerät privat und kann von Mitarbeitern noch immer als solches benutzt werden.

Administrationsaufwand

Normalerweise ist das Schaffen von mobilen Arbeitsplätzen mit viel Aufwand für IT-Administratoren verbunden. Die IT-Infrastruktur muss neuen Anforderungen angepasst werden, indem neue Server bzw. Softwarepakete installiert werden. Womöglich muss jedes einzelne Mobilgerät angefasst und für den Unternehmenseinsatz konfiguriert werden. Falls ein Gerät verloren geht, bleibt IT-Administratoren oft keine andere Wahl als die gesamten Daten auf dem Mobilgerät per Remote Wipe zu löschen. Mit HOBLink Mobile reduziert sich der Aufwand für IT-Administratoren erheblich. Auf Unternehmensseite muss lediglich der HCU Server installiert und mit dem Exchange Server verknüpft werden. Anwender können sich einfach und unkompliziert die HOBLink Mobile App über den Apple App Store herunterladen. Nach Eingabe von Benutzername, Passwort und Servername können die Mitarbeiter direkt auf ihre

E-Mails, Kontakte, Kalender und Notizen zugreifen. HOBLink Mobile überzeugt zudem mit seiner hohen Skalierbarkeit. Neue Mitarbeiter können durch einige Klicks seitens der Administration einfach hinzugefügt werden. Genauso einfach kann der Zugang gesperrt werden, wenn Mitarbeiter das Unternehmen verlassen. Da zu keiner Zeit geschäftliche Daten auf dem Gerät gespeichert wurden, muss dieses im Nachhinein auch nicht bereinigt werden. Es reicht vollkommen aus, den Benutzerzugang zentral zu sperren.

Fazit

Mobiles Arbeiten bietet Unternehmen und Mitarbeitern gleichermaßen Vorteile. Mitarbeiter profitieren von mehr Flexibilität in ihrem Beruf und Unternehmen von einer höheren Produktivität. Ein besonderer Trend ist die Nutzung von (privaten) Smartphones und Tablets für den Zugriff auf Unternehmensdaten. Dabei können für Unternehmen Sicherheitsrisiken, datenschutzrechtliche Probleme und ein erhöhter Administrationsaufwand entstehen.

HOBLink Mobile bietet Unternehmen die Möglichkeit diese Probleme zu beseitigen. Da zu keiner Zeit Daten auf dem Endgerät gespeichert werden und die Kommunikation zwischen Client und Server verschlüsselt erfolgt, können Sicherheitsrisiken minimiert werden. Dank des Sandboxkonzepts von HOBLink Mobile bleiben geschäftliche und private Daten dauerhaft voneinander getrennt, wodurch Bedenken bezüglich des Datenschutzes ausgeräumt werden. Der Administrationsaufwand kann aufgrund der zentralen Verwaltung von Benutzern ebenfalls minimiert werden.

Weitere Informationen zu HOBLink Mobile finden Sie auf rer Website und in der Info-Broschüre zu HOBLink Mobile. Gerne können Sie uns auch telefonisch oder per E-Mail kontaktieren.

Quellenverzeichnis

1 – BITKOM 2013: „Jeder Dritte greift mobil auf Unternehmensdaten zu“. http://www.bitkom.org/de/themen/64026_76620.aspx

2 – Citrix 2012: „Studie: Deutschland beim mobilen Arbeiten führend“. http://www.citrix.de/news/announcements/mar-2012/studie-deutschland-beim-mobilen-arbeiten-fhrend.html

3 – HOB 2013: „HOB Trend Guide: HOB Umfrage enthüllt neue Trends rund um Remote
cess“. http://www.hob.de/news/2013/news2213.jsp

4 – BITKOM 2012: „Private Smartphones werden für den Job genutzt“. http://www.bitkom.org/de/themen/54633_73615.aspx

(09.04.2014 TE)

HOB GmbH & Co. KG
Schwadermühlstr. 3
90556 Cadolzburg

Tel: +49 9103 715 3715
E-Mail: marketing@hob.de
Internet: www.hob.de