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

Remote Access über Hardware Appliances oder über Software

Februar 2013

Your knowledge.

Your people.

Your future.

Beim Einsatz von Remote Access Lösungen hat der Kunde die Wahl zwischen Hardware Appliances für das Gateway in der Firmen-Zentrale oder dem Einsatz einer reinen Software-Lösung.

Wenn eine Hardware-Appliance eingesetzt wird, dann stellt sich sofort die Frage: wie ist das beim Ausfall der Hardware, z.B. mit Ersatzteilen.
Bei Hardware muss man immer mit Ausfällen rechnen, wegen bewegten Teilen und Problemen wegen der anfallenden Hitze. Festplatten und Netzteile fallen häufig aus.

Wird eine Hardware-Appliance eingesetzt, dann müssen die Administratoren lernen, damit umzugehen, sowohl mit der Hardware der Appliance, als auch mit der darauf laufenden Software.
Es muss sich auch mehr als ein Administrator auskennen, Remote Access soll ja immer verfügbar sein.

Die Hardware-Appliance muss ins Netzwerk der Firma eingebunden werden, es müssen Netzwerk-Einstellungen wie z.B. auch DNS-Zugriffe konfiguriert werden.

Oft müssen in der Hardware-Appliance alle User angelegt werden, welche zugreifen sollen, welche sich authentifizieren müssen. Ein zusätzlicher Aufwand für zero-day User oder wenn ein Mitarbeiter das Unternehmen verlässt.

Es muss Datensicherung betrieben werden für die Konfiguration bzw. auch andere Software in der Hardware-Appliance.

Hat eine Hardware-Appliance Vorteile gegenüber einem Standard-Server, z.B. durch besondere Hardware-Komponenten?

Hardware-Appliance für Remote Access basieren heute auch auf Standard-Servern, es sind eventuell mehr NICs, Netzwerk-Karten, eingebaut.

Bei Switchen, welche wegen den schnellen Leitungen mit ASICs gebaut werden, also mit Hardware-Logik, könnte eine Software die Pakete nicht so schnell schalten.
Aber Router und alles war zum Zugriff über das Public Internet verwendet wird, verwenden Standard-Komponenten; schnelle Internet-Verbindungen sind auch sehr teuer. Die bei Remote Access verwendeten Internet-Verbindungen lassen sich sehr gut mit Standard-Komponenten abarbeiten, die Logik ist in Software implementiert und nicht in ASICs.

Wächst die Anzahl der über Remote Access angebundenen Benutzer, so muss eine größere Hardware-Appliance angeschafft werden. Das bedeutet zusätzliche Kosten.

Wie ist das mit einer Software-Lösung für Remote Access?

Die Software wird auf Standard-Servern installiert; in den Rechenzentren findet man Marken-Server welche auch für Remote Access genutzt werden können.

Die Administratoren kennen sich mit der eingesetzten Hardware und den Basis-Software-Komponenten bestens aus. Zusätzliche Schulung dieser Komponenten ist nicht von Nöten. Auch die Einbindung ins Netzwerk funktioniert bei Remote Access Software-Lösungen genauso wie bei anderer Software.

Standard-Server bieten auch Unterstützung für Verschlüsselung welche bei Remote Access eingesetzt wird.
Der gängiger Verschlüsselungs-Algorithmus ist heutzutage AES, Advanced Encryption Standard. AES ist sicher und weit verbreitet.
Neuere Intel CPUs bieten AES-Verschlüsselung in Hardware, direkt in der CPU, diese Funktion nennt Intel AES-NI. Auch andere Prozessor-Hersteller bieten AES-Verschlüsselung in Hardware oder haben diese Funktion auf der Roadmap.

Marken-Server sind oft schon mit mehreren Netzwerk-Karten (NICs) ausgestattet, zusätzliche Netzwerk-Karten einzubauen ist kein großer Aufwand und Netzwerk-Karten sind auch preiswert. Beim Einsatz in der DMZ (demilitarized zone) verwendet man oft unterschiedliche Netzwerk-Karten, einmal für das Public Internet, und einmal zum Zugriff auf das Firmen-Netzwerk.

Marken-Server haben spezifische Management-Funktionen integriert.
Die Administratoren kennen sich mit den Management-Funktionen der eingesetzten Marken-Server aus, andere Hardware wie Appliances für Remote Access zu managen bedeutet zusätzlichen Aufwand.

Software-Lösungen für Remote Access lassen sich auch virtualisiert betreiben, z.B. mit VMware oder Microsoft Hyper-V. Fällt ein Server aus oder muss Wartung erfolgen, so lässt sich die installierte Software schnell und bequem auf einen anderen Server übertragen.

Software-Lösungen lassen sich sehr gut in die Infrastruktur des Unternehmens integrieren. Dazu gehört auf Zugriff auf das LDAP-System in dem alle Benutzer-Einstellungen gespeichert sind. Oft wird als LDAP-System Active Directory von Microsoft eingesetzt.

Datensicherung kann durchgeführt werden mit den Tools welche sowieso im Einsatz sind.

Integration mit Kerberos ist möglich, dadurch bekommen die Benutzer secure single sign on beim Remote Zugriff.
Die beim Betrieb der Remote Access Lösung entstehenden Logs können archiviert werden, damit ist dann ein Auditing möglich.

Die Konfiguration der Software-Lösung kann jeweils in einem Repository abgespeichert werden; diese dient einseits der Dokumentation, andererseits kann auch bei einem Auditing auf ältere Konfigurationen zugegriffen werden.

Fazit: der Einsatz einer rein Software-basierten Lösung bietet viele Vorteile. Die Administration wird weniger belastet, das Unternehmen spart Kosten.

Manchmal kommt als Argument für die Hardware-Appliance: das wäre doch gehärtet, das wäre sicherer. Ich kenne keinen technischen Grund welcher diese Behauptung rechtfertig.
Umgekehrt ist es so, je besser sich die Administratoren mit der Lösung auskennen, desto seltener entsteht durch falsche Konfiguration ein Sicherheits-Loch.
Und es ist für Administratoren leichter, sich mit einer rein Software-basierten Remote Access Lösung auszukennen.

11.02.2013 KB