



HOB GmbH & Co. KG
Schwadmühlstr. 3
90556 Cadolzburg

Tel: 09103 / 715-0

Fax: 09103 / 715-271

E-Mail: support@hob.de

Internet: www.hob.de

WhitePaper

HOB Desktop-on-Demand -

Sicherer Zugriff auf Ihren Arbeitsplatz – orts- und plattformunabhängig

November 2010

HOB Desktop-on-Demand - Sicherer Zugriff auf Ihren Arbeitsplatz - orts- und plattformunabhängig

Verschiedenartige Einflüsse können den Ablauf von Unternehmensprozessen und damit die Business Continuity empfindlich stören. An Banken, Kreditinstitute, Finanzdienstleistungsinstitute und Versicherungen werden umfangreiche Forderungen seitens der Gesetzgebung gestellt. Diese sind unter anderem im KontTraG, HGB, KWG, aber auch AktG zu finden. Im Gesetz über das Kreditwesen (Kreditwesengesetz oder KWG) und in den Mindestanforderungen an das Risikomanagement (MaRisk) der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) werden spezielle Anforderungen an Banken, Kreditinstitute, Finanzdienstleistungsinstitute und Finanzdienstleister gestellt. Für Versicherer und Versicherungsunternehmen gilt analog das Gesetz über die Beaufsichtigung der Versicherungsunternehmen (Versicherungsaufsichtsgesetz oder VAG) und demnächst der Entwurf eines Rundschreibens Aufsichtrechtliche Mindestanforderungen an das Risikomanagement (MaRisk VA).

Durch den Ausbruch des isländischen Vulkans im März 2010 wurde deutlich, wie unerwartet die Geschäftsabläufe gefährdet werden können. Unzählige Geschäftsleute saßen an Flughäfen oder an anderen Orten fest und waren durch den Vulkanausbruch von Ihrer Firma bzw. von Ihrer Arbeit abgeschnitten. In diesem Zusammenhang ist es enorm wichtig auch andere Umwelteinflüsse, wie Pandemien (Schweinegrippe, Vogelgrippe, uvm.), Umweltkatastrophen (Tsunamis, Erdbeben, Vulkanausbrüche, uvm.) oder auch einfach nur die Schließung des Firmengebäudes aufgrund eines Bombenfundes in der Umgebung zu bedenken. Es gibt sehr vielfältige Einflüsse, welche sich auf die Business Continuity auswirken. Die aufgeführten Beispiele sollen dies verdeutlichen. Die Folgen einer Notfallsituation können empfindliche Störungen der Geschäftsprozesse, Ausfallzeiten oder personelle Ausfälle sein. Das es auch eine Kombination aus alledem sein kann, verdeutlichte der vor kurzem ausgebrochene isländische Vulkan. Um die Fortführung des Unternehmensgeschehens auch im Katastrophenfall abzusichern, bedarf es einer Lösung, welche die Abwicklung der Geschäfte auch von außerhalb des Unternehmens ermöglicht.

Der Remotezugriff auf den Arbeitsplatz-PC ist auch für flexible Arbeitsmodelle ein wichtiger Punkt. Seit Jahren ist in der Arbeitswelt der Trend hin zu flexiblen Arbeitsmodellen zu verfolgen. Geprägt von dem Wunsch nach Vereinbarkeit von Beruf, Familie und Privatleben sind flexible Arbeitszeiten und -plätze in vielen Unternehmen stark gefragt, ganz im Sinne einer Work-Life-Balance. Starre Arbeitsmodelle können so aufgeweicht werden und flexible Arbeitsmodelle nehmen ihren Platz ein und tragen hiermit dem demografischen Wandel und den veränderten Geschlechterrollen in der Arbeitswelt Rechnung.

Durch das Internet sind wir es gewohnt, jederzeit und von überall aus auf Informationen jeglicher Art zuzugreifen. Der Zugriff von unterwegs auf firmeninterne Applikationen oder Netzlaufwerke ist bereits Realität. Was jedoch, wenn sich die benötigten Daten auf dem eigenen Arbeitsplatz-PC befinden und dieser ausgeschaltet ist?

Beispiel: Vor dem Antritt Ihrer Geschäftsreise benötigen Sie noch Dokumente oder Dateien von Ihrem Arbeitsplatzrechner in der Firma. Sie können nun einen freundlichen Kollegen bitten, sich mit Ihrem Passwort (!) an Ihrem Rechner anzumelden und sich die benötigten Dokumente via Email schicken lassen. Natürlich können Sie auch selbst in die Firma fahren und die benötigten Dokumente oder Dateien holen.

Diese und auch andere Möglichkeiten sind mit teilweise enormen Kosten, aber auch Zeitaufwand verbunden. Inwiefern derartige Vorgehensweisen mit den Unternehmenssicherheitsrichtlinien zu vereinbaren sind, muss selbstverständlich ebenfalls geprüft werden. Mit HOB Desktop-on-Demand (HOB DoD) bieten wir Ihnen eine Softwarelösung mit deren Unterstützung Sie sich derartige Kosten einsparen und entspannt von jedem beliebigen Ort aus sicher arbeiten können. Alles was Sie benötigen, ist ein Zugang zum Internet, sowie einen Java-fähigen

Webbrowser (z.B. Mozilla Firefox, MS Internet Explorer, Opera, Safari, u.a.). Auf Ihrem Arbeitsplatz-PC muss für den Zugriff eines der folgenden Betriebssysteme installiert sein:

- ✓ Microsoft Windows XP^{*}
- ✓ Microsoft Windows Vista^{*}
- ✓ Microsoft Windows 7^{*}
- ✓ Linux (optional)
- ✓ Mac OS X (optional)

Der User von HOB DoD muss nichts auf dem lokalen Rechner installieren und benötigt daher auch keine Administrator-Rechte. Dieser wichtige Vorteil, kombiniert mit der einfachen, benutzerfreundlichen Bedienung verringert erheblich die Kosten der Einführung einer solchen Lösung. HOB DoD, als browserbasierte Lösung, ist plattformunabhängig und kein Third-Party Service. Die Komponenten werden im Firmennetz installiert und administriert. Gegenüber gewöhnlichen Third-Party Services bietet die Lösung aus dem Hause HOB auch den Vorteil, dass die Daten nur einmal über das Internet gesendet werden müssen. Hierdurch steigt die Performance und die Antwortzeiten sind kürzer. In der nachfolgenden **Abbildung 1** ist der schematische Ablauf eines Verbindungsaufbaus (SSL-verschlüsselt!) von einem externen Client, über ein öffentliches Netz, an den lokalen Arbeitsplatz-PC in der Firma dargestellt.

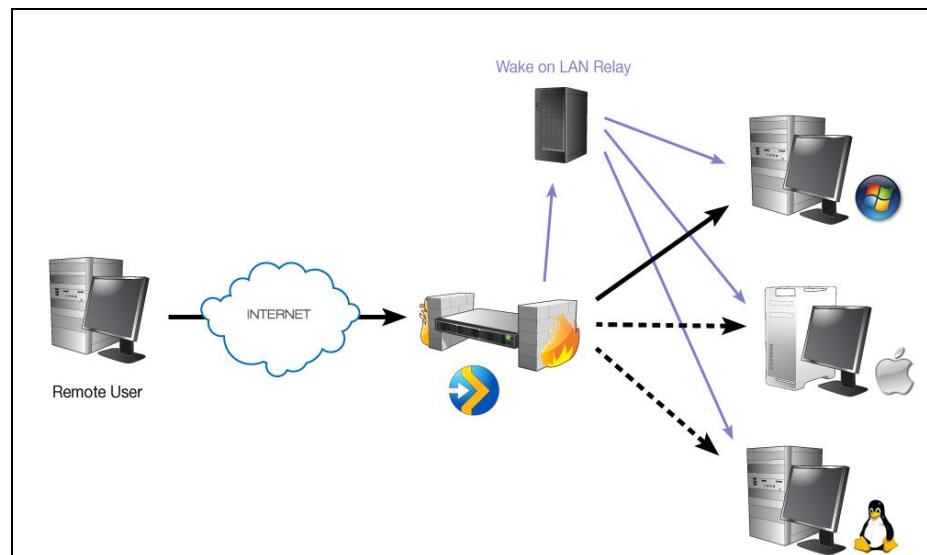


Abbildung 1: Schema HOB Desktop-on-Demand

Der Zugang auf den eigenen Arbeitsplatz funktioniert im Detail wie folgt:

Der Benutzer ruft über seinen favorisierten Webbrowser eine entsprechende, definierte Webseite auf. Bereits ab diesem Punkt wird eine sichere, SSL geschützte Verbindung zum Client etabliert. Auf dieser „Startseite“ wird der Benutzer mittels Anmeldefenster aufgefordert sich, entsprechend den gewählten Standards, zu authentifizieren. Nach erfolgreicher Authentifizierung beginnt der automatische Download der Clientsoftware HOBLink JWT. Wenn das Java-Applet erfolgreich geladen wurde (Downloadgröße <1MB), wird im nächsten Schritt das den Logindaten zugewiesene Profil automatisiert an den Client übertragen. Anhand des Profils wird entweder ein Zielauswahlfenster (Session Manager) angezeigt oder es wird direkt die Verbindung zum Arbeitsplatz-PC hergestellt.

Sämtliche Verbindungen sind SSL-verschlüsselt. In der Firewall ist es lediglich notwendig, einen Port (standardmäßig 443) zu öffnen. Es werden alle gängigen Verschlüsselungsalgorithmen, auch AES (Advanced Encryption Standard) mit bis zu 256 Bit Schlüssellänge unterstützt.

^{*} Aufgrund der Beschaffenheit der Betriebssysteme, sind Home-Editionen nicht für den Einsatz mit Desktop-on-Demand geeignet, da hier der integrierte RDP-Server von Microsoft nicht komplett freigeschalten wurde.

Die Zuordnung zwischen Benutzer und Arbeitsplatzrechner kann wahlweise in der Proxy-Konfiguration selbst oder im HOB Enterprise Access Server hinterlegt sein. Letztere Ablage der Konfigurationsdaten ermöglicht die Authentifizierung des Benutzers beispielsweise an Microsoft Active Directory Services oder anderen Authentisierungslösungen wie RSA SecurID oder VASCO DigiPass. Voraussetzung hierfür ist eine vorhandene RADIUS-Schnittstelle der beteiligten Komponenten.

Hat sich ein Benutzer mit dem Browser erfolgreich gegenüber dem HOB WebSecureProxy (WSP) authentifiziert und möchte nun auf seinen Desktop PC zugreifen, sendet der WSP ein Wake-on-LAN-Paket zu dem Arbeitsplatz-Rechner des Benutzers. Wake-on-LAN ist eine Technologie, welche seit 1995 besteht und heutzutage in fast allen PCs (genauer der Netzwerkkarte) implementiert ist.

Wake-on-LAN Pakete müssen als UDP Broadcast gesendet werden. Ist der WSP in der DMZ, so sind eventuell Broadcast Pakete durch die Firewall zum internen Netz geblockt. Auch diese Eventualität ist berücksichtigt und die Lösung ist wie folgt integriert:

Der WSP kann auch IP Unicast Pakete senden, welche problemfrei durch die Firewall gehen und dann von einem Wake-on-LAN Relay in ein Broadcast Paket umgeformt werden.

Das Wake-on-LAN Relay ist ebenfalls als plattformunabhängige Java-Applikation erhältlich und kann auf einem beliebigen Server im firmeninternen Netz Installiert werden.

Wird ein PC über Wake-on-LAN eingeschaltet, so dauert es eine gewisse Zeit, bis die RDP-Dienste beim Ziel-Arbeitsplatz-PC hochgefahren sind und der WSP die Verbindung zwischen User und dem nun hochgefahrenen PC herstellen kann. Der Benutzer wird über die vorrausichtliche Wartezeit (abhängig von der PC-Hardware und dem installierten Betriebssystem) informiert.

HOB DoD ist Teil der umfassenden Security-Lösung HOB RD VPN. HOB RD VPN ist vom BSI (Bundesamt für Sicherheit in der Informationstechnik) nach Common Criteria zertifiziert. Die Zertifizierung ist nach EAL2 unter dem Kenn-zeichen BSI-DSZ-CC-0260-2004 erfolgt. Aktuell wird die Zertifizierung nach EAL4+ durchgeführt.

Die HOB Desktop-on-Demand Lösung erlaubt jedem Benutzer, rund um die Uhr auf seinen Arbeitsplatz und dessen Anwendungen bzw. Daten zuzugreifen. Dabei spielt es keine Rolle ob der Zielrechner sich im ausgeschalteten Zustand befindet oder nicht. Egal ob es sich um kleinere, mittelständische Unternehmen oder Firmen mit Firewalls und DMZ handelt, der Zugang auf den Arbeits-platzrechner ist jederzeit und von überall möglich. Auf der Clientseite ist dafür nichts extra zu installieren, es wird lediglich ein Standard-Webbrowser und Java-Unterstützung vorausgesetzt. Ob ein Windows-, Mac- oder Linux-Betriebssystem am Client Verwendung findet, spielt dabei keine Rolle.